BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

MOBİL BULUT BİLİŞİMİN KİŞİSEL VERİ GÜVENLİĞİ AÇISINDAN İNCELENMESİ VE ELEKTRONİK HABERLEŞME SEKTÖRÜ AÇISINDAN DEĞERLENDİRMELER

Esra DURUOĞLU

Bilişim Uzmanlığı Tezi

Ocak 2024

Ankara

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

MOBİL BULUT BİLİŞİMİN KİŞİSEL VERİ GÜVENLİĞİ AÇISINDAN İNCELENMESİ VE ELEKTRONİK HABERLEŞME SEKTÖRÜ AÇISINDAN DEĞERLENDİRMELER

Esra DURUOĞLU

Bilişim Uzmanlığı Tezi

Ocak 2024

Ankara

Esra DURUOĞLU tarafından hazırlanan *"Mobil Bulut Bilişimin Kişisel Veri Güvenliği Açısından İncelenmesi ve Elektronik Haberleşme Sektörü Açısından Değerlendirmeler*" adlı bu tezin Bilişim Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Bilişim Uzmanı Dr. Savaş ÇITLAK

Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı tezi olarak kabul edilmiştir.

Başkan : _____
Kurul Üyesi, Nurettin ŞAR

Üye : _____
Daire Başkanı, Orhan KOCA

Üye : _____
Daire Başkanı, Nuray HATIRNAZ

Üye : _____
Bilişim Uzmanı, Osman ŞAHİN

Üye : _____
Bilişim Uzmanı, Dr. Savaş ÇITLAK

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Mobil Bulut Bilişimin Kişisel Veri Güvenliği Açısından İncelenmesi ve Elektronik Haberleşme Sektörü Açısından Değerlendirmeler
Türü	Bilişim Uzmanlığı Tezi
Yazar	Esra DURUOĞLU
Teslim Tarihi	23.01.2024
Anahtar Kelimeler	Bulut Bilişim, Mobil Bulut Bilişim, Mobil Bulut Bilişimin Kullanıldığı Sektörler, Mobil Bulut Bilişimde Kişisel Veri Güvenliği
Tez Danışmanı	Dr. Savaş ÇITLAK
Sayfa Adedi	viii+213

Özet

Dünya genelindeki akıllı cihaz sayısı, sunulan mobil uygulamalar, hız, kapsama ve hizmet kalitesinin artışı gibi etkenler mobil teknolojilere yönelik çalışmaları da tetiklemiş ve bu bağlamda ortaya çıkan mobil bulut bilişim kavramı tez kapsamında incelenmiştir. Bu doğrultuda, mobil bulut bilişim teknik açıdan ele alınmış ve kişisel veri güvenliğine yönelik çeşitli incelemeler yapılmıştır. Ayrıca mobil bulutun kullanıldığı başlıca sektörlere, örnek ülke uygulamalarına ve mobil bulut bilişimin ana bileşenleri olan bulut teknolojisi ile mobil bilgi işlemdeki kişisel veri güvenliğinin sağlanmasına yönelik yaklaşımlar açıklanmıştır. Son olarak mobil bulut bilişimi temel unsurları bulut teknolojisi ve mobil bilgi işlemin, veri güvenliğine yönelik tehditler ve alınabilecek önlemlere değinilmiştir. Tezin sonuç ve öneriler kısmında ise tüm bu incelemeler ışığında hem ülkemiz hem de Kurumumuza yönelik çeşitli önerilerde bulunulmuştur.

ABSTRACT

INFORMATION AND COMMUNICATION TECHNOLOGIES AUTHORITY	
Thesis	Investigation Of Mobile Cloud Computing in terms of Personal Data Security and Evaluations for The Electronic Communication Industry
Type	ICT Expert Thesis
Author	Esra DURUOĞLU
Submission Date	23.01.2024
Key Words	Cloud Computing, Mobile Cloud Computing, Sectors Using Mobile Cloud Computing, Personal Data Security in Mobile Cloud Computing
Advisor	Dr. Savaş ÇITLAK
Total Page	viii+213

Abstract

Factors such as the number of smart devices worldwide, mobile applications offered, speed, coverage and service quality have triggered studies on mobile technologies and the concept of mobile cloud computing, which emerged in this context, is examined in this thesis. In this context, mobile cloud computing is discussed from a technical perspective and various examinations on personal data security are made. In addition, the main sectors where mobile cloud is used, sample country applications and approaches to ensuring personal data security in cloud technology and mobile computing, which are the main components of mobile cloud computing, are explained. Finally, threats to the data security of cloud technology and mobile computing, which are the main components of mobile cloud computing, and the measures that can be taken are discussed. In the conclusion and recommendations part of the thesis, in the light of all these examinations, various suggestions have been made for both our country and our organization.

TEŞEKKÜR

Çalışma yaptığım süre boyunca bilgi ve tecrübeleri ile yardımlarını esirgemeden beni yönlendiren danışmanım Sayın Savaş ÇITLAK'a, yardımları ve süreç boyunca göstermiş olduğu anlayışı için Daire Başkanım Sayın Nuray HATIRNAZ'a, her zaman yanımda olarak bana güç veren ve sonsuz sevgileri ile daima en büyük desteğim olan kıymetli annem, babam ve biricik ablama, değerli çalışma arkadaşlarıma, içten dostluğu ile beraber beni hep cesaretlendiren sevgili arkadaşım Elif YILDIRIMLI AYDINLI'ya teşekkürlerimi sunarım.

TABLO LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

2N	İkinci Nesil Haberleşme Sistemleri
3N	Üçüncü Nesil Haberleşme Sistemleri
4N	Dördüncü Nesil Haberleşme Sistemleri
5N	Beşinci Nesil Haberleşme Sistemleri
AB	Avrupa Birliği (European Union)
ABD	Amerika Birleşik Devletleri
API	Uygulama Programlama Arayüzü (Application Programming Interface)
APT	Gelişmiş Sürekli Tehdit (Advanced Persistent Threat)
BM	Birleşmiş Milletler (United Nations)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CPU	Merkezi İşlem Birimi (Central Process Unit)
CSA	Bulut Güvenliği Birliği (Cloud Security Alliance)
DNS	Alan Adı Sistemi (Domain Name System)
DoS	Hizmet Dışı Bırakma Saldırısı (Denial of Service)
EHK	5809 sayılı Elektronik Haberleşme Kanunu
GDPR	Genel Veri Koruma Tüzüğü (General Data Protection Regulation)
GPS	Küresel Konumlandırma Sistemi (Global Positioning System)
HA	Uç Aracısı (Home Agent)
IaaS	Hizmet Olarak Altyapı (Infrastructure as a Service)
ISO	Uluslararası Standardizasyon Kurumu (International Standardisation Organization)

KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
LAN	Yerel Alan Ağı (Local Area Network)
MaaSB	Hizmet Aracısı Olarak Mobil Bulut Bilişim (Mobile as a Service Broker)
MaaSC	Hizmet Tüketicisi Olarak Mobil Bulut Bilişim (Mobile as a Service Consumer)
MaaSP	Hizmet Sağlayıcı Olarak Mobil Bulut Bilişim (Mobile as a Service Provider)
MAC	Medya Erişim Kontrolü (Media Access Control)
NaaS	Hizmet Olarak Ağ (Network as a Service)
NIST	Uluslararası Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)
OECD	Ekonomik İşbirliği ve Kalkınma Teşkilatı (Organisation for Economic Co-operation and Development)
PaaS	Hizmet Olarak Platform (Platform as a Service)
P2P	Eşler Arası (Peer-to-Peer)
QoS	Ağ iletişim Hizmet Kalitesi (Quality of Service)
RAN	Radyo Erişim Şebekesi (Radio Access Network)
SaaS	Hizmet Olarak Yazılım (Software as a Service)
SMS	Kısa Mesaj Servisi (Short Message Service)
SQL	Yapısal Sorgulama Dili (Structured Query Language)
TBMM	Türkiye Büyük Millet Meclisi
TCK	5237 sayılı Türk Ceza Kanunu
TCP	Geçiş Kontrol Protokolü (Transmission Control Protocol)

TSE	Türk Standartları Enstitüsü
USOM	Ulusal Siber Olaylara Müdahale Merkezi
VM	Sanal Makine (Virtual Machine)
WAN	Geniş Alan Ağı (Wide Area Network)
WLAN	Kablosuz Yerel Alan Şebekesi (Wireless Local Area Network)
WWAN	Kablosuz Geniş Alan Şebekesi (Wireless Wide Area Network)
XSS	Siteler Arası Komut Dosyası Çalıştırma (Cross-Site Scripting)

GİRİŞ

Dünya genelinde yaşanan teknolojik ilerleme ve gelişmelerle birlikte bilgi iletişim araçları da değişmiş ve çeşitlenmiştir. Bu bağlamda, bireylerin bilgiye her an her yerde erişme isteği mobil teknolojilere yönelik ilgiyi artırmış ve mobil teknolojilerde yaşanan gelişmeler neticesinde kişilerin kullanım alışkanlıklarını değiştirmiştir. Özellikle mobil internet hizmetlerinde yaşanan gelişmelerle birlikte akıllı mobil cihazların kullanım alanları da genişlemiş, kullanıcıların birçok işlemi mobil cihazları ile yapmayı tercih etmesi sonucu bağlantılı sektörlerdeki ürün ve hizmet yelpazesinin de giderek büyümesiyle bu alana ilişkin araştırmalar ivme kazanmıştır.

Her geçen gün eklenen özellikler ile daha da akıllı hale getirilmeye çalışılan mobil cihazlar, doğaları gereği sınırlı kaynaklara sahiptir. Bu sebeple, mobil güçlendirme çözümleri ile mobil cihazların bilgi işlem yeteneklerinin ve depolama kapasitesinin artırılarak, sınırlı kaynaklardan bağımsız olarak kullanıcılar için ölçeklenebilir, sürekli ve güvenli bilgisayar benzeri hizmetlerin sağlanması hedeflenmektedir. Aynı doğrultuda, mobil cihazların kaynak sınırlamalarının azaltılmasına yönelik olarak bulut bilişimi mobil bilgi işlemle birleştiren ve bulut bilgi işlemin avantajlarını mobil alana uygulanmasını hedefleyen mobil bulut bilişim (MCC) adlı yeni bir platform ortaya çıkmıştır. Bu yenilikçi teknoloji, mobil cihazların barındırdığı hesaplama, enerji ve depolama sınırlamalarını, bulut tabanlı platformlar tarafından desteklenen bir sistemle entegre ederek bulut tabanlı zengin mobil bilgi işlem ortamını inşa etmiş, akıllı mobil cihazların bilgi işlem ve depolama kapasitesi gibi özelliklerini cihaz modelinden ve sahip olduğu teknolojiden bağımsız bir şekilde geliştirerek arzu edilen yer ve zamanda yüksek veri hacmine sahip bilgilerin erişimine, depolanmasına, paylaşılmasına, sunulan yazılım ve hizmet servisleri ile karmaşık işlemlerin gerçekleştirilmesine imkan tanımıştır. Ayrıca, sunulan ‘teknolojiden bağımsız’ sınırsız veri depolama alanı ve bilgi işlem gücü ile zengin kullanıcı deneyiminin daha geniş kullanıcı yelpazesine ulaştırılmasını sağlamıştır.

Mobil bulut teknolojisi; mobil cihaz, kablosuz iletişim kanalı ve bulut teknolojisi olmak üzere üç ana bileşene sahiptir. Bulut bilişimin sunmuş olduğu büyük depolama

alanı ile bilgi işlem kapasitesinden yararlanıldığı bu teknolojide, mobil cihazlar üzerinden sunulan bulut tabanlı uygulamalar sayesinde kullanıcılar günlük hayatındaki birçok işlemi cihazları üzerinden gerçekleştirebilmekte, kullanıcıyı doğrudan veya dolaylı yoldan tanımlayabilecek veriler depolanıp, yedeklenebilmekte ve ihtiyaç halinde başkalarıyla paylaşılabilmektedir. Bu bağlamda, mobil bulut bilişim sistemleri, kullanıcısına birçok kolaylık ve avantaj sunmasına rağmen gizlilik ve kişisel verilerin korunması bakımından birtakım riskleri de beraberinde getirmektedir. Bu sebeple, bireylerin mahremiyetini sağlamak ve verilerini güvende tutabilmek için gerekli tedbirlerin alınması büyük önem taşımaktadır.

Mobil bulut bilişimin teknik açıdan ele alındığı ve kişisel veri güvenliğine yönelik çeşitli incelemelerin yapıldığı bu tez çalışmasında; mobil bulutun kullanıldığı başlıca sektörlere, örnek ülke uygulamalarına ve mobil bulut bilişimin ana bileşenleri olan bulut teknolojisi ile mobil bilgi işlemdeki kişisel veri güvenliğinin sağlanmasına yönelik yaklaşımlara odaklanılmıştır. Bu tez çalışmasındaki amaç; mobil bulut bilişime yönelik genel bir bakış açısı oluşturarak, teknik yönden değerlendirmek, mobil bulut bilişim konusunda çalışmalar gerçekleştiren bazı ülkelerin yaklaşımlarını incelemek, mobil bulut bilişimin sacayaklarından bulut teknolojisi ile mobil bilgi işlemi kişisel veri güvenliği bakımından ele almak ve elektronik haberleşme sektöründe kullanımına yönelik bir analiz gerçekleştirerek Bilgi Teknolojileri ve İletişim Kurumu için öneriler sunmaktır.

Tez dört bölümden oluşmakta olup, ilk bölümde bulut bilişim ve mobil bulut teknolojisi hakkında bilgi verilerek, mobil bulut bilişimin temel kavramları tanıtılacaktır. Mobil bulut bilişim ve bulut bilişim hakkında bilgilendirme yapılarak, mimarisi ile özelliklerine değinilecektir. Ayrıca her iki teknoloji de karşılaştırılacak ve mobil bulut teknolojisinin bazı olumsuzluklar ortaya çıkarabilecek özellikleri açıklanacaktır. Tezin ikinci bölümünde, mobil bulut bilişimin başlıca sektörler özelinde kullanım senaryoları tanıtılacak ve ülkelerdeki örnek uygulamalara yer verilecektir. Bu kapsamda Bağımsız Düzenleyiciler Grubu (Independent Regulators Group- IRG) üyesi ülkelere gönderilen sualname ve ülkemizde yer alan bazı bulut hizmet sağlayıcıları ile yapılan görüşmelerden edinilen bilgilerle mobil bulut bilişimin

kullanımına dair nitel bir araştırma yapılacaktır. Tezin üçüncü bölümünde, kişisel verilerin korunması çerçevesinde ulusal ve uluslararası düzenlemeler ele alınacak ve bulut bilişim kapsamında kişisel verilerin korunmasına yönelik çalışmalar belirtilecektir. Tezin son bölümünde ise mobil bulut bilişim kapsamında veri güvenliğine yönelik tehditler ve alınabilecek önlemler anlatılacaktır. Araştırma sonucunda elde edilecek bulgular değerlendirilerek elektronik haberleşme sektöründe mobil bulut bilişimin kullanımına, önemine ve kişisel veri güvenliğinin sağlanmasına yönelik bir sonuç elde edilecektir. Gerçekleştirilecek tüm bu incelemeler ve araştırmanın sonucunda birtakım öneriler sunulacaktır.

1. MOBİL BULUT BİLİŞİM

Kablosuz teknolojinin gelişmesiyle birlikte akıllı telefonlar ve saatler gibi mobil cihazlar günlük hayatta iletişim için en etkili araçlar haline gelmiştir. Bu cihazların yaygınlaşması ve donanım kapasitelerinin gelişmesiyle birlikte kullanıcıların bilgi işleme yönelik eğilimleri değişmiş; mobil cihazların basit bilgi işlem yerine daha karmaşık ve her yerde hızlı hizmet sunması beklenmiştir. İnternet üzerinden bilgi işleme, depolama, hizmetler ve uygulamalar sağlanırken, bulut teknolojisi sermaye maliyetini düşürmeyi kolaylaştırıp, hizmetleri temel teknolojiden ayırmış ve kaynak sağlama açısından esneklik sağlamıştır. Akıllı mobil cihazlarda görüntü işleme, video işleme, e-ticaret ve çevrim içi sosyal şebeke hizmetleri gibi çok çeşitli uygulamaların kullanılabilmesiyle beraber; bu aygıtlar zaman ve mekândan bağımsız en etkili ve kullanışlı iletişim aracı olarak insan yaşamının vazgeçilmez bir parçası haline gelmiştir (Prasad ve diğerleri, 2012).

Kullanıcılar, kablosuz şebekeler aracılığıyla cihazlarda veya uzak sunucularda çalışan mobil uygulamalardan zengin deneyimler elde etmekte, mobil şebeke ve taşınabilir terminallerin hızlı gelişimi ile akıllı telefonları giderek daha fazla tercih etmektedir. Günümüzde bu tür hizmetlere erişmek için mobil cihazları kullanmak bir alışkanlık haline gelmiştir.

Ancak mobil cihazların, bu isteği tam olarak karşılamak için işleme kapasitesi, depolama ve pil ömrü gibi yeterli kaynaklardan hala yoksun olması sebebiyle söz konusu isteği tam olarak karşılamak için tüketiciler, mobil cihazların bilgi işlem kapasitesi ve depolama açısından sağlayamadığı zengin kullanıcı deneyimini mobil uygulamalardan talep etmişlerdir. Ortaya çıkan mobil güçlendirme çözümlerinin ana hedefinin; mobil cihazların bilgi işlem yetenekleri ile depolamasının artırılması ve sınırlı kaynaklardan bağımsız olarak kullanıcılar için ölçeklenebilir, sürekli ve güvenli bilgisayar benzeri hizmetleri sağlanması olduğu belirtilmiştir.

Mobil cihazların kaynak sınırlamalarının azaltılmasına yönelik umut verici bir çözüm olarak da bulut bilişimi mobil bilgi işlemle birleştiren mobil bulut bilişim adlı yeni bir

araştırma alanı ortaya çıkmış ve bulut bilgi işlemin avantajlarının, mobil alana uygulanması hedeflenmiştir. Bu yenilikçi teknolojide, mobil cihazların hesaplama, enerji ile depolama sınırlamalarına bulut bilişim tarafından bir çözüm sunulmuştur. Bulut tabanlı zengin mobil bilgi işlem ortamının, bütünleşik görünüm, düşük ağırlık, çoklu bağlantı, yüksek kaliteli grafikler, artan bilgi işlem ve cihaz bağlama gibi özelliklere sahip akıllı telefon, tablet gibi taşınabilir mobil cihazlar çerçevesinde arzu edilen zaman ve yerde bilgi işlem isteğini gerçekleştirebileceği düşünülmüştür (Gu ve Guirguis, 2014).

Özetle, mobil cihaz, kablosuz iletişim kanalı ve bulut teknolojisi olmak üzere üç bileşene sahip olan mobil bulut teknolojisinde, aynı düzeyde kullanıcı deneyimi sağlayamayan, kaynakları kısıtlı mobil cihazların, kaynak korunması ile hizmetlere erişmesi kapsamında bulut bilişimin sunmuş olduğu büyük depolama alanı ve bilgi işlem kapasitesinden yararlanılmıştır.

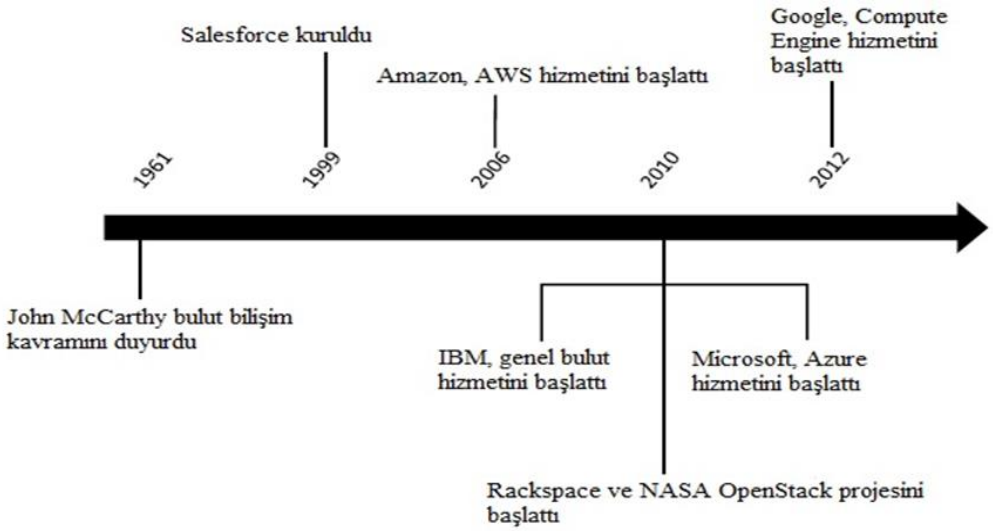
1.1 Bulut Bilişim Teknolojisi ve Gelişim Süreci

Bir ağ (tipik olarak internet) üzerinde veri depolayabilen ve ortak bilgi paylaşımına izin veren bir hizmet olan bulut bilişim (cloud computing) fikirsel açıdan 1961 yılında MIT Yüzüncü Yıl konferansında John McCarthy'in yaptığı bir konuşma ile ortaya konulmuştur (Küçüksille ve diğerleri, 2012). Bulut bilişimin kavramsal açıdan tanımını ise ilk olarak Ramnath Chellapa, 1997'de "bilgi işlemin sınırlarının sadece teknik sınırlamalar yerine ekonomik gerekçelerle belirlenebildiği yeni bilgi işlem paradigması" şeklinde yapmıştır (Dataversity, 2021). Bulut bilişimin teknolojisinin tarihçesine bakıldığında ise 1999 yılında bulut bilişim kavramı ile çalışan ilk şirketlerden biri olarak Salesforce kurulmuştur. Söz konusu şirket, kullanıcılarına müşteri ilişkileri yönetimi sağlayan Hizmet Olarak Yazılım (SaaS, Software as a Service) servisini sağlamaya başlamıştır. Ardından Amazon, 2006 yılında bulutta bilgi işlem ve depolama gibi hizmetler sağlayan Elastic Compute Cloud (EC2), Hizmet Olarak Altyapı (IaaS, Infrastructure as a Service) modelini sunmuş ve aynı yıl Google ise Google Dokümanlar hizmetlerini başlatmıştır.

Amerika Birleşik Devletleri'nde yer alan üniversitelerin çoğu 2007'de Google ve IBM ile iş birliği yapmış ve üniversitelerdeki bulut bilişim programlarını desteklemiştir. Bulut bilişim, akademik araştırma maliyetinin düşürülmesi, kaynakların öğrenciler arasında paylaşılması ve internet üzerinden erişebilmesi için önemli bir bilgi işlem gücü haline gelmiştir.

Temmuz 2010'da NASA ve Rackspace aralarında AMD, Intel ve Dell'in de bulunduğu çeşitli satış firmalarıyla OpenStack adlı ortak bir proje başlatmış, OpenStack'i tanıtmak için de Eylül 2012'de OpenStack Vakfı isimli kâr amacı gütmeyen bir kuruluş kurulmuştur. Ekim 2011'de, Cloud Security Alliance (CSA) tarafından geliştirilen Güvenilir Bulut Girişimi, bulut hizmeti sağlayıcılarının endüstri standartları gereksinimlerini karşılayan, güvenli, erişimi kontrol edilebilir, birlikte çalışabilir ve yönetilebilir bulut hizmetleri geliştirmelerine yardımcı olmak için bir tanıtım yazısı yayımlamıştır (Surbiryala ve diğerleri, 2019). Aşağıda yer alan Şekil 1.1'de bulut bilişimin tarihçesi verilmektedir.

Şekil 1.1 Bulut Bilişim Tarihçesi



Kaynak: Surbiryala ve diğerleri, 2019

Amerika Ulusal Standartlar ve Teknoloji Enstitüsü (NIST, National Institute of Standards and Technology); bulut bilişim kavramını, minimum yönetim çabası veya hizmet sağlayıcısı etkileşimi gerektiren, hızlı bir şekilde sağlanabilen ve kullanıcıların inisiyatifine bırakılabilen, aynı zamanda yapılandırılabilir bilgi işlem kaynaklarının (örneğin ağlar, sunucular, depolama, uygulamalar ve hizmetler) paylaşıldığı bir havuza dayalı bir model olarak tanımlamıştır (Surbiryala ve diğerleri, 2019). Bu model, herhangi bir yerden, uygun ve isteğe bağlı ağ erişimi ile erişilebilen bir yapı sunmaktadır.

Tanımlanan bulut modeli, beş temel özellikten, üç hizmet ve dağıtım modelinden oluşmaktadır. Basit bir ifadeyle bulut bilişim, bilgisayarımızın sabit diski yerine internet üzerinden veri ve programların depolanması ve bunlara erişilmesi şeklinde tanımlanabilmektedir (Rashid ve Chaturvedi, 2019).

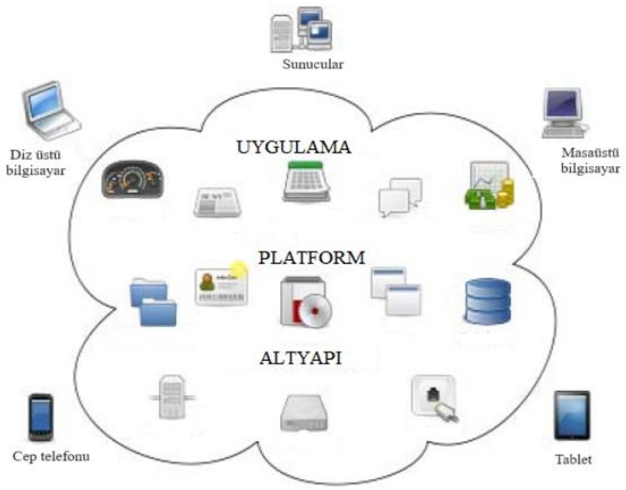
Bulut bilişim teknolojisinin temeli olarak ifade edilebilecek birkaç özelliği bulunmaktadır. Bunlar, esneklik, isteğe bağlı kendi kendine (self) servis, paylaşılan kaynak havuzu, geniş ağ erişimi ve çoklu kiracılıktır (Perez ve Kumar, 2017).

Bulut bilişimin temel özelliklerinden biri olan isteğe bağlı self servis, kullanıcılara bulut bilişim kaynaklarını hizmet sağlayıcı veya insan etkileşimi olmaksızın kendi başlarına kullanma yeteneği sunmaktadır. Diğer bir deyişle, kullanıcılar, herhangi bir insan etkileşimi gerektirmeden bulut bilişim kaynaklarını kullanabilir ve bilgi işlem yeteneklerini kendi ihtiyaçlarına göre kontrol edebilirler. (GlassHouse, 2021).

Esneklik, bulut bilişimde hızlı bir şekilde kaynakların artırılması veya azaltılmasına olanak tanıyarak kullanıcının her zaman sınırsız kaynağa erişim sağlama düşüncesini güçlendirmeyi amaçlamaktadır. Bu özellik sayesinde, kullanıcılar ihtiyaçlarına göre kaynakları kolayca ölçeklendirebilirler. Aynı zamanda, çoklu kiracılık, farklı işletmelerin aynı altyapıyı paylaşmasını mümkün kılmaktadır. Yani, bulut bilişim altyapısı üzerinde birden çok kiracı bulunabilmekte ve bu şekilde kaynaklar daha verimli bir şekilde paylaşılabilmektedir.

Geniş ağ erişimi ise bulut bilişimin diğer önemli bir özelliğidir. Bulut hizmetlerine, ideal olarak yüksek geniş bant bağlantısı gibi bir ağ üzerinden, internet gibi geniş bir alanda veya özel bulutlarda yerel alan ağı (LAN, Local Area Network) üzerinden erişilebilmektedir. Bu geniş ağ erişimi, kullanıcılara her yerden, uygun bir şekilde ve isteğe bağlı ağ erişimi ile bulut hizmetlerine erişim sağlama imkânı tanımaktadır (Perez ve Kumar, 2017). Şekil 1.2'de bulut bilişimin genel yapısı verilmektedir.

Şekil 1.2 Bulut Bilişimin Genel Yapısı



Kaynak: Perez ve Kumar, 2017

1.1.1 Bulut Bilişim Mimarisi

Bulut bilişim, her katmanın önemli bir bölümünü temsil ettiği üç seviyeye bölünmüştür.

- Uygulama katmanı; web arayüzlerini, programlama arayüzlerini, uygulama çekirdeği olarak bilinen bulut uygulamalarını, ana motorlar gibi istemciler tarafından kullanılan verileri ve çeşitli uygulamaları içermektedir.

- Sanallaştırma katmanında, uygulamalara gerekli kaynaklar ve talepler sağlanarak yedeklenmektedir. Veritabanı erişimi ve sunucu işlevselliğinin yanı sıra İnternet Protokolü ve Alan Adı Sistemi (DNS, Domain Name System) gibi

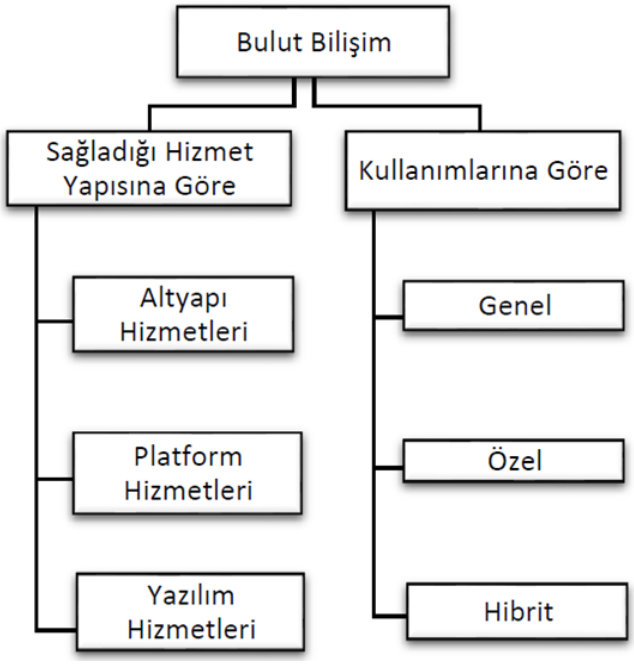
bağlantı bileşenleri de bu katmanda bulunmaktadır. Ayrıca burada, sanal makinelerle ilgili her şeyin tanımlandığı ve kontrol edildiği fiziksel altyapının sanallaştırılması da sağlanmaktadır.

- Fiziksel katman, yukarıdaki iki katmanın gerekli görevleri yerine getirmesi için kullanılan donanım ve kaynaklardır. Donanım, bireysel sunucuları, anahtarlayıcıları ve yönlendiricileri içermektedir. Ayrıca donanımı barındıran tesisler de fiziksel bileşenlerin düzgün çalışmasını sağlayan güç sistemleri ile birlikte bu katmanın bir parçasıdır (Perez ve Kumar, 2017).

1.1.2 Bulut Bilişim Hizmet ve Dağıtım Modelleri

Bulut bilişimin sınıflandırma şeması Şekil 1.3'te verilmiştir.

Şekil 1.3 Bulut Bilişim Sınıflandırılma Şeması



Kaynak: Paşaoğlu ve Cevheroğlu, 2020

1.1.2.1 Bulut Bilişim Hizmet Modelleri

Bulut bilişimin önemli özelliklerinden biri olarak kaynakların veya yeteneklerin bir hizmet olarak sunulması bulunmaktadır. Bu kapsamda, bulut bilişim tanımlamak için kullanılan üç hizmet modeli bulunmaktadır. Bunlar, Hizmet Olarak Yazılım, Hizmet Olarak Platform ve Hizmet Olarak Altyapı şeklinde ifade edilmektedir.

a) Hizmet Olarak Altyapı (IaaS)

Hizmet Olarak Altyapı'da kullanıcı, bulut hizmeti sağlayıcısının gerçek altyapısına erişebilmekte ve söz konusu altyapı üzerinde uygulamalar oluşturmak için geliştirme araçlarını kullanarak, sanal donanımdan yararlanabilmektedir. İstemci, sistem yöneticileri ve geliştiriciler de dâhil olmak üzere üst düzey bilgi teknoloji personelini içermektedir. IaaS sağlayıcıları, ham donanım altyapısı satmak yerine genellikle hizmet olarak sanallaştırılmış altyapı sunmaktadır. Hizmet olarak altyapının avantajları arasında, altyapının talep üzerine esneyebilmesi ve çok sayıda kullanıcının tek bir donanım kullanmasından dolayı maliyetlerin düşürülmesi yer almaktadır. IaaS, bu avantajları sağlamak için çeşitli hizmetler sunmaktadır. Örneğin, Amazon Web Services (AWS) içinde bulunan Elastic Compute Cloud (EC2) ve Simple Storage Service (S3) gibi hizmetler bu kapsamda değerlendirilebilmektedir (Perez ve Kumar, 2017).

b) Hizmet Olarak Platform (PaaS)

Hizmet Olarak Platform (PaaS, Platform as a Service), kullanıcıların kendi uygulamalarını oluşturup buluta dağıtabilecekleri modelin tersi şeklinde tanımlanmaktadır. Bu uygulamalar, programlama ile yapılandırma araçları yardımıyla geliştirilmekte ve çoğunlukla geliştiriciler, test ediciler veya yöneticiler tarafından kullanılmaktadır. Bu platform, kullanıcıların uygun ortamı yerel olarak oluşturmasına gerek kalmadan uygulama geliştirmelerine olanak tanımaktadır. Geliştiriciler, temeldeki donanım altyapısı hakkında endişelenmeye gerek duymadan uygulamalarını

belirli bir platformun özelliklerine göre yazabilmektedirler. PaaS'ın barındırdığı faydalara, geliştiricilerin gereksinimleri karşılamak için talep üzerine yeni platformlar oluşturmalarına olanak tanıyan artırılmış esnekliği ve verilerin yedeklenmesi ile kurtarılmasını içeren güvenlik avantajları verilmektedir. Uygulamaların Google'ın altyapısında çalıştırılmasına izin veren Google App Engine ve Salesforce'un Force platformu örnek olarak verilmektedir (Perez ve Kumar, 2017).

c) Hizmet Olarak Yazılım (SaaS)

Hizmet Olarak Yazılım'da kullanıcıların uygulamayı kendi bilgisayarlarına yüklemelerine gerek kalmadan bulut uygulamalarına erişmelerine olanak tanınmaktadır. Hizmet sağlayıcı, bulut bilgi işlem altyapısının bakımını yaparken, kullanıcının ise uygulama kontrol ayarları üzerinde yetkisi bulunmaktadır.

Söz konusu modelin avantajları arasında yazılım lisanslama maliyetlerinin düşürülmesi, güvenlik ve birden çok istemcinin aynı uygulamayı aynı anda kullanmasına izin verilmesi yer almaktadır. Bu avantajlar, Yazılım olarak Hizmet (SaaS) modelini etkili kılan unsurlardır. SaaS, bulut bilişimin son kullanıcıları için en görünür katman olarak öne çıkmakta ve erişilen ve kullanılan yazılım uygulamalarıyla ilgili bir hizmet sunmaktadır. Salesforce, Google Mail, Google Belgeler ve e-Tablolar gibi Google Uygulamaları, kullanıcılara çeşitli iş ihtiyaçları için hızlı ve erişilebilir yazılım çözümleri sunan örnek SaaS hizmetlerdir. (Perez ve Kumar, 2017).

Aşağıda yer alan Tablo 1.1'de bulut bilişim hizmet modellerinin avantajları ve dezavantajları karşılaştırmalı olarak verilmektedir.

Tablo 1.1 Bulut Bilişim Hizmet Modellerinin Avantajları ve Dezavantajları

Bulut Bilişim Hizmet Modeli	Avantajları	Dezavantajları
IaaS	• Kullanım başına ödeme • Toplam maliyetin azalması • Elastik kaynaklar • Daha iyi kaynak kullanımı • Yeşil bilgi ve iletişim teknolojilerinin desteklenmesi	• Güvenlik sorunları • Birlikte çalışabilirlik sorunları • Performans sorunları
PaaS	• Hızlı geliştirme ve dağıtım • Toplam maliyetinin azalması • Çevik yazılımların desteklenmesi • Birlikte çalışabilirlik • Kullanım kolaylığı • Daha az bakım masrafı • Ölçeklenebilir uygulamaların oluşturulması	• Satıcı kilitleme sorunu • Güvenlik sorunları • Daha az esneklik • İnternet bağlantısına bağımlılık
SaaS	• İstemci tarafında kurulumun olmaması • Toplam maliyetin azalması • Daha az bakım gerektirmesi • Erişim kolaylığı • Dinamik ölçeklendirme • Felaket kurtarması (disaster recovery) • Çoklu Kiracılık	• Güvenlik sorunları • Bağlantı gereksinimleri • Kontrol kaybı

Kaynak: Shamshirband ve diğerleri, 2020.

1.1.2.2 Bulut Bilişim Dağıtım Modelleri

Bulut bilişim sistemleri dağıtım modelleri, kullanım şekline göre üç sınıfa ayrılmış olup; bu modeller, Genel Bulut, Özel Bulut ve Hibrit Bulut olarak adlandırılmıştır.

a) Genel Bulut (Public Cloud):

Google ve Amazon gibi üçüncü şahıslar tarafından çalıştırılarak, hizmetlerini internet aracılığıyla şirketlere ve tüketicilere sunan genel bulutta, kullanıcı sınırlaması bulunmamaktadır. Bünyesinde bulunan hizmetler sanallaştırılmış bir ortamda toplanmakta ve bu hizmetlere internet üzerinden erişilebilmektedir. Genel bulut servislerine Hizmet Olarak Yazılım, Hizmet Olarak Altyapı ve Hizmet Olarak Platform örnek olarak gösterilmektedir. Kullanıcı sadece paylaştırılmış kaynaklar üzerinde kendi alanını kullanabilirken, bulut sağlayıcısı veri merkezlerini çok farklı yerlere kurabilmektedir. Bu yüzden kullanıcılar verilerinin fiziksel olarak nerede tutulduğunu bilmemekte dolayısıyla, kendi özel bulutlarına sahip olma eğiliminde olmaktadırlar (Paşaoğlu ve Cevheroğlu, 2020).

b) Özel Bulut (Private Cloud)

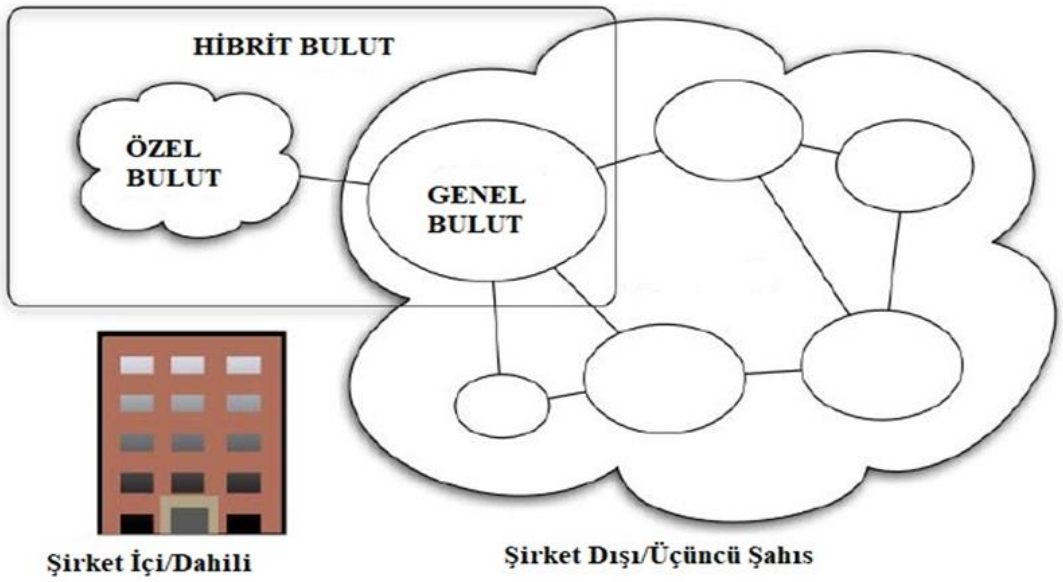
Özel bulutta, altyapı üzerinde çalışan uygulamalar ve bu uygulamaların çalıştırıldığı yerler, onu kullanan kişi veya kuruluşlara, yani altyapının her yönü üzerinde tam kontrole sahip olan tek bir şirkete aittir. Başka bir ifadeyle, belirli bir kurum veya organizasyon için oluşturulan bu bulutta, hizmet sağlayıcı ya kuruluşun kendi altyapısını yönetmekte ya da hizmeti üçüncü bir bulut hizmet sağlayıcısından temin etmektedir. Özel bulut, kurumun mevcut altyapısını sanallaştırma esasına dayanmaktadır. Bu sayede, altyapı üzerinde tam kontrol sağlanmakta ve sanallaştırmanın sunduğu tüm avantajlar elde edilmiş olmaktadır (Patidar ve diğerleri, 2012).

c) Hibrit Bulut (Hybrid Cloud)

Hibrit bulut, özel ile genel bulutun bir kombinasyonundan oluşan ve iş yüklerinin, birbirine bağlı iki ortam arasında hareket ettiği bir bulut türüdür (Bulutistan, 2021). En temel avantajı, önemli veriler özel bulutta tutulurken, daha az kritik veriler genel bulutta tutulabilmektedir. Hibrit bulutta, özel ve genel bulutlar bir arada kullanıldığında yönetim sorumluluğu iki bulut sağlayıcı arasında bölünmekte, bu durum sonucunda güven veya karşılıklı çakışma sorunları oluşabilmektedir. Ayrıca, bu teknolojide senkronizasyon ve verilerin güvenliği gibi konulara da dikkat edilmesi gerekmektedir (Paşaoğlu ve Cevheroğlu, 2020).

Şekil 1.4'te bulut bilişim dağıtım modelleri verilmektedir.

Şekil 1.4 Bulut Bilişim Dağıtım Modelleri



Kaynak: Patidar ve diğerleri, 2012

1.2 Mobil Bulut Bilişim Teknolojisi

Mobil cihazlar; yetenekleri, işlem güçleri, depolama, özellik desteği ve uygulamalar açısından çok hızlı bir şekilde gelişmektedir. Ancak mobil cihazlar, bant genişliği,

bilgi işlem gücü ve enerji bakımından sınırlı kaynaklardır. Bununla birlikte, teknolojik yeniliklerin hızla gelişmesi, bu aygıtları işlem hızı ve depolama açısından giderek daha yetenekli hale getirmekte ve 4N, 5N gibi mobil teknolojiler sahayı şekillendirerek, daha düşük gecikme süresi ile daha yüksek hız sunmaktadır.

Günümüzde kullanılan mobil uygulamalar; kimlik doğrulama, konuma duyarlı işlevler ve son kullanıcılar için hedeflenen içerikler ile iletişimin sağlanması gibi görevleri ifa ederken, veri depolama kapasitesi, bellek ve işlem gücü gibi kapsamlı hesaplama kaynaklarına ihtiyaç duymaktadır. Bu aşamada bulut bilişim, mobil cihazlara kolayca yararlanabileceği bol miktarda bilgi işlem gücü sunmaktadır. Kaynak kısıtlamalı mobil cihazlara sunulan kablosuz altyapı ve bulut teknolojisi, yeni bir bilgi işlem kavramı için zemin hazırlamış ve mobil bulut bilişim ortaya çıkmıştır (Ahmed ve diğerleri, 2015).

Mobil bulut bilişim hem veri işlemenin hem de veri depolamanın mobil ortam dışında gerçekleştirildiği sistemler olarak ifade edilmektedir. Hesaplamalar ve veri depolamanın doğrudan mobil cihazda yapılması yerine bulutta yürütülmesiyle uygulamalar daha geniş bir kapsama sahip olmaktadır (Perez ve Kumar, 2017). Mobil ve kablosuz şebeke erişim teknolojilerinin ortaya çıkmasıyla birlikte, giderek popülerleşen mobil bulut bilgi işlem sayesinde mobil cihazlar, buluta bağlanarak kablosuz ağ üzerinden her zaman ve her yerde erişim sunmaktadır (Şekil 1.5).

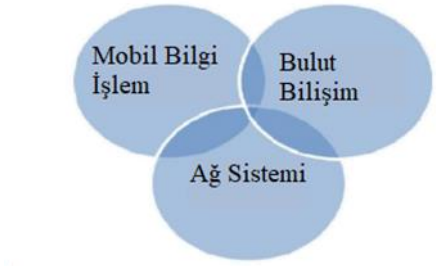
Mobil bulut bilişim, mobil uygulamalar için yeni bir paradigma olmakla birlikte; uygulamalarla ilişkili işleme ve veri depolamanın çoğu, mobil cihazdan bulutta yer alan güçlü, merkezi bilgi işlem platformlarına taşınmaktadır. Bu merkezileştirilmiş uygulamalara daha sonra cihazdaki ince yerel istemci veya web tarayıcısı kullanılarak internet üzerinden erişilmektedir.

Mobil bulut bilişim, bulut teknolojisinin ilkeleri üzerine kuruludur. Bu teknoloji, mobil alana isteğe bağlı erişim ve Hizmet Olarak Ağ'ı (NaaS, Network as a Service) ekleyerek; isteğe bağlı kapasitelerde sunulan hizmet ile uygulamaların, uzman

uygulama sunucularına ihtiyaç duymadan, mobil şebekenin sunduğu tüm olanaklardan faydanılmasını sağlamaktadır (Prasad ve diğerleri, 2012).

Geleneksel mobil bilgi işlem teknolojilerinden farklı olarak, mobil bulut bilişimdeki kaynaklar sanallaştırılmakta ve yerel bilgisayarlar veya sunucular yerine çok sayıda dağıtılmış bilgisayar grubuna atanmaktadır. Bu kapsamda, günümüzde bulut bilişim tabanlı birçok uygulama geliştirilerek kullanıcıların hizmetine sunulmaktadır.

Şekil 1.5 Mobil Bulut Bilişim Kapsamı



1.2.1 Mobil Bulut Bilişim Literatür Taraması

Literatürde mobil bulut bilişime yönelik birçok tanım bulunmaktadır. Bu tanımlardan bazıları şunlardır;

- Bahl ve arkadaşları mobil bulut bilişimi, mobil bulut uygulama üzerinden şu şekilde tanımlamıştır; genel buluttan (örneğin Amazon EC2 ve Windows Azure) yararlanan mobil uygulamalara, mobil bulut uygulamaları ya da kısaca mCloud uygulamaları denilmektedir. Diğer bir deyişle, mobil uygulamaları sorunsuz bir şekilde destekleyen genel bulut teknolojisi mCloud olarak adlandırılmaktadır (Bahl ve diğerleri, 2012).

- Dai ve arkadaşları, mobil bulut bilgi işlemi; tüketici, kuruluş, Femtocell'ler, kod çevrimi, uçtan uca güvenlik, ağ geçitleri ve mobil genişbant özellikli hizmetler de dâhil olmak üzere birçok unsuru içeren bir mobil ekosistemde,

bulut bilgi işlem hizmetlerinin kullanılabilirliği şeklinde tanımlanmıştır. Araştırmacılar mobil bulut bilişimi mobil bilgi işlem, mobil internet ve bulut bilişimin birleşimi olarak görmüşlerdir (Dai ve diğerleri, 2012).

- Lin ve arkadaşlarının yapmış olduğu tanıma göre, mobil bulut bilişim, bulut bilgi işlemi, mobil cihazlar ve her yerde bulunan kablosuz altyapı ile birleştiren yeni bir bilgi işlem paradigmasıdır (Lin ve diğerleri, 2014).

- Mobile Cloud Computing Forum, mobil bulut bilişimi en basit haliyle hem veri depolamanın hem de veri işlemenin mobil cihazın dışında gerçekleştiği altyapı şeklinde tanımlamıştır (Gayathri ve Srinivas, 2014).

- Sanaei ve arkadaşlarına göre, mobil bulut bilişim, internet üzerinden her yerde ve her zaman çok sayıda mobil cihaza hizmet sunma amacıyla çeşitli bulut hizmetlerini ve şebeke teknolojilerini birleştiren, kullanıcıların sadece kullandıkları kadar ödeme yapmalarına dayalı bir ilkeyi benimseyen bir teknolojidir. Bu yaklaşım, işlevsellik, depolama ve mobilite gibi çeşitli alanlarda elastik kaynakları etkili bir şekilde kullanarak zengin bir mobil bilişim deneyimi sağlamaktadır (Sanaei ve diğerleri, 2014).

- Mollah ve arkadaşları, mobil bulut bilgi işlemi, cep telefonu ortamında veya mobil gömülü sistem ortamında sunulan bulut bilişim hizmetleri olarak tanımlamıştır. Ayrıca esneklik, isteğe bağlı self servis, paylaşılan kaynak havuzu, geniş ağ erişimi ve çoklu kiracılık gibi bulut teknolojisinin temel özellikleri ile mobil bilgi işlemin bütünleştiğini belirtmişlerdir (Mollah ve diğerleri, 2017).

- Zhou ve Buyya, kaynak kısıtlaması olan mobil cihazların performansını artırmak için bulut bilgi işlem kaynaklarından yararlanan bilgi işlem türünü mobil bulut bilgi işlem şeklinde adlandırmışlardır (Zhou ve Buyya, 2018).

- Karthik ve Manhar, mobil bulut bilişimi mobil istemcilere yönelik bulut altyapıları, platformları ve hizmet uygulamalarının geliştirilmesi için mobil bilgi işlem, şebeke ve bulut bilişimden yararlananılan bir paradigma şeklinde tanımlamıştır. Mobil bulut bilişimin temel hedefi kullanıcılara ölçeklenebilir mobil bulut kaynaklarına dayanan, hareket kabiliyetine sahip ve konum bilgisine duyarlı mobil hizmetleri, şebekelerde, bilgisayarlarda, depolarda ve mobil cihazlarda sunmaktır (Karthik ve Manhar, 2020).

- NIST, mobil bulut bilgi işlemi hem veri depolamanın hem de veri işlemenin mobil cihazın dışında gerçekleştiği bir altyapı olarak tanımlamıştır. Ayrıca mobil bulut uygulamaların, bilgi işlem gücünü ve veri depolamayı cep telefonlarından buluta taşıyarak, uygulamaları ve mobil bilgi işlemi yalnızca akıllı telefon kullanıcılarına değil, çok daha büyük bir mobil abone yelpazesine genişlettiği de ifade edilmiştir (Fellah ve diğerleri, 2020).

Genel olarak bakıldığında, mobil bulut bilişim, akıllı telefon ve tablet gibi mobil cihazlar üzerinden sunulan bulut bilişim hizmetleri olarak tanımlanabilmektedir. Mobil bulut bilişimde, kullanıcılar bulutta depolanan kaynaklara, uygulamalara ve verilere erişebilmekte; bulut bilgi işlem yoluyla çeşitli hizmetleri dağıtabilmektedir. Bu durum mobil cihazların bilgi işlem gücünün, depolama kapasitesinin ve bağlamsal farkındalığının artırmasını sağlamaktadır.

Mobil bulut bilişim, kullanıcılarına, şebeke işletmecilerine ve bulut bilişim sağlayıcılarına zengin bilgi işlem kaynakları sunmak için bulut bilişim, mobil bilgi işlem ve kablosuz şebekeleri birleştiren bir platformdur. Bu yenilikçi teknolojinin nihai hedefi, uygulamaların mobil cihaz üzerinde zengin bir kullanıcı deneyimiyle yürütülmesini sağlamaktır. Mobil bulut bilişim, bulut uygulamalarını, bilgi işlem gücünü ve veri depolamayı mobil cihazlardan uzağa, ince yerel istemciye dayalı kablosuz bağlantı üzerinden erişilebilen bulutlarda yer alan merkezi ve güçlü bilgi işlem platformlarına taşınması mantığı ile çalışmaktadır (Hiremath ve Mallapur, 2015).

Mobil bulut bilişim tanımları genel olarak üç farklı kavram çerçevesinde ele alınarak yapılmıştır. Bu kavramlar şu şekildedir;

- Mobil cihaz bir ince istemci gibi davranmakta ve bulut sunucusu ağır ve yoğun kaynak gerektiren işlemleri yapmaktadır (örneğin Gmail mobil uygulaması). Mobil ince istemcinin daha az kaynak talebi, bir bulut platformuyla birleştiğinde oldukça iyi genel performans elde edilen, nispeten az güçlü mobil cihazlar oluşturmasını sağlamaktadır. Böylece mobil istemciler, yalnızca kullanıcı etkileşimini yönetmekte ve uygulama çalışmaları ile verileri buluta boşaltmaktadır.

- Yerel bir bulut ağındaki her mobil cihaz, ağ içindeki diğer mobil cihazlara hizmet vermekte ve bu cihazlar tarafından sunulan eşler arası bir model altında hareket etmektedir. (Örnek olarak bir çeviri uygulaması çalıştıran bir cep telefonu verilebilir, diğer eşler kaynak sağlayıcı olarak hareket etmektedir.)

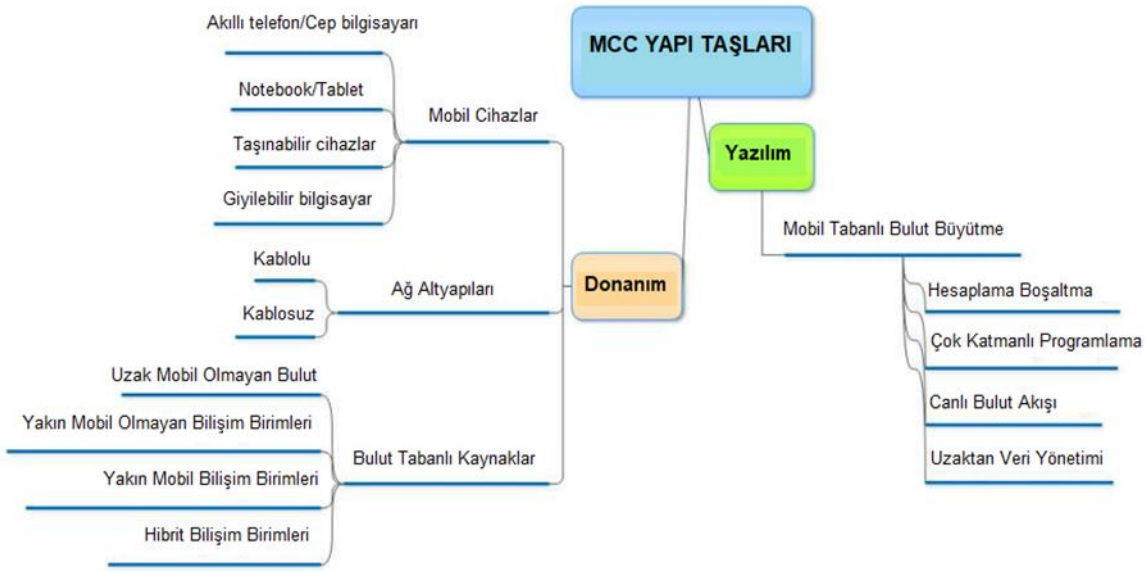
- Cloudlet kavramı ile mobil cihaz, iş yükünü buluta bağlı birden çok sunucudan oluşan yerel bir bulut uygulamasına aktarmakta veya taşımaktadır. Cloudlet, mobil cihaz ile bulut arasında bir aracı görevi görmektedir. Böylece cep telefonunun ağa bağımlılığından kaynaklanabilecek bant genişliği veya gecikme sorunlarının üstesinden gelinmesi hedeflenmektedir (Fernando ve diğerleri, 2012).

Bulut bilişim üzerinden bilgi işlem yapılması ve verilerin boşatılması, mobil bilgi işlemin barındırdığı zorlukların üstesinden gelmek için kullanılmaktadır. Kullanıcılara mobilite ve kullanım kolaylığı sunan mobil bulut bilişim, bulut bilişimin bir alt kümesi olarak ortaya çıkmıştır. Mobil bulut bilişimi, genel olarak mobil ortamlarda kullanılan bulut bilgi işlem hizmetlerini ifade etmektedir. Bu kavram, bulut bilgi işlem ve mobil ağ özelliklerini birleştirerek mobil kullanıcılara en uygun hizmetleri sunar. Mobil bulut bilişim ortamında, mobil cihazın yüksek bellek kapasitesi veya yüksek CPU hızına ihtiyaç duyulmadan, tüm veriler ve karmaşık bilgi işlem modülleri bulut hizmetleri üzerinde yürütülebilmektedir (Alizadeh ve diğerleri, 2013).

1.2.2 Mobil Bulut Bilişimin Temel Unsurları

Mobil bulut bilişimi oluşturan ana yapı taşları ise donanım ve yazılım olmak üzere iki açıdan incelenmektedir. Mobil bulut bilişimde donanım yapı taşı ile çeşitli yazılım programları tarafından kullanılabilen zengin bir mobil hesaplama platformu sağlanmaktadır. Aşağıda yer alan Şekil 1.6'da mobil bulut bilişimi oluşturan yapı taşlarının genel sınıflandırılması verilmiştir (Abolfazli ve diğerleri, 2015).

Şekil 1.6 Mobil Bulut Bilişim Yapı Taşlarının Sınıflandırılması



Kaynak: Abolfazli ve diğerleri, 2015

a) Donanım

Heterojen kaynak kısıtlamalı mobil cihazlar, bulut tabanlı kaynaklar ve ağ altyapıları da dâhil olmak üzere donanım altyapıları, mobil bulut bilişimin somut yapı taşlarını oluşturmaktadır. Bu minvalde heterojenlik, mobil ve bulut bilgi işlem teknolojilerinden gelmektedir. Mobil bulut bilişim çok sayıda farklı cihaz, altyapı, teknoloji ve özelliğin etrafında yoğunlaşmaktadır.

- **Mobil Cihazlar**: Mobil bulut bilişim, çeşitli sınırlı bilgi işlem yeteneklerine sahip, batarya ile çalışan, kablosuz olarak bağlanabilen çok sayıda heterojen mobil cihazla (akıllı telefon, tablet veya giyilebilir bilgisayar gibi) kullanılmaktadır.

- **Bulut Tabanlı Kaynaklar:** Mobil bulut bilişimde, bulut bilgi işlem teknolojileri ve ilkelerine dayalı olarak oluşturulan bulut tabanlı kaynaklar kullanılmaktadır. Bu kapsamda, uzak mobil olmayan bulutlar, yakın mobil olmayan bilişim birimleri, yakın mobil bilişim birimleri ve hibrit olmak üzere dört tür bulut tabanlı kaynak tanımlanmıştır.

- **Ağ Altyapıları:** Mobil bulut bilişimde verimli, güvenilir ve yüksek performanslı ağ iletişimi hem kablolu hem de kablosuz ağ teknolojileri ile altyapılarının dağıtımını gerektirmektedir. Mobil cihazlar yalnızca kablosuz iletişim gerçekleştirse de sabit bulut tabanlı kaynakların kullanımında, dijital içeriklerin güvenilir ve yüksek hızlı bir ortamda farklı bilgi işlem aygıtlarına iletilmesi için kablolu iletişim gerekmektedir (Abolfazli ve diğerleri, 2015).

b) Yazılım

Mobil bulut bilişimin yazılım yapı taşı, mobil cihazların eksikliklerini azaltmak için bulut tabanlı kaynaklardan verimli bir şekilde yararlanmaya yönelik büyütme protokollerini ve çözümlerini içermektedir. Bulut tabanlı mobil büyütme; kaynak açısından zengin bulut tabanlı kaynaklarda, yoğun kaynak kullanan mobil uygulama bileşenlerini yürüterek mobil cihazların bilgi işlem yeteneklerini artırmak, geliştirmek ve optimize etmek için bulut bilgi işlem teknolojilerinden ve ilkelerinden yararlanan son teknoloji mobil büyütme modelidir.

Başlıca bulut tabanlı mobil büyütme yaklaşımları, hesaplama-boşaltma, canlı bulut akışı, çok katmanlı programlama ve uzaktan veri yönetiminden oluşmaktadır (Abolfazli ve diğerleri, 2015).

Hesaplama-boşaltma, mobil uygulamaların yoğun kaynak kullanan bileşenlerini belirleme, bölümleme ve bulut tabanlı kaynaklara geçirme işlemidir. Yoğun bileşenlerin belirlenmesi ile bölümleme; statik, dinamik ve hibrit olmak üzere üç farklı yaklaşımda gerçekleşebilmektedir. Statik bölümleme, tasarım ve geliştirme sırasında mobil uygulamanın yoğun bileşenlerini tanımlama ve bölümleme için bir defalık bir işlem olmakla birlikte, bir mobil cihaza çalışma zamanı yükü getirmemektedir. Ayrıca uygulama bölümlendikten sonra, aynı bölümler yürütme için tekrar kullanılabilmektedir. Bununla birlikte, statik bölümleme ortam değişikliklerine ve dinamizmine uyarlanamamaktadır. Dinamik bölümleme ise mobil bulut bilişim ortamının dinamizmini daha iyi karşılamak adına çalışma zamanında gerçekleşmektedir. Ancak dinamik bölümlemede, yoğun görevleri belirleme, ortamı izleme, uygulamayı bölümleme ve boşaltma gibi bileşenler aşırı yük getirmektedir. Bu yüzden, bölümleme ek yükünü azaltmak ve çevresel değişikliklere uyum sağlamak için uygulamanın bir kısmının tasarım zamanında ve bir kısmının ise çalışma zamanında bölümlendiği hibrit bir modelin kullanılması önerilmektedir.

Çok katmanlı programlama, uzakta kaynak yoğun hesaplamalar (genellikle web hizmetleri) gerçekleştirerek, gevşek bağlı uygulamalar oluşturan kod bölümleme ve boşaltma ek yükünü azaltmak için önerilmiştir. Kaynak yoğun hesaplamalar, yürütme için çağrılacak uzak sunucularda her zaman mevcut olduğundan, mobil cihazdan uzak kaynaklara görevleri tanımlama, bölümleme ve taşıma yükü ortadan kalkmaktadır. Yoğun görevler başarılı bir şekilde yürütülmekte ve ardından sonuçlar mobil cihazdaki yerel bileşenlerle senkronize edilmektedir. Bu modelde, uzak kaynaklara yalnızca veriler iletilmekte, kodlar mobil cihazdan taşınmamaktadır. Böylece iletim yükü önemli ölçüde azaltılmaktadır. Uygulama çalışma anında yüksek yürütme yoğunluğuna ulaştığında, yerel yürütmeyi duraklatmakta ve yürütme için uygulama yığını belleği ile ham verileri uzak kaynaklara iletmektedir. Yürütmenin tamamlanmasının ardından ise sonuçlar bütünleştirilerek, yürütmeye devam edilmektedir. Ancak bu çözümlerdeki uygulama işlevselliği veya başarısızlıkları, uygulama yürütmesini etkileyen uzak işlevlere ve hizmetlere bağlıdır. Örneğin, navigasyon uygulamalarındaki konuşma bileşeni, mobil cihazın içinde kabul edilebilir bir doğrulukla yürütülmesi imkânsız olan yoğun kaynaklı bir görevdir.

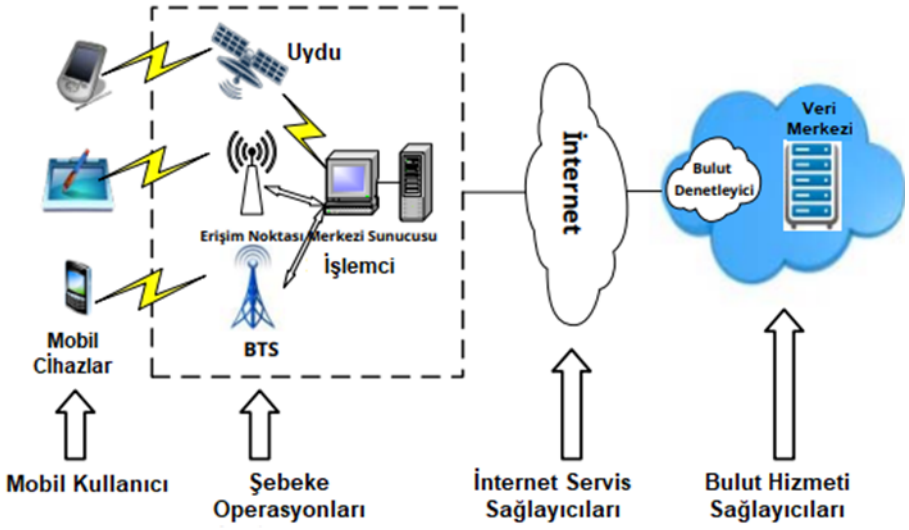
Canlı bulut akışı, tüm hesaplamaları mobil cihazın dışında gerçekleştirerek mobil cihazları büyütmeyi amaçlayan başka bir yaklaşımdır. Sonuçlar, mobil cihaza canlı olarak aktarılan, önceden derlenmiş ekran görüntüleri şeklinde kullanıcılara iletilmektedir. Bu yaklaşım, mevcut teknolojileri kullanarak, kurulması zor olan, düşük gecikme süreli, yüksek verimli, güvenilir kablosuz ağ gerektirmektedir.

Diğer bir yaklaşım ise kullanıcıların dijital içeriklerini bulut tabanlı kaynaklarda depolayarak, mobil depolamanın sanal olarak genişletildiği Dropbox gibi uzaktan veri yönetimi çözümleridir. Bilgi işlemdeki büyümeye paralel olarak, dijital veriler de hızla artmakta ve mobil cihazlarda daha büyük depolama alanlarına ihtiyaç duyulmaktadır. Bu durum mobil cihazların benimsenmesini ve kullanılabilirliğini daha da zorlaştırmaktadır. Bu minvalde, bulut depoları mobil cihazların depolama eksikliğini azaltmakta ve veri güvenliğinin iyileştirilmesine katkı sağlamaktadır (Abolfazli ve diğerleri, 2015).

1.2.3 Mobil Bulut Bilişim Mimarisi

Kavramsal açıdan mobil bulut bilişimin mimarisi incelendiğinde, baz istasyonu, erişim noktası veya uyduların kullanımı yoluyla mobil cihazlar şebekelere bağlanmakta ve kullanıcılar tarafından yapılan bilgi ile taleplerin (konum-kimlik), ağ servislerini sağlayan sunuculara bağlı merkezi işlemcilere kanalize edildiği görülmektedir (Şekil 1.7). Mobil şebeke işletmecileri, abonelerinin veri tabanlarında tuttukları verilere göre yetkilendirme, kimlik doğrulama ve muhasebe gibi hizmetleri kullanıcılara sunabilmektedir. Abonelerden gelen talepler ise internet hizmeti kullanılarak buluta gönderilmekte, bulut içindeki bulut denetleyicileri, yapılan talepleri işleyerek, istenilen hizmetleri sunmaktadır. Bu hizmetleri geliştirmek için sanallaştırma, hizmet odaklı mimari ve yardımcı bilgi işlem (veri tabanı sunucuları, uygulama ve web) kavramları kullanılmaktadır (Alizadeh ve diğerleri, 2013).

Şekil 1.7 Mobil Bulut Bilişim Mimarisi



Kaynak: Alizadeh ve diğerleri, 2013

Bir mobil bulut bilgi işlem ortamı, bulut sunucu yapısı ve şebeke yapısından oluşmaktadır. Mobil cihaz kullanıcıları, bulut sunucusuyla bir şebeke üzerinden iletişim kurmaktadır. Mobil cihaz verileri ve hizmetleri, gerçek zamanlı yoğun mobil uygulamaların performansını artırmak için uç buluta taşınmaktadır. Bulutun sorunsuz hizmet sağlaması için çok iyi tanımlanmış bir mobil bulut bilişim mimarisi gerekmektedir. Bu bağlamda, MCC ortamlarında sorunsuz iletişim elde edilmesine, uç sunucularda veri yükleme ve yoğun hesaplama gerektiren görevlerin zahmetsizce hesaplanmasına izin veren bir mimari oluşturulmalıdır (Costant ve diğerleri, 2021).

Genel olarak mobil bulut bilişimin çalışma prensibi şu şekildedir;

- Şebekeler ile mobil cihazlar arasındaki bağlantılar ve işlevsel arayüzleri kuran ve kontrol eden baz istasyonları aracılığıyla cihazlar mobil şebekelere bağlanmaktadır.
- Mobil kullanıcıların istekleri ve bilgileri, mobil şebeke hizmetleri sağlayan sunucuların bağlı olduğu merkezi işlemcilere iletilmektedir.
- Kullanıcıların istekleri internet üzerinden buluta gönderilmekte ve burada bulut denetleyicileri, mobil kullanıcıların talep ettiği hizmetlerini sağlamak

üzere bu istekleri işlemektedir (Hiremath ve Mallapur, 2015).

Mobil bulut bilişim ekosistemi, mobil cihaz kullanıcıları, şebeke operatörleri, internet servis sağlayıcıları, uygulama hizmetleri ve bulut bilişim sağlayıcıları gibi farklı katılımcılardan oluşmaktadır. Bu paydaşların tümü çeşitli şebekeler aracılığıyla birbirine bağlanmaktadır. Mobil cihazlar şebekelere, baz istasyonları (örneğin, baz istasyonu, erişim noktası veya uydu) aracılığıyla bağlanırken; mobil şebeke, mobil cihaz ile bulut ortamı arasında da baz istasyonları veya uydular üzerinden bağlantı sağlanmaktadır. Mobil şebeke mimarisi, mobil cihaz kullanıcısı veya bir mobil cihaz, radyo erişim şebekesi (RAN, Radio Access Network), çekirdek ağ (CN, Core Network) ve şebekeler arası radyo kanalından oluşmaktadır. Kullanıcı, mobil şebekeler ve/veya uydular vasıtasıyla birden çok bağlantıya erişebilmektedir.

Mobil kullanıcının istek ve bilgileri (örneğin kimlik ve konum), mobil şebeke hizmetlerini sağlayan sunuculara bağlı merkezi işlemcilere iletilmekte ve burada mobil şebeke operatörleri, uç aracı (home agent- HA)[1] ve abonenin veritabanlarında saklanan verilerine dayanarak, mobil kullanıcılara kimlik doğrulama, yetkilendirme ve hesaplama (AAA) hizmetlerini sunabilmektedir. Ardından abonenin istekleri internet üzerinden bir buluta yönlendirilmektedir. Bulutta ise bulut denetleyicileri tarafından mobil kullanıcılara ilgili bulut hizmetlerini sağlanması için talepler işlenmektedir (Pallavi ve Vadla, 2014).

Farklı bağlamlar açısından bakıldığında ise mobil bulut bilişim mimarisinin ayrıntıları değişiklik göstermektedir. İlk olarak, aşağıda yer alan mobil bulut bilişim için önerilen üç bulut mimarisi ele alınmıştır. Bu mimariler, mobil cihazların yeni özelliklerini kullanmak ve mobil uygulamaların yeni ihtiyaçlarını karşılamak için tasarlanmıştır.

[1] Uç aracısı (home agent - HA), mobil düğümlere (mobile node - MN) veya ağ sınırları boyunca hareket eden cihazlara yönelik mobilite yönetim hizmetleri sağlayan mobil şebeke sistemindeki bir bileşendir. Bu aracı, mobil IP (MIP) mimarisi içindeki, verileri hâlihazırda yabancı bir şebekeye bağlı olan mobil düğümlere yönlendirmekten sorumlu olan işlev olarak da ifade edilmektedir.

a) Mobil İstemci-Sunucu Mimarisi

Akıllı telefonlar gibi mobil cihazlar, internet erişimi, küresel konumlandırma sistemi (GPS, Global Positioning System), sensörler ve çeşitli uygulamalarla zengin kullanıcı deneyimi sağlamaktadır. Doğal olarak, cep telefonlarının yeteneklerinin ötesinde yoğun bilgi işlem gerektiren uygulamaların kullanılabilmesi için bulut hizmetlerinden yararlanılmaktadır. Bu modelde, bulut bilişim ile mobil uygulamalar için klasik istemci-sunucu modeli uygulanmaktır. Cep telefonları, sunucuya göz atmak için kullanıcı arabirimi sağlayan ince istemciler olarak işlev görmekte ve bulut sunucuları ise tüm uygulamaları çalıştırmaktadır. Cep telefonu, internet sunucularından kaynak talep etmesine benzer bir şekilde bulut üzerinde hesaplama yoğun uygulamaların yürütülmesini talep etmektedir. Ancak bu geleneksel istemci-sunucu modelinde, akıllı telefonların hiçbir avantajı kullanılmamakta ve birçok özelliği göz ardı edilmektedir (Gu ve Guirguis, 2014).

Akıllı telefonları geleneksel cep telefonlarından ve masaüstü bilgisayarlardan ayıran ana özelliklerden biri, mobil bilgi işlemle ilgili bağlam farkındalığıdır. Bağlam farkındalıklı bilgi işlem, mobil cihazların fiziksel çevrelerini algılamaları ve davranışlarını buna göre uyarlamaları sürecine verilen genel bir tanım olmakla beraber, temel bağlamlar kullanıcının nerede, kiminle beraber olduğu ve çevresinde hangi kaynakların bulunduğu şeklindeki sorulara verilen cevaplarla belirlenmektedir. Bağlam farkındalığı için konum farkındalığı temel bir girdi olarak yer almaktadır. Ayrıca, mobil cihazda bulunan algılayıcıların varlığına göre yakındaki kişiler (Bluetooth), ışık düzeyi (kamera), ses düzeyi (mikrofon), internet erişiminin varlığı (WiFi, 2N, 3N, 4N, 5N) gibi bağlam verileri de elde edilmektedir. Akıllı kişisel yardımcılar gibi sistemler kişilerin günlük davranışlarını belirlemek için bağlam farkındalıklı bilgi işlemden yararlanmaktadırlar (Anabilgi Anadolu, 2020).

Bağlam farkındalığı, akıllı telefonlardaki zengin sensörler tarafından etkinleştirilmektedir. Bağlam kavramı, mekânsal bağlam, etkinlik bağlamı ve grup bağlamı olmak üzere üç bileşen içermektedir. Mekânsal bağlam, telefonun GPS sensörü ve konum tabanlı hizmet (LBS) tarafından toplanan verilerle belirlenmektedir.

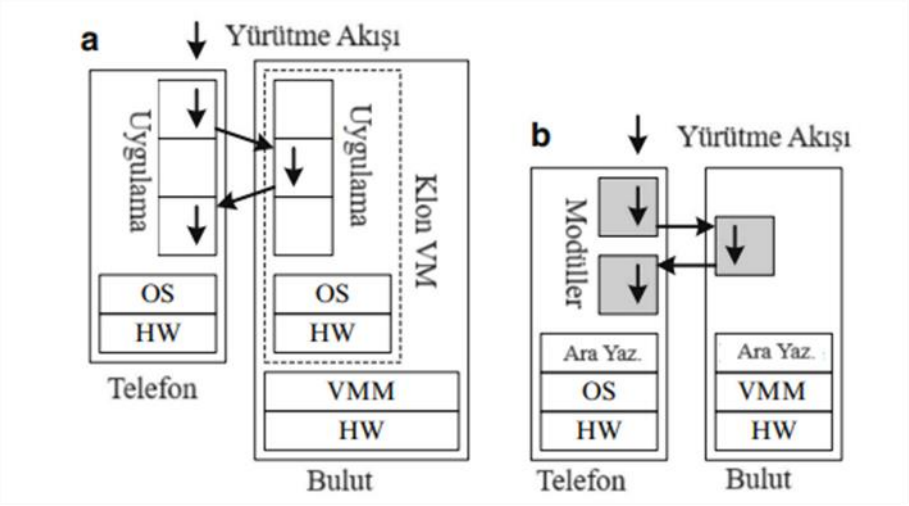
Bu veriler, mobil uygulamalara kullanıcının mevcut konumu ve geçmiş hareketlilik bilgilerini sağlamak için kullanılmaktadır. Etkinlik bağlamı, kullanıcının örneğin araba kullanırken, alışveriş yaparken veya konuşurken gerçekleştirdiği aktiviteleri temsil etmektedir. Etkinlik bilgileri, özelleştirilmiş mobil uygulamaların kullanıcıya gerekli işlevselliği sağlamasına olanak tanımaktadır. Grup bağlamı ise kullanıcıyı çevreleyen mobil cihazları ve diğer kullanıcıları temsil etmektedir (Gu ve Guirguis, 2014).

Mobil uygulamalar yakındaki diğer mobil cihazlarla etkileşime, mekânsal bağlamlarının ve etkinlik bağlamlarının sayesinde girmektedir. Ayrıca bağlamların sağladığı veriler, hizmet sağlayıcılara mobil kullanıcıların ihtiyaçlarına göre bilgi işlem gerçekleştirebilmeleri için ekstra bir veri de sağlamaktadır. Mobil bulut bilgi işlemi, geleneksel istemci sunucu bilgi işlem modelinden farklı kılan bir diğer özellik ise bulut sunucularında hesaplamayı mobil kullanıcıların talep etmesidir. Mobil uygulamalar bulut sunucularında yürütülebilse de mobil uygulamaların nasıl çalışacağına mobil cihazlar karar vermektedir. Bir mobil cihaz bir uygulamayı çalıştırdığında, uygulamanın yoğun bilgi işlem gerektiren kısmını tanımlamakta ve bu kısmı işlenmek üzere bulut sunucusuna aktarmaktadır. Bulut sunucuları, genellikle mobil uygulamaları gerçekleştirmek için ekstra bilgi işlem kaynakları sağlayan ikincil işlemciler ve depolama olarak kabul edilmektedir. Bu tür dağıtılmış bilgi işlemin koordinasyonu, esas olarak mobil cihazlar tarafından kontrol edilmektedir.

Mobil bilgi işlemin yeni gereksinimlerini karşılayarak, mobil cihazların yeni özelliklerinden yararlanmak ve buluttaki mobil uygulamaları artırmak için iki tür yeni istemci-sunucu mimarisi önerilmiştir. İlk mimari türünde bulutta bir cep telefonu klonu oluşturulmakta ve telefon ile klon periyodik olarak veya talep üzerine senkronize edilmektedir (Şekil 1.8-a). Bir uygulamanın yürütülmesi sırasında, telefon bulutta yürütülmesi gereken bir hesaplama bloku algılarsa, telefondaki uygulama işlemi, uyku durumuna geçmekte ve işlem bulutta devam etmektedir. Bulut yürütmeyi tamamladığında ise telefonun durumunu güncellemektedir.

Diğer mimari türünde ise bir telefonun tüm görüntüsünü klonlamak yerine, mobil uygulamalar modüler hale getirilmekte ve uygulamalar ile telefonun işletim sistemleri arasına bir ara katman eklenmektedir (Şekil 1.8-b). Bir mobil uygulama, işlevleri, veri ve işlevsellik bağımlılıklarına göre birden fazla modüle bölünmektedir. Modüller daha sonra hesaplama ihtiyaçları, depolama ihtiyaçları ve etkileşim miktarları gibi kaynak isteklerine göre taşınabilir veya taşınamaz olarak etiketlenmektedir. Taşınabilir modüller, mobil cihazlar ve bulut arasında geçiş yapabildiğinden, bu mobil uygulamalara, elastik mobil uygulamalar denmektedir. Taşınabilir modülleri mobil cihazlar kendi kaynaklarıyla çalıştıramadığında, bu modüller buluta yüklenmektedir. Ara yazılım, yani elastik yönetici, yüklenen modüllerle ilişkili veri ve kodun taşınmasını yönetmektedir. Elastik yönetici bir internet hizmetinin üzerine inşa edilebilmekte ve buna bağlı olarak uygulama modülleri weblet adı verilen birden çok bileşene bölünmektedir. Bu weblet'ler, normalde kaynakları kısıtlı cep telefonlarının yeteneklerini (bilgi işlem gücü, depolama) artırarak, cihazlarda veya bulutta çalışabilmektedir. Mobil cihazlar da genişletilmiş web istekleri aracılığıyla internet uygulamalarının taşınmasını ve yürütülmesini talep etmektedir (Gu ve Guirguis, 2014).

Şekil 1.8 Mobil İstemci-Sunucu Mimarisi



Kaynak: Gui ve Guirguis, 2014

b) Cloudlet Mimarisi

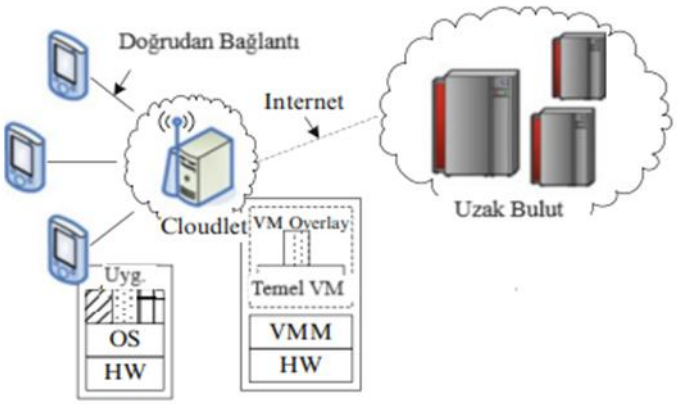
İstemci-sunucu mobil bulut mimarisi, mobil bilgi işlemin gereksinimlerini destekleyebilmesine rağmen, mobil cihazların erişim bağlantılarının sınırlamalarından etkilenmektedir. Temel sınırlama, şebekedeki gecikme süresidir. Mobil cihazlar, kablosuz geniş alan şebekesi (WWAN, Wireless Wide Area Network) ve internet üzerinden bulut sunucularıyla etkileşime girmektedir. Her iki şebekede de etkileşimli mobil uygulamalar için ihmal edilemez bir gidiş-dönüş gecikmesi olmaktadır. Başka bir gecikme ise bant genişliği sınırlı WWAN üzerinden toplu veri ve kod aktarımlarında ortaya çıkmaktadır.

Kablosuz genişbant teknolojileri büyük ölçüde gelişse de WWAN'ın bant genişliği, kablosuz yerel alan şebekesinin (WLAN, Wireless Local Area Network) bant genişliğinden önemli ölçüde daha küçük ve verilerin aktarım süresi hala tatmin edici olmaktan uzaktır (Gu ve Guirguis, 2014).

Bu mimaride, güçlü ancak uzak bulut sunucularıyla gecikme sınırlamasının üstesinden gelebilmek için kaynak açısından zengin bir bulut uygulaması, mobil kullanıcıların yakınına dağıtılmaktadır. Cloudlet olarak adlandırılan, bu mobilite açısından geliştirilmiş küçük ölçekli bir bulut veri merkezi, güçlü bilgisayarlardan veya yeterli bilgi işlem yeteneği ve gücüne sahip bir kümeden oluşmaktadır (Şekil 1.9). Cloudlet kurmanın temel amacı, bulut ile iletişim kurarken cihazların ağ gecikmesini azaltmaktır. Ayrıca, birden çok kullanıcının yüksek bant genişliği talebinin çözülmesine de yardımcı olmaktadır.

Burada, WiFi gibi tek sekmeli yüksek bant genişliğine sahip bir kablosuz erişim üzerinden mobil cihazlara bulut hizmeti sağlanmaktadır. Bulut uygulaması kullanılarak, mobil cihazlar ile bulut ortamları arasında kısa ve sınırlı gecikme sayesinde gerçek zamanlı etkileşim oluşturulmaktadır. Cloudlet, yönetim kolaylığı için bir kablosuz erişim noktası ile entegre edilebilmektedir (Gu ve Guirguis, 2014).

Şekil 1.9 Cloudlet Mimarisi



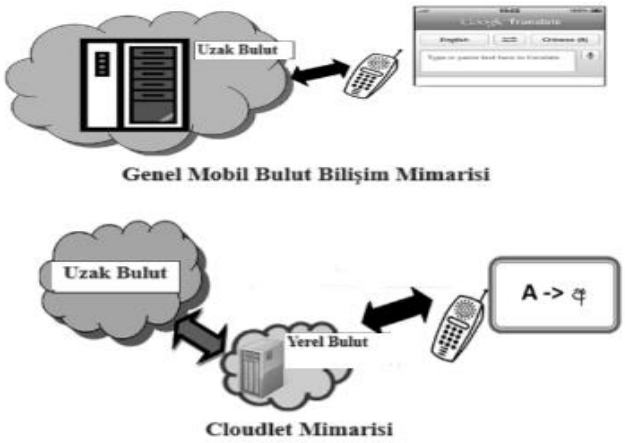
Kaynak: Gui ve Guirguis, 2014.

Bulutların kısa gecikme süresinden yararlanabilmesi için geleneksel bulut sunucuları kullanmak yerine yeni mekanizmalar gerekmektedir. Bu kapsamda araştırmacılar, geçici bir Cloudlet çözümü olarak dinamik sanal makine (VM, Virtual Machine) sentezini önermektedir. Bir mobil cihaz, bir uygulamayı yürütmek için bir Cloudlet'e ihtiyaç duyduğunda, uygulama için yer paylaşımlı sanal makine (VM overlay) üretmektedir. Yer paylaşımlı VM, uygulamanın yürütülmesi için esnek durum (soft state) içermektedir. Ardından cihaz, yer paylaşımlı VM'yi Cloudlet'e iletmektedir. Bu öneride, Cloudlet'e, minimum sistem çekirdek bileşenlerine sahip olan ve çoğu uygulamanın çalıştırılmasını destekleyebilen temel bir sanal makine önceden yüklenilmektedir. Cloudlet, yer paylaşımını tabanla birleştirmekte ve ardından uygulamayı yer paylaşımlı sanal makine depolanan esnek durum üzerinden yürütmektedir. İşlem tamamlandığında, Cloudlet sonuçları mobil cihaza geri göndermekte ve paylaşılan sanal makineden çıkarmaktadır (Gu ve Guirguis, 2014).

Genel mobil bulut bilişim mimarisinde mobil istemci buluttan istediği hizmeti talep etmekte ve bulut bu hizmeti sağlamaktadır. Bulut, bir kuruluşa veya bulut sağlayıcısına ait olup, aynı anda binlerce kullanıcıya hizmet vermektedir. Bu mimaride ana dezavantaj, uzak buluttan hizmet alınması ortaya çıkan iletişim gecikmesidir. Bu sorunun çözümü olarak, Cloudlet'in önbelleğe alınmış veri kopyasını içeren Cloudlet

mimarisi önerilmektedir. Cloudlet istemci ve bulut arasında kurulmaktadır. Bu bulut uygulaması, yalnızca birkaç kullanıcıya hizmet vermekte ve buluta kıyasla daha az iletişim gecikmesine sahip olmaktadır. Aşağıda yer alan Şekil 1.10'da genel mobil bulut bilişim ile Cloudlet mimarileri arasındaki fark gösterilmektedir.

Şekil 1.10 Genel Mobil Bulut Bilişim Mimarisi ve Cloudlet Mimarisi



Kaynak: Malik ve Chatuvedi, 2013.

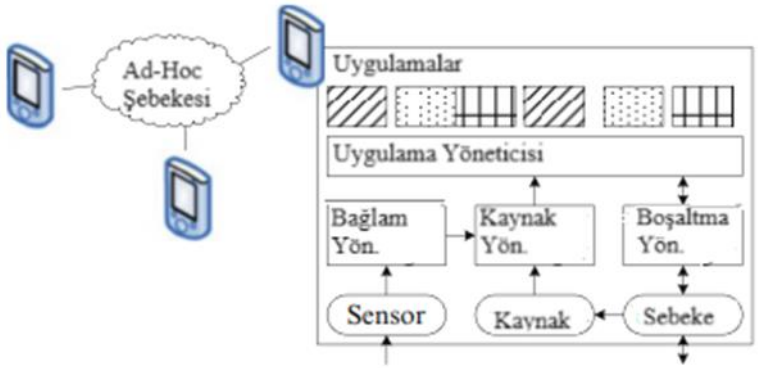
c) Ad-Hoc Mobil Bulut Mimarisi[2]

Mobil bilgi işlem için ilk iki bulut mimarisi, mobil cihazlar için uygulamaların yönetilmesi ve yürütülmesi konusunda umut verici olsa da bulut hizmetini barındırmak ve mobil cihazlara erişim sağlamak için bir altyapıya ihtiyaç duymaktadır. Ancak altyapının bir bölümünü yok eden bir doğal afet yaşandığı durumda, mobil cihazlar, Ad-Hoc modunda Bluetooth ve WiFi kullanmak dışında neredeyse hiçbir hizmete erişememektedir. Ayrıca, özellikle yalnızca yüksek maliyetli kablosuz veri bağlantılarının (örneğin hücresel bağlantı ve uydu bağlantısı) mevcut olduğu alanlarda, altyapı aracılığıyla bulut hizmetine erişmek çok pahalı olabilmektedir. Bulut hizmetlerine erişim olmadığında ortaya çıkan sorunları ele almak için Ad-Hoc mobil

[2] Ad-Hoc Şebekesi, iki veya daha fazla aygıt arasında iletişim ve veri aktarımının sağlandığı, herhangi bir kablosuz erişim noktası ya da Router'a ihtiyaç duyulmayan şebeke bağlantıları olarak tanımlanmaktadır.

bulut çözümü önerilmektedir. Bu çözüm, özellikle yakın lokasyonlarda bulunan ve ortak aktiviteleri paylaşan mobil kullanıcıların ihtiyaçlarına uygundur. Örnek bir senaryoda, turistler müzeleri ziyaret ederken, sergilerin açıklamalarıyla ilgilenmektedir. Burada, kişi metnin fotoğraflarını çekebilmekte ve metin tanıma yazılımını çalıştırabilmektedir. Böylece metni cep telefonunda saklayabilmektedir. Ancak, tüm metni işlemek, telefonun sahip olduğu bilgi işlem yeteneklerinden daha fazla kaynak gerektirmektedir. Kişi daha sonra yakındaki turistlerden yardım istemekte ve diğer turistler de açıklamayla ilgilenebileceğinden, düşük maliyetli WiFi iletişimini kullanarak özel bir şebeke oluşturmakta ve metin tanıma işlemini gerçekleştirmektedir. Tanınan metin daha sonra telefonlarında saklanmaktadır. Bu tür konumla sınırlı grup etkinliklerini desteklemek için kullanılabilen Ad-Hoc mobil bulut mimarisi, aşağıda yer alan Şekil 1.11'de gösterilmektedir (Gu ve Guirguis, 2014).

Şekil 1.11 Ad-Hoc Mobil Bulut Mimarisi



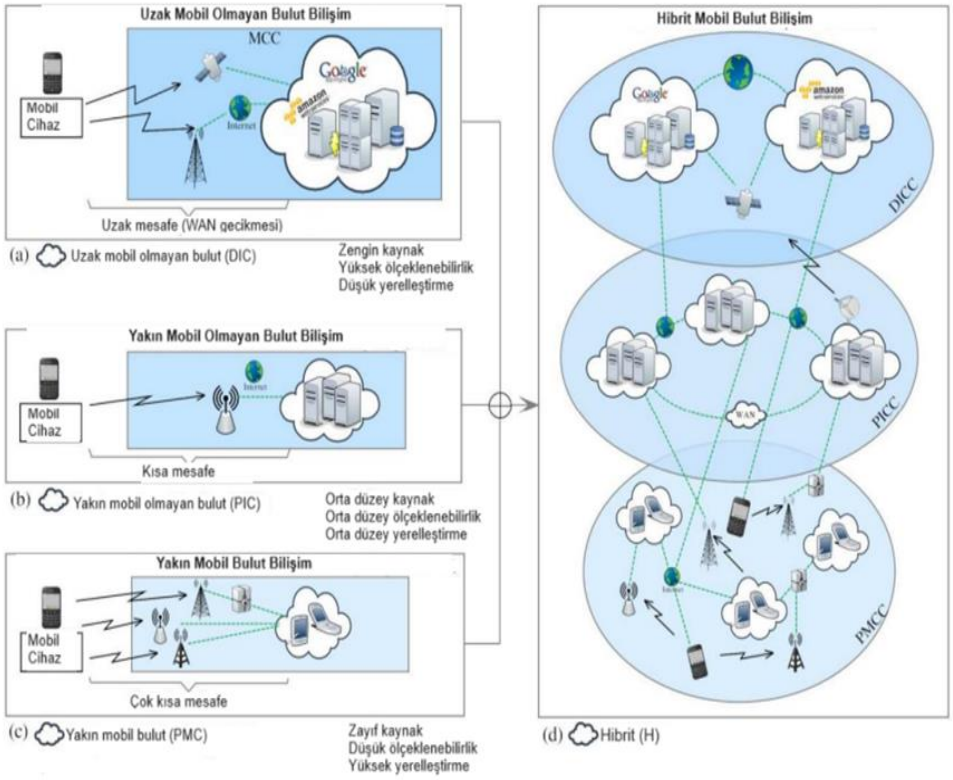
Kaynak: Gui ve Guirguis, 2014

Mimari; kaynak, uygulama, bağlam ve boşaltma yöneticisi şeklinde dört ana bileşenden oluşmaktadır. Kaynak yöneticisi uygulamaların ihtiyaçlarının profilini çıkarmakta ve mevcut kaynağı izlemektedir. Bir uygulama yürütüldüğünde, mevcut kaynak bilgileriyle birlikte bu profiller, bulut desteğinin gerekli olup olmadığına karar vermek amacıyla kontrol edilmektedir. Uygulama yöneticisi ise uygulamaların yüklenmesini ve yürütülmesini yönetmektedir. Bir uygulamayı başlatmak için buluta ihtiyaç duyulursa uygulama yöneticisi, boşaltma için uygulamaya ilave bilgiler eklemekte ve bu kapsamda etraftaki mobil cihazların konumu ile sayısını izlemektedir.

Böylece cihazların hareketliliği izlenerek, mobil cihazdan diğer cihazlara işler gönderilmekte ve yönetilmektedir. Ancak bu durumda, yük boşaltma ek görevi nedeniyle, yükü boşaltılan uygulamaların genel performansının, tek bir cihazda çalıştırmaya göre daha kötü olacağı endişesi oluşmaktadır. Bu doğrultuda bir çalışma yürütülmüş ve çıkan sonuçlara göre boşaltmalı yürütmenin normal yürütmeye göre yalnızca %1 daha yavaş olduğunu gösterilmiştir (Gu ve Guirguis, 2014).

Ayrıca literatürde, uzak mobil olmayan bulut bilişim, yakın mobil olmayan bulut bilişim, yakın mobil bulut bilişim ve hibrit bulut bilişim olmak üzere dört ana mobil bulut bilişim mimarisi de yer almaktadır (Şekil 1.12).

Şekil 1.12 Mobil Bulut Bilişim Mimarileri



Kaynak: Abolfazli ve diğerleri, 2015

a) Uzak Mobil Olmayan Bulut Bilişim:

Uzak mobil olmayan bulut terimi, bulut bilişim sağlayıcılarının yönettiği sanal sunucuları ifade etmektedir. Örneğin, Amazon Elastic Compute Cloud (Amazon EC2) bulut sunucuları bu kategoriye girmektedir. Geliştiriciler, uygulama kodunu yazmakta ve kodu bu sanal sunuculara dağıtmaktadır (Amazon, 2023a). Daha sonra sunucular mobil veri isteklerini işlemekte ve yanıtlamaktadır.

Mobil bulut bilişim için önerilen bu mimaride, mobil kullanıcı internet kanalı ile genel bulutların hesaplama kaynaklarını kullanmaktadır. Bu modelde, hesaplama görevleri, uzak mobil olmayan bulut kaynakları ve sonuçları mobil istemciye geri gönderilmektedir. Uzak mobil olmayan bulut bilişimin ana avantajları, yüksek hesaplama yeteneği, kaynak esnekliği ve nispeten yüksek güvenliktir. Yüksek bilgi işlem yeteneği ve esnekliği, uzaktan hesaplama süresini en aza indirmekte ve mobil pil tasarrufu sağlamaktadır. Uzak mobil olmayan bulut bilişimde veri merkezlerinin kullanım maliyeti, diğer modellere göre oldukça düşük kalmaktadır.

Bununla birlikte, uzak mobil olmayan bulut kaynakları ile mobil cihazlar arasındaki mevcut mimari, donanım ve platform heterojenlikleri, mobil ile bulut bilgisayarlar arasında kod ve veri taşınması kapsamında birlikte çalışabilirliği karmaşık hale getirmektedir. Ayrıca geniş alan ağı (WAN, Wide Area Network) gecikmesi de veri iletim hızı ve bant genişliğindeki önemli gelişmelere rağmen kablosuz iletişimde önemli bir sorun olarak yer almaktadır

Uzun WAN gecikmesi, uygulama yürütme performansını düşürmekte ve sınırlı olan mobil cihazın pil gücünü boşa harcamaktadır. Bununla birlikte, bir yandan hizmet tüketicilerinin hareketli olması ancak bulutların hareketli olmaması, WAN gecikmesini yoğunlaştırmakta ve mobil bulut bilişim çözümlerinin etkinliği ile verimliliğini düşürmektedir (Abolfazli ve diğerleri, 2015).

b) Yakın Mobil Olmayan Bulut Bilişim

Uzun WAN gecikmesinin etkilerini azaltmak amacıyla bilgi işlem kaynaklarına en az sayıda ara atlama ile erişmeye çalışılmış ve mobil bulut bilişim için alternatif mimari olarak yakın mobil olmayan bulut bilişimi önerilmiştir.

Bu mimaride mobil cihazlar, kafeler ve alışveriş merkezleri gibi halka açık yerlerdeki masaüstü bilgisayarların bilgi işlem kaynaklarını kullanmaktadırlar. Yakın mobil olmayan bulut bilişimde, uzak mobil olmayan bulut bilişimindeki gibi yoğun hesaplamalarda çok sayıda atlamadan geçmek yerine, görevler yakınlarda yer alan tek sekme mesafesindeki ortak bilgisayarlarda yürütülmektedir.

Yakın mobil olmayan bulut bilişim mimarisinin pek çok dezavantajı da bulunmaktadır. Yakın mobil olmayan bulut bilişimin bilgi işlem kaynaklarının kullanılması, özellikle hizmet sağlayıcının ve tüketicilerin güvenliği ile mahremiyetini sağlanması, kullanılan bilgisayarın ana işletim sisteminin konuk mobil işletim sisteminden izole edilmesi, bilgisayar sahiplerinin yakınlarındaki mobil cihazlarla kaynakları paylaşmaya teşvik edilmesi, isteğe bağlı kullanılabilirlik gibi birçok eksiklik barındırmaktadır (Abolfazli ve diğerleri, 2015).

c) Yakın Mobil Bulut Bilişim

Literatürde önerilen üçüncü mimari olarak yer alan yakın mobil bulut bilişimde, kaynak kısıtlamalı mobil cihazların yakınında yer alan ve kaynak paylaşmaya istekli zengin mobil cihazlar kullanılmaktadır. Özellikle akıllı telefonlar ve tabletler olmak üzere çağdaş mobil cihazların hızla artan popülaritesi ve sürekli artan çeşitliliği ile yakın mobil bulut bilişime avantaj sağlamaktadır.

Bu mimaride, eşler arası ve istemci-sunucu olmak üzere iki farklı bilgi işlem modeli uygulanmaktadır. Eşler arası (P2P, Peer-to-peer) bilgi işlem modelinde, hizmet tüketicisinin yakınlarda uygun mobil hizmet sağlayıcıyı bulmak için enerji tüketen düğüm bulma görevini gerçekleştirmesi gerekmektedir. Ancak hizmet tüketicisi,

cihazına saldırabilen ve gizliliğini ihlal edebilen sahte hizmet sağlayıcılara karşı savunmasız kalmaktadır.

İstemci-sunucu bilgi işlem modelinde ise mobil istemci, güvenilir bir arabulucu ile iletişim kurmakta ve yakınında bulunan en güvenilir düğüm talebinde bulunmaktadır. Arabulucu, farklı hizmet sağlayıcıları takip edebilmekte ve karşılıklı iletişimlerde güvenlik takibi yapabilmektedir. Bu tür kaynakları kullanmanın önemli avantajları, hizmet sağlayıcı ve tüketicinin heterojenliği, kaynak yaygınlığı ve kısa WAN gecikmesinin ihmal edilebilmesidir.

İstemci-sunucu veya P2P bilgi işlem modellerinde, hizmet sağlayıcı ve tüketicinin yakınlığı nedeniyle ara sekme sayısı azdır. Yakın mobil bulut kaynaklarının yaygınlığı, mobil istemcinin görevlerini herhangi bir zamanda herhangi bir yerde yürütülmesini sağlamaktadır.

Ancak bu mimaride kaynak çokluğu yüksek olmasına rağmen, ölçeklenebilirlik ve esneklik, bireysel mobil cihazların kısıtlamalı bilgi işlem gücü nedeniyle sınırlıdır. Mobilite yönetimi de bu mimarinin bir başka zorlu özelliği olarak ifade edilmektedir. Yakın mobil bulut bilişimde, mobil hizmet sağlayıcıları ile mobil hizmet tüketicilerinin sınırsız hareketliliği, kesintisiz bağlantı ve mobiliteyi önemli ölçüde karmaşıklaştırmakta, büyütme çözümlerinin verimliliğini önemli ölçüde düşürmektedir. Bir kullanıcı (hizmet tüketicisi veya sağlayıcı) farklı bant genişlikleri, titreşimleri ve gecikme süreleri olan heterojen kablosuz ağlarda hareket etmeye başladığında; değişen ağ çıktıları, artan mobil bulut mesafesi ve sık sık gerçekleşen ağ bağlantı kesilmeleriyle WAN gecikmesi artmakta ve bu durum uygulama yanıt süresi ile enerji verimliliği üzerinde doğrudan etki etmektedir. Ayrıca yakın mobil bulut bilişimin kullanım maliyeti, diğer hareketsiz kaynaklara göre daha yüksektir. Bu modelin başka bir zayıf noktası ise mobil cihazlarda güvenlik, gizlilik ve veri güvenliği eksikliğidir. Mobil cihazlar, fiziksel zarar, hırsızlık, donanım arızası ve kayıp riski gibi durumlar nedeniyle kullanıcı verilerini depolamak için yeterince güvenli değillerdir. Bu durumlar, mobil cihazların güvenlik zafiyeti oluşturmasına neden olmaktadır (Abolfazli ve diğerleri, 2015).

d) Hibrit Mobil Bulut Bilişim

Yukarıda yer alan üç mimarinin her biri, verimli mobil hesaplama artışı için en uygun kullanım kapsamında çeşitli avantajlar ve dezavantajlar içermektedir. Bu mimarilerin eksiklerinin azaltılması ve mobil bulut bilişim çözümlerinin daha verimli bir şekilde sunulması için bu üç mimarinin de kombinasyonu olan hibrit mobil bulut bilişim mimarisi öne sürülmüştür.

Çok katmanlı bir altyapısı olan bu mimari ile hesaplama ihtiyaçlarının en iyi şekilde karşılaması ve kullanıcının maliyet, güvenlik ile gecikme süresi gibi gereksinimlerinin optimizasyonunun yapılması hedeflenmiştir. Ancak, artan sayıda mobil hizmet tüketicisi ile hibrit bulut tabanlı kaynaklar, sistem karmaşıklığını artırmakta ve yönetim ile bakımı karmaşıklaştırmaktadır. Bu mobil bulut bilişim mimarisi için hafif kaynak keşfi ve zamanlama algoritmalarının kullanılması önerilmiştir (Abolfazli ve diğerleri, 2015).

1.2.4 Mobil Bulut Bilişimin Özellikleri

Mobil bulut bilişim aşağıda yer alan temel özelliklere sahiptir.

Otomatik kaynak sağlama ve yönetimi: Mobil bulutlar, otomatik kaynak sağlanmasına ve bulut bilgi işlem kaynaklarının, şebeke kaynaklarının ve mobil cihazın kaldırılmasına olanak sağlamaktadır (Chang ve diğerleri, 2013).

Otomatik kaynak sağlanmasında, kullanıcılar belirli rollere göre uygulamalara eklenmektedir. Bir kullanıcıya bir rol atandığında, bu kullanıcı ilgili uygulamada otomatik olarak oluşturulmakta ve erişim izinleri verilmektedir. Uygulamalardaki yetkilendirmeler kaldırmak istenildiğinde ise ayarlanılan yapılandırma tercihlerine bağlı olarak kullanıcının tüm uygulamalardaki hesapları silinmekte veya askıya alınmaktadır.

Ölçeklenebilirlik: Mobil bulut bilişimde ölçeklenebilirlik; bulut ölçeklenebilirliği, şebeke ölçeklenebilirliği ve mobil kullanıcılar ile cihazlar açısından mobil ölçeklenebilirlik olmak üzere üç boyut içermektedir. Mobil bulut bilişim için önerilen çerçeveler, kullanıcı sayısında bir artış olduğunda performansta bozulma veya fiziksel altyapıda değişiklik olmaksızın uyarlanabilir bir şekilde ele alınabiliyorsa, yüksek oranda ölçeklenebilir olarak kabul edilmektedir. Eğer bu çerçeveler, bir üçüncü şahıs tarafından yönetilen bazı merkezi sunuculara bağımlıysa orta düzeyde, aksi takdirde zayıf kabul edilmektedir (Chang ve diğerleri, 2013).

Esneklik ve erişilebilirlik: Mobil bulutlar, mobil kullanıcıların bulut uygulamaları ile hizmetlerine her zaman ve her yerde erişmelerini sağlamaktadır (Chang ve diğerleri, 2013). Mobil bulut bilişim, bölgesellik sınırlamasını ortadan kaldırarak kullanıcıların istedikleri zaman ve istedikleri yerde internetten veri elde etmelerini sağlamaktadır. Aynı zamanda, gerçek zamanlı kaynak kullanımını izleyebilmekte ve gerektiğinde kaynakların tahsisini yeniden dengeleyebilmektedir (Dai ve diğerleri, 2012).

Mobil bulut hizmeti bağlantısı: Mobil bulutlar, farklı şebekeler ve standartlar ile üçüncü taraf yazılımlar arasında kolay ve güvenli bağlantı sağlamak için uygulama programlama arayüzleri (API, Application Programming Interface) ile protokoller sunmaktadır (Chang ve diğerleri, 2013).

Sanallaştırma: Mobil bulutlarda, şebeke sanallaştırması, çeşitli bilgi işlem kaynakları için bulut sanallaştırması ile mobil cihazların ve kaynakların sanallaştırılması şeklinde üç tür sanallaştırma desteklenmektedir (Chang ve diğerleri, 2013).

Çoklu kiracılık: Bu özellik, tek bir mobil bulut yazılımın kablosuz bir internet veya heterojen ağlar üzerinde birden çok mobil kiracıya hizmet vermesine olanak tanımaktadır (Chang ve diğerleri, 2013).

Mobil siber güvenlik: Mobil siber güvenlik; mobil cihazları, heterojen ağları, bulut sunucuları, mobil uygulama hizmet programları ile verileri, yetkisiz erişim gibi

saldırılardan korumak için tasarlanmış güvenlik yetenekleri, teknolojileri, süreçleri ve uygulamaları kapsamaktadır (Chang ve diğerleri, 2013).

Mobil hizmet faturalaması: Mobil bulut bilişimde hizmetlerin kullanılması hem mobil hizmet sağlayıcısını hem de bulut hizmeti sağlayıcısını içermektedir. Bununla beraber, mobil hizmet sağlayıcıları ile bulut hizmet sağlayıcılarının farklı hizmet yönetimi, müşteri yönetimi, ödeme yöntemleri ve fiyatları bulunmaktadır. Bu yüzden hizmetin fiyatının nasıl belirleneceği, fiyatın farklı varlıklar arasında nasıl paylaştırılacağı ve müşterilerin nasıl ödeyeceği dikkat edilmesi gereken hususlar arasında yer almaktadır. Örneğin, bir mobil kullanıcı bulutta mobil oyun uygulaması çalıştırdığında; bu durum oyun hizmeti sağlayıcısını (bir oyun lisansı sağlanması), mobil hizmet sağlayıcısını (veriye baz istasyonu aracılığıyla erişilmesi) ve bulut hizmet sağlayıcısını (bir veri merkezinde oyun motoru çalıştırılmasını) içermektedir. Kullanıcının ödemesi gereken tutar bu üç sağlayıcı göz önünde bulundurularak hesaplanmalıdır (Jalan ve Bhagat, 2014).

1.2.5 Mobil Bulut Bilişim Modelleri

Mobil bulut bilişim teknolojisinin incelenmesi için kavramsal bir model öne sürülürken, mobil bulut bilişim sistemlerinin yönetilmesi amacıyla da çeşitli modeller sunulmuştur. Mobil bulut bilişim teknolojisinde, bulut bilişim modellerinin genel özelliklerden farklı olarak bulut ve istemci arasındaki ilişkiye odaklanılmıştır (Alizadeh ve diğerleri, 2013).

Çeşitli bulutlar ile ağ teknolojilerinin birleşik elastik kaynaklarından yararlanan ve zengin bir mobil bilgi işlem teknolojisi olarak tanımlanan mobil bulut bilişimde; genellikle gerekli kaynaklar ve sağlanan hizmetlere yönelik kullandıkça öde yaklaşımı ile daha düşük bir maliyet elde etmek amacıyla hizmet faturalandırma modeli benimsenmektedir.

Mobil bulut bilişimin sınıflandırılması sanallaştırmaya dayalı olmakla beraber, mimarisini ise mobil istemciler, ara yazılımlar ve bulut hizmetleri bileşenleri

oluşturmaktadır. Ara yazılım, mobil istemcilerin bulut hizmetlerine erişimini sağlayarak, bulut platformlarında barındırılan bir vekil sunucu (Proxy) görevi görmekte olup; mobil istemciler ile bulut hizmetleri arasındaki, optimizasyon ve önbelleğe alma gibi etkileşimleri iyileştirmektedir. Genel olarak, ara katman yazılımı mobil istemciler ve bulut hizmetleri arasındaki etkileşimin işlevselliğini, güvenilirliğini ve uyumluluğunu artırmaktadır (Perez ve Kumar, 2017).

Mobil bulut bilişim kavramsal bir model olarak incelendiğinde; bulut ve istemci karşılıklı olarak yer alırken, aralarında iletim kanalı adı verilen bir bileşen bulunmaktadır. İletim kanalı, mobil istemcinin kanalda yer alan protokolleri kullanarak buluta bağlandığı farklı kablosuz iletişim protokollerinden oluşmaktadır. İletim kanalı bileşeni üzerinde ise bulut ve istemci tarafında yer alan bağlam yönetimi ve kaynak yönetimi bölümleri bulunmaktadır. Kaynak planlamasında, bilgisayar ve depolama kaynakları, sanal makineler kullanılarak yönetilmektedir. Bağlam yönetiminde ise, bağlam parametreleri izlenir ve bu parametreler, bağlam koşullarına bağlı olarak değiştirilmektedir (Alizadeh ve diğerleri, 2013).

Kullandıkça öde prensibine dayanan, heterojen ortamlar ve platformlar ne olursa olsun, internet kanalı aracılığıyla çok sayıda mobil cihaza her yerde, her zaman hizmet vermek için sınırsız işlevsellik ve depolama sunmayı hedefleyen mobil bulut bilişimin hizmet modelleri aşağıdaki gibi sınıflandırılmıştır.

- **Hizmet Olarak Mobil Ağ (MNaaS)**

Bu modelde, mevcut bulut altyapılarına bağlantı sunulması amacıyla heterojen ağ altyapısı ile ilgili kaynaklar, kablosuz ağ altyapısının dinamik olarak yapılandırılması, dağıtılması ve isteklere yanıt verebilmesi için satıcı tarafından istemcilere sağlanmaktadır.

Hizmet olarak mobil ağ şeklinde adlandırılan bu mobil bulut bilişim modelinin en büyük avantajı bir şebeke hizmeti satıcısı için nispeten düşük bir başlangıç maliyeti sağlaması ve yüksek ölçeklenebilirliği olmakla birlikte, örnek olarak açık kaynaklı bir

bulut işletim sistemi olan OpenStack Networking verilmektedir. Bu modelde, kullanıcıların kendi ağlarını oluşturmasına, trafiği kontrol etmesine, sunucuların ve cihazların bir veya daha fazla ağa bağlamasına olanak tanınmaktadır (Chang ve diğerleri, 2013).

- **Hizmet Olarak Mobil Bulut Platformu (MPaaS)**

Bu modelde, mobil bulut bilişim platformu hizmet olarak sağlanmaktadır. Genellikle mobil uygulama geliştirme, dağıtma ve barındırma desteklenmektedir. Bu kapsamda, MPaaS'a örnek olarak AppMobile uygulaması verilmektedir. Uygulama, mobil uygulama geliştirilmesini ve dağıtımını mümkün olduğunca kolaylaştırmak için geliştirme, barındırma ve analitikle ilgili zengin bir araç seti sunmaktadır (Karthik ve Manhar, 2020).

- **Hizmet Olarak Mobil Bulut Altyapısı (MIaaS)**

Bu modelde, kullandıkça öde yaklaşımıyla kullanıcılara mobil özellikli bir bulut altyapısı ve kaynakları sağlanmaktadır. MIaaS'ta, bilgi işlem ve depolama kaynaklarının yanı sıra ağ bileşenleri ile cihazları, isteğe bağlı mobil istemci isteklerine göre sağlanmakta ve yönetilmektedir (Chang ve diğerleri, 2013).

- **Hizmet Olarak Mobil Veri (MDaaS)**

Bu modelde, veri işlemlerinin, yönetiminin ve kablosuz internet üzerinden erişimlerinin desteklenmesi için kullanıcılara büyük ölçekli mobil özellikli veritabanları (veya veri depoları) ile gerekli depolama kaynakları sağlanmaktadır (Chang ve diğerleri, 2013).

- **Hizmet Olarak Mobil Yazılım (MSaaS)**

Hizmet olarak mobil yazılım modelinde, mobil özellikli yazılım ile ilgili hizmetler, mobilite ve konum algılama özelliğiyle müşterilere sunulmaktadır. Bir mobil uygulama, bulut üzerinde dağıtılıp yürütülmektedir. Ayrıca mobil kullanıcıların, mobil uygulama hizmetlerine kablosuz internet iletişimine dayalı ince mobil istemci aracılığıyla erişmesini ve doğrulamasını desteklemektedir (Chang ve diğerleri, 2013).

- **Hizmet Olarak Mobil Uygulama (MAaaS)**

Hizmet olarak mobil uygulama, mobil uygulama için çeşitli e-mobil uygulamaların konuşlandırılabildiği, yönetilebildiği, barındırılabildiği ve izlenebildiği bir hizmet iş modeli şeklinde tanımlanmaktadır (Chang ve diğerleri, 2013).

- **Hizmet Olarak Mobil Test (MTaaS)**

Hizmet olarak mobil test; kullandıkça öde modeli ile çeşitli mobil tabanlı test cihazlarının, araçlarının ve hizmetlerinin bir sağlayıcı tarafından istemcilerin mobil tabanlı testlerinin desteklenmesi için kaynak olarak sağlandığı bir hizmet modelidir (Chang ve diğerleri, 2013).

- **Hizmet Olarak Mobil Topluluk (MCaaS)**

Bu model, çeşitli mobil sosyal ağların ve toplulukların, kullandığın kadar öde modeli aracılığıyla mobil müşterilere sosyal topluluk hizmetleri ile ağ sağlamak için dinamik olarak oluşturulup yönetilebilen hizmet modelini ifade etmektedir (Karthik ve Manhar, 2020).

- **Hizmet Olarak Mobil Multimedya (MMaaS)**

Bu model, filmler ve dijital oyunlar gibi zengin medya tabanlı uygulama hizmetlerinin müşterilere multimedya hizmetleri sunmak için dağıtılabildiği, yönetilebildiği ve barındırılabildiği bir hizmet modelidir (Chang ve diğerleri, 2013).

Yukarıda yer alan hizmet olarak mobil yazılım (MSaS), hizmet olarak mobil veri (MDaaS), hizmet olarak mobil altyapı (MIaaS) gibi mobil bulut bilişim modellerinde, sanallaştırma katmanları dikkate alınarak sınıflandırılma yapılmıştır. Ancak yapılan çalışmalar doğrultusunda hem siber fiziksel sistemin hem de siber sanal sistemin dâhil olması nedeniyle, mobil bulut modellerinin, hizmet çerçevesinde yer alan bileşenlerin rollerine göre sınıflandırılmasının daha uygun olacağı ifade edilmiştir. Bu doğrultuda, mobil bulut bilişim hizmet modellerinin sınıflandırılmasında, mobil varlıklar ile bulut tabanlı kaynaklar arasındaki ilişkilerin kullanılması önerilmiştir. Bu görüşe dayanarak, mevcut mobil bulut teknolojisi, hizmet tüketicisi olarak mobil bulut bilişim (MaaSC, Mobile as a Service Consumer), hizmet sağlayıcı olarak mobil bulut bilişim (MaaSP Mobile as a Service Provider) ve hizmet aracısı olarak mobil bulut bilişim şeklinde (MaaSB, Mobile as a Service Broker) üç ana modelde sınıflandırılmıştır (Pallavi ve Vadla, 2014).

- **Hizmet Tüketicisi Olarak Mobil Bulut Bilişim (MaaSC)**

MaaSC, sanallaştırma, ayrıntılı erişim kontrolü ve diğer bulut tabanlı teknolojilerin ortaya çıkmasıyla beraber geleneksel istemci-sunucu modelinden türetilmiştir. Mobil cihazlar, daha yüksek performans ve geniş uygulama kapasitesi elde etmek amacıyla hesaplama ve depolama işlevlerini dış kaynak olarak buluttan alabilir. Bu mimaride, hizmet mobil cihazlara tek yönlü olarak sağlanmakta ve mobil cihazlar hizmeti tüketen taraf olarak işlev görmektedir. Birçok mevcut mobil bulut hizmeti, bu kategoriye dahildir. Bu modeli kullanan mobil cihazlar, bilgi işlem ve depolamayı buluta yaptırarak, daha yüksek performans elde edebilmekte ve daha geniş uygulama yeteneklerine sahip olabilmektedir (Pallavi ve Vadla, 2014).

- **Hizmet Sağlayıcısı Olarak Mobil Bulut Bilişim (MaaSP)**

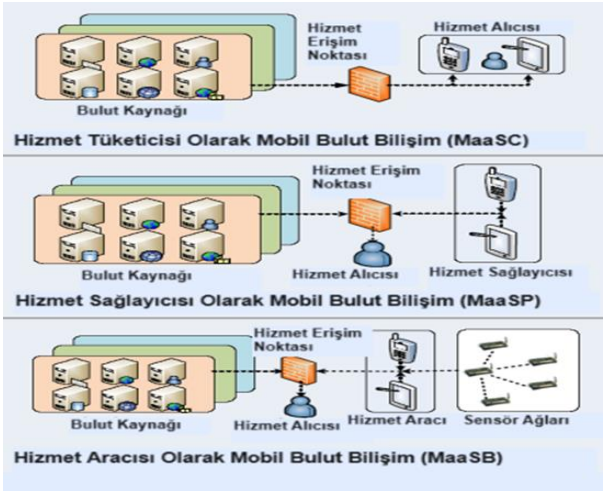
Bu modelde, mobil cihazın rolü, hizmet tüketicisinden hizmet sağlayıcıya çevrilmiştir. Örneğin, yerleşik sensörler (GPS modülü, kamera, jiroskop vb.) sayesinde mobil cihazlar, komşu ortamlardan gelen verileri algılayabilmekte ve bulut aracılığıyla diğer

mobil cihazlara hizmet sunabilmektedir. Mobil cihazlar tarafından sağlanan hizmet türleri, algılama ve işleme yeteneklerine bağlı olarak çeşitlilik göstermektedir (Pallavi ve Vadla, 2014). Her istemci servis sağlayıcının yeteneklerine sahip olduğu için MaaSC'nin tam tersi olarak sunulan MaaSP'de sağlanan hizmetler; GPS, kamera ve cihazla ilgili diğer veriler gibi uygulama verilerine bağlanan mobil cihazların algılama ve işleme yeteneklerine dayanmaktadır (Perez ve Kumar, 2017).

- **Hizmet Aracısı Olarak Mobil Bulut Bilişim (MaaSB)**

MaaSB, diğer mobil cihazlar veya algılama düğümleri için ağ oluşturma ve veri iletme hizmetlerinin sunulduğu, hizmet sağlayıcısı modelinin bir uzantısı olarak tanımlanmaktadır. MaaSB, mobil cihazların yeteneklerinin sınırlı olduğu durumlarda kullanılmakla beraber, bulut sınırı mobil cihazlara ve kablosuz sensörlere kadar genişletilmektedir. Böylece, bir mobil cihaz, 2N, 3N, 4N, 5N, Bluetooth, WiFi gibi çeşitli iletişim yaklaşımları aracılığıyla ağ hizmetleri sağlayan bir ağ geçidi veya proxy olarak yapılandırılabilmektedir. Bu hizmet modeli kapsamında, mobil cihazlar aynı zamanda sensör ağları için güvenlik katmanı görevi de görebilmektedir (Pallavi ve Vadla, 2014). Şekil 1.13'te mobil bulut bilişimin üç temel hizmet modeline yönelik genel bir çerçeve verilmektedir.

Şekil 1.13 Mobil Bulut Bilişim Hizmet Modelleri



Kaynak: Pallavi ve Vadla, 2014

Teknolojinin ilerlemesiyle beraber, mobil hizmet uygulamaları ile bulut altyapıları, platformları ve depolarının yanı sıra mobil platformları ve teknolojilerini de kapsayan mobil bulut altyapısındaki bileşenler farklılaşmış, dolayısıyla da mobil bulut bilişime ilişkin mevcut anlayış değişmiştir. Literatürde yer alan bir çalışmada mobil bulut bilişimin ilk çıkışından günümüze olan süreci üç nesil altında incelenmiştir (Karthik ve Manhar, 2020).

a) Birinci Nesil – Kişisel Mobil Bulut

Son yıllarda, mobil kullanıcılarına kişisel mobil bulut sağlayan çok sayıda tedarikçi firma bulunmaktadır. Örneğin Lenovo'nun sunduğu Lenovo Cloud, Apple tarafından hizmete sunulan iCloud veya Acer'in AcerCloud'u bunlardan sadece birkaçıdır. Bu uygulamalar; mobil kullanıcılara veri, içerik, depolama, müzik ve video oynatıcı, takvim, fotoğraflar ile belgeler gibi belirli kişisel uygulama hizmetleri sağlayan kişisel bulutlar olarak bilinmektedir. Mobil kullanıcılar için bu kişisel bulutlar, birinci nesil mobil bulut hizmetlerini sağlamaktadır. Şekil 1.14'te mevcut kablosuz ağlar ve internet tarafından desteklenen kişisel bulut ortak altyapısı gösterilmektedir (Karthik ve Manhar, 2020).

Şekil 1.14 Mobil Kullanıcılar için Kişisel Bulut Altyapıları

Kaynak: Karthik ve Manhar, 2020.

Birinci nesil mobil bulutların temel özellikleri aşağıda verilmektedir.

- **Mobil uygulama hizmeti:** Mobil uygulama sunucuları, bir veri merkezindeki bulut altyapısında (veya platformunda) konuşlandırılmakta, barındırılmakta ve bakımı yapılmaktadır.

- **Ağ iletişimi**: Mobil iletişim, mevcut kablosuz iletişim sağlayıcıları tarafından işletilen mevcut heterojen kablosuz şebekeler tarafından desteklenmektedir.

- **Ölçeklenebilirlik**: Bilgi işlem ve hizmet ölçeklenebilirliği, mevcut bilgi işlem ve depolama bulutlarından yararlanılarak desteklenmektedir.

- **Kaynaklar:** Bilgi işlem ve depolama kaynakları, kullandığın kadar öde faturalandırma modeli ile isteğe bağlı talepler üzerine sağlanmakta ve yönetilmektedir.

- **Senkronizasyon**: Mobil içerik ve uygulama verileri, mobil istemciler için içerik tutarlılığı ve bütünlüğü sağlamak üzere senkronize edilmektedir.

- **Mobilite:** Kişisel mobil bulutların hareketliliği, mevcut konumlarına göre kullanıcı odaklı mobil içerikler için desteklenmektedir.

- **Çoklu Kiracılık:** Önceden tanımlanmış mobil uygulama hizmetlerini desteklemek ve sunmak için tek kiracı tabanlı uygulama sunucusu sağlanmaktadır (Karthik ve Manhar, 2020).

b) İkinci Nesil - Bulut Tabanlı Mobil Bulut Altyapıları

Şekil 1.15'te gösterilen, ikinci nesil mobil bulut hizmetlerinin ortak altyapısı aşağıdaki anahtar özelliklere sahiptir;

- **Mobil uygulama hizmeti:** Mobil özellikli uygulama sunucuları, mobil SaaS sistemleri olarak geliştirilmekte ve veri merkezinde yer alan bulut altyapısı üzerinde konuşlandırılarak, barındırılmakta ve bakımı yapılmaktadır.

- **Ağ iletişimi:** Kişisel bulutlar ile benzer şekilde, mobil iletişim mevcut heterojen kablosuz ağlar tarafından desteklenmektedir.
- **Ölçeklenebilirlik:** Mobil SaaS sistemleri, mevcut bilgi işlem ve depolama bulutlarından yararlanarak bilgi işlem ve hizmet ölçeklenebilirliği sunmaktadır.

- **Kaynaklar:** Mobil SaaS sistemleri, kullandığın kadar öde faturalandırma modeli ile talep üzerine sağlanan ve yönetilen gerekli bilgi işlem ile depolama kaynaklarını sağlamaktadır.

- **Senkronizasyon:** Mobil uygulama verileri ve hizmet içerikleri, önceden tanımlanmış uygulama hizmetlerinin gereksinimlere göre kurumsal kullanıcılar ile kiracılılar için senkronize edilmektedir.

- **Mobilite:** Mobilite, mobil kullanıcılara ve kurumsal müşterilere mevcut konumlarına göre çok kiracılı mobilite hizmetleri sunmak amacıyla Mobil SaaS sistemleri tarafından desteklenmektedir.

- **Çoklu kiracılık:** Çok kiracılı uygulama hizmetleri (SaaS sistemleri gibi), kurumsal kullanıcılara ve müşterilerine çeşitli kiracılı iş mantıklarını, uygulama iş akışlarını, ağ iletişimi hizmet kalitesi (QoS, Quality of Service) gereksinimlerini, kullanıcı arayüzü formlarını ve iş veritabanlarını desteklemek için sağlanmaktadır.

- **İsteğe bağlı hizmet:** Mobil istemcilere yönelik isteğe bağlı mobil veri ve içerik hizmetlerine ek olarak, mobil SaaS sağlayıcılarına da isteğe bağlı bilgi işlem ve depolama hizmetleri sağlanmaktadır (Karthik ve Manhar, 2020).

Şekil 1.15 İkinci Nesil – Mobil Bulut Altyapısı

Kaynak: Karthik ve Manhar, 2020.

c) Üçüncü Nesil – Mobil Bulut Hizmetleri

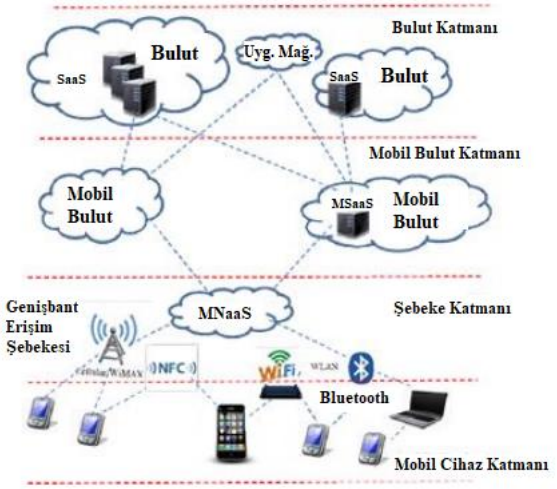
Mobil veri kullanımındaki büyüme; mobilitenin işletmelerdeki kullanılma biçiminde dramatik değişimlere, ödemelerde kredi kartlarının yerini mobil ödemenin almasına ve yazılım tanımlı ağ teknolojisi ile ağ sanallaştırması gibi teknolojilerin gelişmesine yardımcı olmaktadır. Ancak mobil erişim trafiği yeni bir değişim sürecine girerken, kablosuz şebeke iletişim hizmetlerinde;

- Şebeke bant genişliklerinde ve trafik desteğinde sınırlı ölçeklenebilirlik,
- Taşıyıcı odaklı şebeke altyapıları,
- Kablosuz hizmet sağlayıcıları tarafından barındırılan ve işletilen farklı kablosuz ağlar arasında sınırlı taşınabilirlik,
- Sınırlı ağ kaynağı paylaşımı, ağ kaynaklarının verimsiz kullanımı,
- Önceden yapılandırılmış fiziksel ağ bileşenlerine ve cihazlarına yüksek oranda bağımlılık,
- Şebekelerde yeşil bilgi işleme daha az önem verilmesi

gibi hala bazı sınırlamalar bulunmaktadır (Karthik ve Manhar, 2020).

Belirtilen kısıtlamalar, mobil bulut bilişimin gelişmesinde önemli engeller olarak yer almaktadır. Bu kapsamda, mobil şebeke hizmetlerinde elastik ölçeklenebilirliğin elde edilebilmesi için kablosuz şebeke bilişiminin, ağ bulut merkezleri ve ağ sanallaştırma çözümleriyle üçüncü nesil mobil bulutlara taşınarak, mevcut kablosuz şebeke altyapısının güncellenmesi önerilmektedir. Şekil 1.16'da üçüncü nesil mobil bulut hizmeti altyapısı gösterilmektedir.

Şekil 1.16 Üçüncü Nesil Mobil Bulut Hizmeti Altyapısı



Kaynak: Karthik ve Manhar, 2020

Mobil bulut hizmeti altyapısı aşağıdaki dört katmandan oluşmaktadır;

- **Bulut katmanı:** Bu katmanda, çeşitli arka uç mobil uygulama sunucularının; bilgi işlem kaynağı paylaşımı, ölçeklenebilirlik, daha yüksek kaynak kullanımı ve maliyet azaltılması için mevcut bulut altyapıları ile bulut platformlarından yararlanabilmek amacıyla yerleşik yazılım olarak seçilen bir bulutta konuşlandırılıp yürütüldüğü bulut altyapıları bulunmaktadır. Bulut bilişim hizmetleri esnektir ve bulut bilişim hizmeti kullanıcılarının taleplerine göre artırılabilmekte veya azaltılabilmektedir (Karthik ve Manhar, 2020).

- **Mobil bulut katmanı:** Bu katman, enerji tasarruflu çözümler, mobil bulut kaynak sağlanması ve yönetilmesi, konuma duyarlı yönetim hizmetleri ve

mobil bulut güvenlik yönetimi gibi mobil bulut bilişimdeki temel hizmet yeteneklerinden oluşmaktadır (Karthik ve Manhar, 2020).

- **Şebeke katmanı:** Elastik ağ ölçeklenebilirliği ile daha yüksek ağ kaynağı kullanımı elde edebilmek için ağ sanallaştırma çözümleri ve enerji tasarrufu teknikleri kullanılarak; şebeke kaynakları, NaaS tarafından gruplandırılmakta, yönetilmekte ve sunulmaktadır (Karthik ve Manhar, 2020). Bu katmandaki mobil şebeke kullanımı ise şu şekildedir; kullanıcı taleplerini ele alan birden fazla mobil şebeke işletmecisi bulunmakta ve bilgiler baz istasyonları aracılığıyla iletilmektedir. Mobil kullanıcının istekleri ve bilgi aktarımları, uç aracısı (HA, Home Agent) tarafından sağlanan kimlik doğrulama, yetkilendirme ve hesaplama (AAA, Authentication, Authorization, Accounting) gibi mobil şebeke hizmetleri tarafından ele alınmaktadır. Bu noktada, mobil şebeke işletmecileri, HA aracılığıyla abonelerin veritabanlarında depolanan bilgilerin tanımlanmasına yardımcı olmaktadır. Başarılı kimlik doğrulama ve yetkilendirmeden sonra işletmeci, mobil kullanıcı taleplerini internet üzerinden buluta iletmektedir. Kullanıcı daha sonra buluttaki denetçiler tarafından sağlanan ilgili hizmetlere erişebilmektedir (Noor ve diğerleri, 2018).

- **Mobil cihaz katmanı:** Mobil kullanıcılara, güvenli uçtan uca mobil işlemler ve bağlantının yanı sıra güçlü kullanıcı gizliliği ile mobil bulut uygulama hizmetlerine kapsamlı erişim için mobil bağlantı arayüzleri sağlanmaktadır (Karthik ve Manhar, 2020). Bu katman, mobil cihazları (akıllı telefonlar ve tabletler gibi) kullanarak bulut hizmetlerine erişen birçok mobil bulut hizmeti kullanıcısından oluşmaktadır. Bu mobil cihazlar, kablosuz erişim noktaları, baz istasyonu veya uydu kullanarak şebeke katmanına bağlanmaktadır (Noor ve diğerleri, 2018).

Üçüncü nesil mobil bulut bilişim, diğer iki nesile göre birtakım avantajlar barındırmaktadır. Bu avantajlar şu şekildedir;

- Kablosuz ağların elastik ölçeklenebilirliği, kaynak kullanımı ve paylaşımı artmaktadır.

- Farklı pazar segmentlerine hitap eden iş modellerinin yanı sıra çeşitli erişim teknolojilerini destekleyen mobil ağ kaynaklarının geliştirilmesi kapsamında sermaye harcamaları azaltılmaktadır.

- Enerji tasarrufu çözümleri ve birden fazla hizmetin bir arada bulunması nedeniyle konuşlandırılmış kaynakların daha yüksek kullanımı sayesinde işletme maliyetleri azaltılmaktadır.

- Arka uç hizmetlerinin esnekliği ve birleşik erişim sayesinde mobil uygulama geliştirme maliyetleri azaltılmaktadır.

Bununla birlikte modelde, çeşitli engeller de bulunmaktadır. Model, bulut katmanındaki temel zorluk olarak mobil uygulamalar içinde vekil sayısal hizmetlerin sunulmasını belirtmektedir. Bulut altyapısı yönetimi, içerik ve yazılım dağıtım ağları, standart bulut hizmetleriyle paylaşılan konular olup, aynı zamanda mobil bulut uygulamalarının başarısı için kritik öneme sahiptir. Ek olarak, mobil bulutların ses tanıma veya görüntü işleme gibi görevleri için mobil cihazlara yüklenen hesaplama yükünü azaltma ihtiyacı da bulunmaktadır. Bu gibi durumlarda, belirli bir uygulama için iletişim ve hesaplama gecikmesi arasındaki toleransa bağlı olarak; uygulamanın yürütülmesi kapsamında verimli ve etkili uyarlanabilir teknikler geliştirmek, başarılı mobil bulut hizmeti sunumunun temel bileşenlerinden biridir. Şebeke katmanı için ise mobil şebeke işletmecileri tarafından görselleştirilmeye ilişkin araştırmalar bir süredir devam etmektedir. Genellikle radyo erişim ağı seviyesinde uygulanan ağ paylaşımı, özellikle orta ölçekli operatörler arasında yaygın hale gelmektedir. Bu doğrultuda kayda değer başka bir gelişme ise genellikle mobil sanal şebeke işletmecilerinin (MVNO, Mobile Virtual Network Operator) ortaya çıkmasıdır. Ancak teknik açıdan bakıldığında bu tür çözümler statik olmakla birlikte, önemli bir yönetim ve operasyonel ek yük getirmektedir. Öte yandan, cihaz teknolojisindeki mevcut durum,

mobil cihaz katmanında yürütülen ana işlevlerin buluta taşınmasına izin vermemektedir. Bunun yerine bulut ve şebeke katmanlarında, bulut teknolojisi tarafından sunulan hizmetlerin tutarlı ve nispeten şeffaf bir şekilde erişilmesine yönelik önemli gelişmelerin mobil cihaz katmanını da etkileyeceği öngörülmektedir. Burada temel amaç, mobil bulut sistemlerine ve hizmetlerine erişim için uyarlanabilir, verimli mekanizmalar geliştirmektir (Karthik ve Manhar, 2020).

1.3 Mobil Bulut Bilişimin Uygulanması Kapsamındaki Anahtar Gereksinimler

Mobil bulut bilişim, sınırsız hareketlilik, işlevsellik ve depolama sağlamak için doğrulanmış şebeke teknolojilerinden ve bulut bilişim kaynaklarından yararlanılarak, internet aracılığıyla her yerde ve her zaman çok sayıda mobil cihaza hizmet veren zengin bir mobil bilgi işlem teknolojisidir. Özetle, mobil kullanıcılar, bellek kapasitesi ile işlem hızı gibi bilgi işlem ve depolama kaynaklarına ihtiyaç duymadan bulutlardaki mevcut hizmetlere erişebilmekte, tüm karmaşık bilgi işlemleri mobil cihazların dışında gerçekleşmektedir.

Mobil bulut bilişim, ağlar arası ortamda sorunsuz hizmet sunabilmesi için bazı temel özellikleri barındırmalıdır. Kurumsal çözüm sağlayıcısı veya web/mobil uygulama geliştiricisi açısından bir mobil bulut bilişim platformunun temel gereksinimleri şunlardır:

- Mobil hizmetlere şeffaf erişim sunan ve ağ teknolojileri hakkında özel bilgi gerektirmeyen basit arayüz programları,
- Uygulamaların tek bir ticari anlaşma kapsamında birden çok taşıyıcı ağda devreye alınma yeteneği,
- Her bir operatörün, abone katılımı/çıkışı ve gizlilik yönetimi gibi özel ağ politikalarını sorunsuz şekilde yürütmesi (Chavan ve Rajani, 2013).

Ayrıca mobil cihaz, uygulama bölümleme-boşaltma, veri bütünlüğü, güvenlik-gizlilik ve hizmet dönüşüm gereksinimleri de bu teknoloji kapsamında sağlanmalıdır.

a) Mobil cihaz

Mobil cihazların sınırlı kaynak kapasitesine sahip olması nedeniyle daha iyi kaynak kullanımını sağlayan ve bu kaynak kullanımını mobil cihazlar ile mobil bilgi işleme dâhil eden yaklaşımlar ve çözümler tasarlanmalıdır (Al-Janabi ve diğerleri, 2017).

b) Uygulama Bölümleme ve Boşaltma

Bir mobil cihaz ile bulut arasında, güvenlik açısından önemli bir eksiklik olarak uygulama bölümleme, boşaltma ve uzaktan çalıştırma gibi veri iletişimi gerektiren teknolojiler yer almaktadır. Şifreleme yöntemleri bu konuda yardımcı olabilirken, özellikle hesaplamalı boşaltma ve uzaktan yürütmede performans düşüşünü önlemek için bazen bu yöntemlerin kullanılması gerekli değildir. Saldırganlar, verilerin geçici olarak depolandığı işlemcilerin içindeki ve dışındaki bellek konumlarını hedef alabilmekte, bu durum bireyleri savunmasız bırakabilmektedir (Al-Janabi ve diğerleri, 2017).

c) Veri Bütünlüğü

Mobil cihaz kullanıcıları, her yerde ve her zaman mobil bulut bilişimdeki mevcut kaynaklara erişebilmelidir. Bu nedenle, veri bütünlüğü ve kurtarma hayati önem taşımaktadır. Mobil bulut bilişimin kullanılması kapsamında veri bütünlüğü, doğruluğu ve tutarlılığı ile ilgili sorunların üstesinden gelmek için standart bir depolama ve yönetim altyapısı gerekmektedir (Al-Janabi ve diğerleri, 2017).

d) Güvenlilik ve Gizlilik

Mobil bulut bilişimde, verilerin birden çok lokasyondaki bulutta depolanması ve işlenmesi, hizmet sağlayıcıları ile bulut sunucularının farklı bölge ve ülkelerde bulunması gizlilik sorunlarına yol açmaktadır. Veri uygulama, sanallaştırma ve uzaktan yürütme yalnızca hizmet sağlayıcıların kontrolü altında olduğundan, mevcut

engellerin üstesinden gelinmesi daha da zorlaşmakta ve tehditlere karşı savunmasız hale gelmektedir (Al-Janabi ve diğerleri, 2017).

e) Hizmet Dönüşümü

Mobil bulut bilişim, mobil cihazlara bilgisayar benzeri hizmetler sağlamayı amaçlamaktadır. Sabit ve mobil cihazlar ile kablolu ve kablosuz veri iletişimi arasındaki farklılıklar nedeniyle, mobil bulut bilişimde hizmet dönüşümü karmaşıktır. Bu kapsamda, çevre dostu iş ile hizmet modelleri oluşturma, ekonomik planlama ve fiyatlandırma planları gerektirmektedir. Farklı mobil cihazlar ve bulut hizmeti depoları arasındaki zorlukları hafifletmek için çeşitli yaklaşımlar önerilmektedir.

Kullanıcı hareketliliği, geniş uygulama çeşitliliği ve değişen kablosuz şebeke durumu nedeniyle, mobil bulut bilgi işlem bağlamı oldukça dinamiktir. Bu sebeple mobil bulut bilişim hizmetlerini, mevcut çözümlere entegre eden ve halihazırdaki cihaz, şebeke ile bulut sunucusu durumuna bağlı olarak en uygun olanı etkinleştiren kapsamlı bir çerçevenin tasarımına odaklanılmalıdır (Al-Janabi ve diğerleri, 2017).

1.4 Mobil Bulut Bilişim ve Bulut Bilişimin Karşılaştırılması

Bulut bilişim teknolojisi masaüstü istemcileri için zengin esnek bilgi işlem kaynakları sağlamayı hedeflerken; mobil bulut bilişim, mobil kullanıcılara hizmet vermeyi ve hareket halinde sınırsız işlevsellik sunmayı vaat etmektedir. Hizmet sağlayıcıları da bulut bilgi işlem ve mobil bulut bilişimde farklılık göstermektedir. Bulut bilişimdeki kaynaklar, satıcının tesislerinde bulunan ve kurumsal mülkiyet altında bulut veri merkezleri olarak bilinen, paralel ve dağıtılmış bir şekilde çalışan bir veya daha fazla birleşik bilgi işlem varlığından oluşmaktadır. Bununla birlikte, mobil bulut bilişimde kaynaklar, bulut tabanlı kaynaklar olarak adlandırılan mobil cihazların kaynak eksikliklerini azaltabilen bulut teknolojilerini ve ilkelerini devralan herhangi bir bilgi işlem cihazı olabilmektedir (Abolfazli ve diğerleri, 2015).

Bulut bilişim yalnızca kablolu iletişimden yararlanırken, mobil bulut bilişim hem kablolu hem de kablosuz cihazları kullanmaktadır. MCC'deki baskın iletişim modu kablosuz olmasına rağmen, hareketsiz bulut tabanlı kaynaklar, son kullanıcıların hesaplama deneyimini geliştirmek için kablolu ağlardan yararlanmaktadır. Bulut bilişim ile mobil bulut bilişim arasındaki bir diğer önemli fark ise amaçlarıdır. Bulut bilişimde kaynak esnekliği ve kullandıkça öde veya tüketim tabanlı fiyatlandırma politikası kavramları tanıtılarak, özel veri merkezlerini çalıştırmanın sahiplik ve bakım maliyetlerinin azaltılması amaçlanmaktadır. Bulut bilişim, masaüstü kullanıcılarının bilgi işlem kaynaklarını otomatik olarak sağlayabilecekleri ve buna göre ödeme yapabilecekleri, talep üzerine esnek kaynaklar vadetmektedir. Bulut bilişim teknolojisinde kaynak kullanım oranını iyileştirmeye, yoğun bilgi işlemin enerji maliyetini en aza indirmeye ve olumsuz etkileri azaltmaya çalışılmaktadır (Abolfazli ve diğerleri, 2015).

Mobil bulut bilişimde ise kaynak yoğun mobil bilgi işlem görevlerinin uzun süre yürütülmesi sağlanarak mobil cihazların hesaplama yeteneklerinin artırılması hedeflenmektedir. Bulut bilgi işlemdeki kullanıcılar, yüksek kaynak kullanılabilirliği ve talep üzerine yoğun hesaplamaları yürütmenin maliyetinden tasarruf etmek için, mobil hizmet tüketicileri ise uygulama yürütme süresini artırmak, mobil cihazın enerji tüketimini ve kablosuz iletişim maliyetini azaltmak içilln bulut tabanlı hizmetleri kullanmaktadır (Abolfazli ve diğerleri, 2015).

Bu bağlamda, bulut bilişim teknolojisinin en büyük avantajı isteğe bağlı self servisken, artan pil ömrü ve depolama ise mobil bulut bilişimin en büyük avantajı olarak belirtilmektedir. Aşağıda yer alan Tablo 1.2'de bulut bilişim ile mobil bulut bilişimin özellikleri karşılaştırmalı olarak verilmektedir.

Tablo 1.2 Bulut Bilişim ile Mobil Bulut Bilişimin Karşılaştırılması

Özellikler	**Bulut Bilişim**	**Mobil Bulut Bilişim**
Hizmet Tüketicileri	Masaüstü kullanıcıları	Mobil kullanıcılar
Servis Sağlayıcıları	Büyük veri merkezleri	Bulut tabanlı kaynaklar
Ağ Taşıyıcısı	Kablolu	Kablolu-kablosuz
Hedefler	Esneklik, kullandıkça öde	Mobil büyütme
Enerji Çözümleri	Sunucu tarafından enerji tasarrufunun yapılması ve daha az CO_2 salınımı	Bataryanın korunması
Hareketlilik	İstemci-sunucu hareketsiz	İstemci-sunucu hareketli
Son Kullanıcılar	Kaynakların para mülkiyeti ve bakım maliyeti	Zamansal, enerji ve iletişim ek yükü
Uygulamalar	Uzaktan eğitim, depolama	Mobil oyun, mobil sağlık hizmetleri, mobil bankacılık

Kaynak: Abolfazli ve diğerleri, 2015

Genel olarak bakıldığında ise mobil bulut bilişimin, bulut bilişimin bir alt dalı olduğu görülmekle birlikte, iki kavram net sınırlarla birbirinden ayrılamamaktadır. Bu kapsamda bulut bilişim için yapılan çalışmalar, düzenlemeler veya güvenlik tedbirleri mobil bulut bilişimi de etkilemektedir. Bundan dolayı bulut bilişim için yapılan bir düzenleme ya da alınacak güvenlik önlemi mobil bulut bilişimi de kapsamaktadır.

1.5 Mobil Bulut Bilişimin Avantajları ve Dezavantajları

Akıllı telefon ve tablet gibi mobil cihazlar zaman ve mekândan bağımsız, en etkili ve kullanışlı iletişim araçları olarak giderek artan bir şekilde insan yaşamının vazgeçilmez bir parçası haline gelmektedir. Mobil kullanıcılar, kablosuz şebekeler aracılığıyla cihazlarda veya uzak sunucularda çalışan mobil uygulamalar üzerinden çeşitli hizmetleri kullanmaktadır. Bununla birlikte, mobil cihazlar kendi kaynaklarında

(örneğin, pil ömrü, depolama ve bant genişliği) ve iletişimde (örneğin, mobilite ve güvenlik) birçok zorlukla karşı karşıya kalmaktadır. Sınırlı kaynaklar, hizmet kalitesinin iyileştirilmesini önemli ölçüde engellemektedir. Bu kapsamda, mobilite, iletişim ve taşınabilirlik gibi özellikleriyle bulut teknolojisi, mobil bilgi işlem için umut verici bir çözüm olarak sunulmuştur. Mobil uygulamaların hızla büyümesi ve bulut bilişim konseptinin ortaya çıkmasıyla beraber mobil bulut bilişim, mobil kullanıcılar için potansiyel bir teknoloji haline gelmiştir.

Mobil bulut bilişimin temel amacı, kullanıcıların buluta erişmesi ve buluttan veri alması için uygun ve hızlı bir yöntem sağlamaktır ki bu tür kullanışlı ve hızlı yöntemler sayesinde, mobil cihazları kullanarak bulut bilişim kaynaklarına etkin bir şekilde erişilmektedir. Mobil bulut bilgi işlemin en büyük zorluğu olarak mobil cihazların ve kablosuz şebekelerin sınırlamaları ile güvenlik açıkları görülmektedir. Bu zorluklar, mobil ve dağıtılmış cihazlardaki uygulama tasarımını, programlamayı ve devreye almayı sabit bulut cihazlarına göre daha karmaşık hale getirmektedir. Mobil bulut bilişim ortamında, mobil cihaz sınırlamaları, kablosuz iletişimin kalitesi, uygulama türleri ve bulut bilişimden mobil cihazlara entegrasyon bu teknolojinin değerlendirmesini etkileyen önemli faktörler olarak yer almaktadır.

1.5.1 Mobil Bulut Bilişimin Avantajları

Mobil cihazlar çeşitli kısıtlamalar barındırmakta ve bu sorunların üstesinden gelebilmek için çeşitli çözümler önerilmektedir. Ancak bu çözümler, mobil cihazların yapısında bazı değişiklikler veya maliyetin artmasına neden olacak yeni donanımlar gerektirmekte ve tüm mobil cihazlar için uygulanabilir olmamaktadır. Mobil bulut bilişimin, uygulamaları buluta yükleyerek, mobil cihazlardaki büyük hesaplama süreçlerinin azaltılması için kullanılması hedeflenmektedir (Al-Janabi ve diğerleri, 2017).

Mobil bulut bilişim, kullanıcılarına bulut teknolojisinin sunduğu altyapı, platform ve yazılımları düşük maliyetle ve talep üzerine esnek bir şekilde kullanmalarına olanak tanıyarak çeşitli avantajlar sunmaktadır. Ayrıca, mobil bulut bilgi işlem,

kullanıcılarına bulutta veri depolama ve işleme hizmetleri sağlayarak; yoğun kaynak kullanan tüm bilgi işlemlerin bulut içinde gerçekleştirilebilmesi nedeniyle, güçlü bir cihaz yapılandırmasına (işlemci hızı, bellek kapasitesi vb.) yönelik ihtiyacı da ortadan kaldırmaktadır (Hiremath ve Mallapur, 2015).

Bulutta, veriler ile uygulamalar, birkaç bilgisayarda depolanmakta ve yedeklenmektedir. Veriler ile uygulamaların birden fazla bilgisayarda yedeklenmesiyle mobil cihazlardan bilgi kaybı olasılığı azaltılmakta ve güvenilirliği etkili bir şekilde artırılmaktadır. Ayrıca mobil bulut bilişim, mobil kullanıcıların buluttaki mevcut kaynakları depolamasına ve erişmesine izin veren kablosuz ağla kullanılmaktadır. Örneğin, Amazon Simple Storage Service (Amazon S3) dosya depolama hizmetini desteklemekte ve Image Exchange'de bulutlardaki büyük depolama alanı kullanılmaktadır (Al-Janabi ve diğerleri, 2017).

Kaynaklar talep üzerine sağlanmakta olup, bu durum dinamik olarak hem servis sağlayıcılarına hem de mobil kullanıcılarına kaynak ayırmaya gerek kalmadan uygulamaları yürütmek için çeşitli seçenekler sağlamaktadır. Mobil bulut bilişim ile kullanıcıların talep ve beklentilerini karşılamak için mobil uygulama dağıtımı gerçekleştirilmektedir. Ayrıca kullanılan hizmet sayısından bağımsız olarak güvenilir ağ üzerinden hizmet sağlanması ile kaynakların esnek ve ölçeklenebilir kullanılması gerçekleştirilmektedir (Al-Janabi ve diğerleri, 2017).

Mobil bulut bilişimin işletmelere yönelik sunduğu avantajlardan bazıları şunlardır (Karthik ve Manhar, 2020);

- Mobil bulut uygulamalarına bir tarayıcı aracılığıyla erişilebildiğinden, kablosuz internet üzerinden tüm mobil kullanıcılara daha geniş erişim sunulmaktadır. Bu kapsamda, bulut bilişim uygulamalarına yalnızca akıllı telefon kullanıcıları değil, cep telefonunun internet erişimi olan tüm mobil kullanıcılar tarafından erişilebilmektedir.

- Kurumsal mobil bağlantı kapsamı; mobil kullanıcıların yanı sıra sosyal ağ ve sosyal medya bulut kullanıcılarını da içeren bir bulut topluluğuna genişlemektedir.

- Şebekelerde, bulut kaynaklarında ve mobil cihazlarda kaynak paylaşımı ve kullanımı artmaktadır.

- Çeşitli sensör ağlarına ve mobil cihazlara bağlanarak mobil uygulamaları, bulut uygulamaları ve SaaS sistemleri paylaşılarak, mobil özellikli akıllı uygulamaları çeşitli mobil uygulamalarda kolayca geliştirilebilmekte ve dağıtılabilmektedir.

- Mevcut bulut teknolojisinden yararlanarak mobil tabanlı uygulamaların geliştirme, dağıtılma ve bakım maliyetleri azaltılmaktadır.

- Mobil bulut altyapılarında, platformlarında ve mobil SaaS'ta enerji verimli çözümler kullanılarak mobil bulutların enerji tüketimi azaltılmaktır.

Mobil bulut bilişim kullanıcılarına/müşterilerine de çok önemli avantajlar sunmaktadır (Karthik ve Manhar, 2020);

- Bulut tabanlı veri depolama ve kablosuz internet vasıtasıyla erişim hizmetlerinden yararlanılarak; mobil cihazlar, sınırsız sanal mobil veri depolama ve işleme gücünün sağlandığı taşınabilir ve kişisel masaüstü bilgisayarlara dönüştürülmektedir.

- Kablosuz şebeke ve mobil internet üzerinden bulut hesaplama görevi bulut sunucularına yüklenerek mobil cihazların pil ömrü ve hesaplama gücü artırılmaktadır.

- Gelişmekte olan mobil bulut altyapılarına, platformlarına, uygulama mağazalarına, hizmet olarak yazılımlara ve bulut tabanlı uygulamalara sınırsız mobil bağlantı sunulmaktadır.

- Farklı operatörler tarafından sunulan kablosuz şebeke hizmet planlarının bölgesel sınırlamaları, ağ bağlantı ve standart sorunları ile hizmet engelleri ortadan kaldırılmaktadır.

- Kablosuz ağların, mobil cihazların ve bulut altyapılarının çeşitli yöntemler ile sanallaştırmaları sağlanmaktadır.

Mobil bulut bilişim, çeşitli araştırmalarla ortaya çıkarılan birçok uygulama olasılığının yanı sıra mevcut mobil bilgi işlemi de güçlendirmektedir. Mobil bilgi işlemin güçlendirilmesine; doğal dil işleme, görüntü işleme, sorgulama, GPS paylaşma, kalabalık bilişim[3], sensör veri uygulamaları ve internet erişimini paylaşma gibi çeşitli örnekler verilebilmektedir (Alizadeh ve diğerleri, 2013).

Mobil bulut bilişimin sunmuş olduğu avantajlar aşağıda ayrıntılı bir şekilde ele alınmıştır.

i. Pil ömrünün uzatılması

Batarya kapasitesi söz konusu olduğunda, bilgisayar gibi diğer bilgi işlem cihazlarına kıyasla nispeten sınırlı olan cep telefonları, işlevlerinin çoğunu sınırlayan kısıtlı bir hesaplama kapasitesine sahiptir. Örneğin, GPS gibi konum servislerinin kullanımı, çok fazla sensör kullanımını içerdiğinden çok fazla da enerji tüketmektedir. Aynı şekilde, video oyunları için görüntü işleme, doğal dil işleme, artırılmış gerçeklik ve giyilebilir bilgi işlem gibi çok büyük işlem kapasitesi gerektiren bazı uygulamalar da pil kapasitesini hızlı tüketmektedir. Bu kapsamda, işlemci performansını iyileştirmek ve

[3] Kalabalık bilişim, bilgisayarların yapması zor olan görevlerin internet üzerinden dağıtılan çok sayıda insan tarafından gerçekleştirildiği bir dağıtılmış çalışma biçimi olarak tanımlanmaktadır.

güç tüketimini azaltmak için ekranı ve diski akıllıca kontrol etmek gibi çeşitli çözüm önerileri sunulmaktadır. Ancak, sunulan bu çözümler mobil cihazların kurulumunda dönüşüme ihtiyaç duymakta veya daha pahalı olan ve mobil cihazlar için uygun bir seçenek olmayan yeni donanım sistemleri gereksinimleri ortaya çıkarmaktadır. Bu minvalde, hesaplama boşaltma tekniği, sınırlı kaynaklara sahip mobil cihazların, bulutlarda bulunan sunucular gibi daha becerikli araçlara geçirilmesi amacıyla önerilmektedir (Alizadeh ve diğerleri, 2013). Yoğun hesaplama gerektiren uygulama bileşenlerinin uzak bulut sunucularına taşıma görevi hesaplama boşaltma olarak tanımlanmaktadır. Bu teknik ile büyük miktarda güç gerektiren mobil cihazlarda çalışan uygulamalar için harcanan uzun süre azaltılmaktadır. Mobil boşaltmanın potansiyeli, temel olarak hücresel şebeke ve WiFi gibi mobil şebeke teknolojilerine bağlıdır. Hücresel şebeke kullanılarak yapılan veri iletimi, yüksek bant genişliği sunabilmesi nedeniyle WiFi'nin aksine önemli miktarda enerji gerektirmektedir. Bu nedenle hesaplama boşaltma, yerel yürütmenin uzaktan yürütmeye göre daha fazla zaman ve enerji tükettiğinde gerçekleştirilmesi gerektiği belirtilmiştir (Fellah ve diğerleri, 2020).

Yapılan araştırmalar, uzaktan yürütülen uygulamalar ile büyük ölçüde enerji tasarrufu sağlanabildiğini ortaya koymuştur (Alizadeh ve diğerleri, 2013). Enerji sınırlamaları ile ilgili yapılan çalışmalarda, bazı araştırmacılar, mobil oyunlardaki bileşenlerin arayüzünün bulut sunucularına boşaltılması ile pil enerjisi kullanımının bilgisayar oyunları için %27 ve satranç oyunları için %45 oranında azaltabileceğini göstermiştir (Allam ve diğerleri, 2017).

ii. Veri depolama kapasitesinin ve işlem gücünün iyileştirilmesi

Depolama kapasitesi mobil cihazlar için bir kısıtlama olmakla birlikte mobil bulut bilişim, mobil kullanıcıların kablosuz şebeke aracılığıyla büyük verilerinin bulutta depolanmasını/erişilmesini sağlamaktadır. Dosya depolama hizmetini destekleyen Amazon Simple Storage Service (Amazon S3) mobil bulut bilişimin bu şekilde kullanımının ilk örneklerindendir. Bu mobil fotoğraf paylaşım hizmeti, mobil kullanıcıların görüntülerini çektikten hemen sonra bulutlara yüklemekte, kullanıcılar

tüm görüntülere herhangi bir cihazdan erişebilmektedir. Görüntüler, bulutlarda gönderilip işlendiğinden, kullanıcılar mobil cihazlarında önemli miktarda enerji ve depolama alanı tasarrufu yapabilmektedir (Dev ve Baishnab, 2014).

Mobil bulut bilişim, özellikle veri depolama ve işlem gücü olmak üzere tüm mobil cihazlar için genel kaynak yönetimi sunmaktadır. Bulut bilişim, tüm cihazlar için aracı kısmı oluşturmakta ve mobil cihaz, aracısı ile mevcut alanın ötesinde başkalarıyla bağlantı kurmak için iletişim kurmaktadır. Bu mimariyi kullanan bir kullanıcı, yazılım hizmetini özel olarak en yakın buluta sığdırmak için sanal makine teknolojisinden yararlanmakta ve WLAN üzerinden hizmeti kullanabilmektedir (Alizadeh ve diğerleri, 2013).

Özetle mobil bulut bilişim, kullanıcılarına büyük verilerini bulutta depolamasına ve bu verilere erişmesine olanak tanımaktadır. Ayrıca yoğun hesaplama gerektiren uygulamaların işletme maliyetini düşürmeye de yardımcı olmaktadır. Mobil uygulamalar, verilerini bulutta saklamakta ve cihazların depolama kapasitesiyle sınırlandırılmamaktadır (Hiremath ve Mallapur, 2015).

iii. Dinamik Provizyon

Dinamik provizyon, kaynak planlamasının, yapılandırılmasının ve kullanıcıya kaynak sağlanmasının verimli bir şekilde gerçekleştirilmesidir. Uygulamaların yüksek performans göstermesi amacıyla yazılım ve donanım kaynaklarının seçilmesi, geliştirilmesi, yürütülmesini kapsamaktadır. Dinamik provizyon ile hizmet sağlayıcı, ihtiyaç duyulduğunda daha fazla kaynak tahsis etmekte ve ihtiyaç duyulmadığında tahsis edilen kaynakları kaldırmaktadır (Fellah ve diğerleri, 2020).

Mobil bulut bilişimin ana özelliklerinden biri de bilgi işlem için gereken kaynakların hareket halindeyken alınabilmesidir. Geleneksel modellerde tedarik kaynakları en yoğun taleplere dayalıyken, mobil bulut bilişim ile dinamik kaynakların sağlanması mevcut taleplere göre verilmekte ve böylece operasyonların maliyeti düşürülmektedir (Alizadeh ve diğerleri, 2013).

iv. Ölçeklenebilirlik

Ölçeklenebilirlik, sistemin artan sayıda kullanıcıyı yönetme yeteneği olarak tanımlanabilmektedir. Mobil bulut bilişimde, öngörülemeyen kullanıcı taleplerini karşılamak için mobil uygulamalar ölçeklendirilebilmektedir. Ayrıca, servis sağlayıcıları da bir hizmeti kolayca ekleyebilmekte ve genişletebilmektedir (Fellah ve diğerleri, 2020).

Mobil bulut bilişim, hizmet sağlayıcılarının dış kaynaklı veri tabanlarını buluta taşımasıyla birlikte, depolama ve ölçeklenebilirlik konularında büyük avantajlar sağlamaktadır. Bu avantajlar, kullanıcılara veri tabanları oluşturma, depolama ve erişim sağlama konusunda önemli bir hizmet sunan "veri tabanı" olarak adlandırılmaktadır. Özellikle Microsoft Azure ve Amazon SimpleDB gibi uygulamalar, bu hizmeti sunan platformlara örnek olarak gösterilmektedir.

Mobil bir sistemdeki bilgi veri tabanının bulut veri tabanına taşınması, önemli bir görev olmasının yanı sıra, bulutun sanal bir prensipte çalışması sayesinde hızlı bir şekilde yeni bir bilgi işlem ortamına adapte olabilmektedir. Bu durum, kullanıcının tüm bilgisayar ortamını kurma zorunluluğunu ortadan kaldırmaktadır. Eğer bilgi işlem ortamını değiştirme ihtiyacı doğarsa, bulutun sunduğu özelleştirilmiş altyapı kolayca kiralanabilmektedir (Alizadeh ve diğerleri, 2013).

v. Çoklu Kiracılık

Çoklu kiracılık, bir sunucu üzerinde çalışan yazılımın birçok kullanıcıya hizmet sunduğu bir özellik olup, bulut bilişim için önemli gereksinimlerden biridir. Donanım kaynaklarının kullanıcılar arasında paylaşılması, maliyet faktörü göz önüne alındığında oldukça verim sağlamaktadır. Bu özellikte, mobil işletim sistemi kullanmak, kaynak gereksinimleri daha küçük olması sebebiyle bir masaüstü işletim sistemi kullanmaktan çok daha etkili olmaktadır (Fellah ve diğerleri, 2020).

Bir bulut sağlayıcının bilgi kaynakları, sanallaştırma modeli veya çoklu kiracılık ile birden çok kullanıcıya hizmet verebilmeleri için bir araya getirilmektedir. Bu birleştirilmiş modelde, kullanıcılar bilgi işlemin fiziksel kaynaklarını, kullandıkları işlemci ile veri tabanı gibi kaynakların oluşumu, konumu ve orijinalliği hakkındaki bilgileri görememektedir. Örneğin, kullanıcılar verilerinin bulutta tam olarak nerede saklandığını bilmemektedirler (Alizadeh ve diğerleri, 2013).

vi. Entegrasyon Kolaylığı

Bulut ve internet ile talep üzerine kullanıcılara sunulmak için çeşitli sağlayıcılardan gelen birçok hizmet entegre edebilmektedir. Sistem altyapısına, gelişmekte olan sanallaştırma teknolojilerine dayalı olarak, isteğe bağlı, enerji tasarruflu, esnek ve güvenilir hizmetlerin entegrasyonunu basitleştirmektedir (Alizadeh ve diğerleri, 2013).

1.5.2 Mobil Bulut Bilişimin Dezavantajları ve Riskleri

Mobil bulut bilgi işlemin temel amacı, kullanıcılara mobil cihazlarını kullanarak hareket halindeyken buluttaki verilere erişmenin kolay ve hızlı bir yolunu sağlamaktır. Kullanıcının rahatlığını artırırken, mobil bulut bilişim kendi içerisinde birçok sorun barındırmaktadır.

i. Performans Sınırlaması:

Bulut bilgi işlem kullanan mobil cihazlardan bahsederken, dikkat edilmesi gereken ilk unsur kaynak kısıtlamalarıdır. Mobil cihazlar, depolama kapasitesi, ekran boyutu, CPU performansı, kablosuz iletişim ve işletim sistemleri gibi birçok açıdan ilerlemiş olsalar da karmaşık uygulamaları yüklemek için sınırlı bilgi işleme yeteneği ve enerji kaynaklarıyla karşılaşmaktadır.

Enerji, mobil cihazlarda kendiliğinden geri yüklenemeyen kaynak olmakla birlikte yenilenmesi için dış kaynaklara ihtiyaç duyulmaktadır. Enerji tüketiminin azaltmak

ve yerel mobil kaynakları korumak için uygulama hesaplama boşaltma yaklaşımları önerilse de gerçek kullanım senaryolarında kayda değer bir enerji tasarrufu sağlanamamıştır. Akıllı telefonlar hızla gelişirken, mobil bulut bilgi işlem için halen bir kısıtlama olan sınırlı kaynak ömrü devam etmektedir. Enerji tasarrufu sağlanabilmesi amacıyla kullanıcı deneyimi düşürülmektedir (Aery, 2016).

ii. Bağlantı:

Mobil bulut bilişimdeki bir diğer zorluk ise kullanılan farklı mekanizmaları arasında bağlantının sürdürülmesidir. Mobil bulut bilgi işlem ortamındaki veri aktarım hızı sürekli değişmekte ve internet servis sağlayıcısı normalde mobil cihaz kullanıcılarından uzakta olduğundan bağlantı kesintili olarak gerçekleşmektedir. Uygulama hacminin dinamik olarak değiştirilmesi, kullanıcıların hareketliliği ve hatta hava durumu gibi diğer bazı sorunlar, bant genişliği ve ağ çakışmasında değişikliklere yol açmaktadır. Bu nedenle, mobil ağdaki geçiş gecikmesi, kablolu ağdakinden çok daha yüksek olacaktır (Aery,2016).

Kesintisiz bağlantı eksikliği, yani kullanıcı deneyimini önemli ölçüde bozan sık oturum kesintileri nedeniyle uygulama yürütme süresi ve mobil enerji tüketimi artmaktadır. Bu yüzden mobil bulut bilişimin potansiyelinin tam olarak ortaya çıkması için bu tür sorunların üstesinden gelen sistemlerin geliştirilmesi gereklidir. Doğası gereği, mobil cihazlar, kablolu şebekelere kıyasla sınırlı bant genişliğine sahiptir. Kullanıcıya iletilen sinyalin kalitesi uygulamaların yürütülmesindeki orantısız gecikmeden, her zaman açık bağlantının devre dışı bırakılmasından ve sınırlı mobil kaynakların aşırı kullanımından etkilenmektedir (Allam ve diğerleri, 2017).

Mobil bulut bilişimde cihazlar genellikle kablolu şebekelere kıyasla düşük bant genişliğine sahip, kesintili ve daha az güvenilir iletim zeminine sahip kablosuz şebekeler kullanmaktadır. Sürekli bağlantının kesilmesi, sınırlı kaynakların büyük ölçekte kullanılması ve sık uygulama yürütme gecikmeleri, hizmet kalitesinin düşmesine neden olan en önemli sorunlardan bazıları olarak yer almaktadır (Fellah ve diğerleri, 2020).

Düşük bant genişliğine yönelik çeşitli çözüm önerileri de bulunmaktadır.

- **Yeni nesil mobil haberleşme teknolojileri:** 5N gibi teknolojiler ile beraber hızlı veri aktarımı, düşük gecikme süreleri ve geniş bağlantı kapasitesi gibi özellikler bakımından dijital iletişim alanında büyük bir dönüşüm gerçekleşmesi beklenmektedir. Ayrıca, bu tür teknolojilerin enerji tüketiminde de önemli ölçüde düşüş sağlaması ve sürücüsüz araçlar, sanal gerçeklik, artırılmış gerçeklik, akıllı evler ve uzaktan cerrahi operasyonlar gibi çeşitli dikey sektörlerde önemli rol oynaması öngörülmektedir. Ancak söz konusu teknolojiler uygulama maliyeti, şebekelerin aşırı kalabalıklaşması gibi bir dizi sorun da barındırmaktadır.

- **Femtocell:** Evde veya küçük işletmeler gibi görece dar alanlarda kullanılmak üzere tasarlanan küçük, düşük güçlü bu hücresel baz istasyonları servis kapsamını genişletmek için kullanılmaktadır. Mobil iletişim hizmetleri sunan Hay Systems Limited (HSL) adlı bir işletme, mobil operatörler için ekonomik, ölçeklenebilir ve güvenli bir ağ sağlamak üzere femtocell'ler ile bulut bilişimi birleştiren bir teknoloji üzerinde çalışmaktadır. Yürütülen projede, femtocell ağı üzerinden mobil hizmetlerin sağlanması için kullanılan kaynakların, hizmetlere yönelik kullanıcı taleplerine göre genişlemesine veya daralmasına izin verilmektedir. Böylece herhangi bir noktada yalnızca yeterli kaynakların kullanıldığı, talepleri karşılamak için anında ölçeklendirme yeteneğini etkilemeyen oldukça ekonomik bir femtocell ağı sunulmaktadır. Kullanıcıların evlerinde ve ofislerinde bulunan femtocell'ler, operatörlerin ağına erişim elde etmek için internet aracılığıyla buluta bağlanmaktadır. Mobil operatörler ise bulutla bağlantı kurarak abonelerinin buluta bağlı bir femtocell kullanırken kendi ağlarına erişmelerini sağlamaktadır. Bununla birlikte, mobil bulut bilişim kapsamında femtocell kullanıma yönelik çalışmalar ve performans etkisini hala araştırılmaktadır (Jalan ve Bgahat, 2014).

iii. Mobil Cihazların Bireyselleştirilmesi:

Günümüzde çeşitli elde taşınır işletim sistemleri bulunmakta ve elde taşınır cihaza dayalı bir uygulama geliştirmek için uygulama yazılımının istemci tarafı basitleştirilmelidir. Kısaca bu durum, basit istemci ucunun büyük miktarda veri hesaplamanın bulut ile yapılabilmesini ve istemci tarafının, çok fazla değişiklik yapmadan herhangi bir mobil cihazda çalışabilmesi için standart hale getirilmesi anlamına gelmektedir (Aery, 2016).

iv. Kullanıcı Arayüz Sorunları:

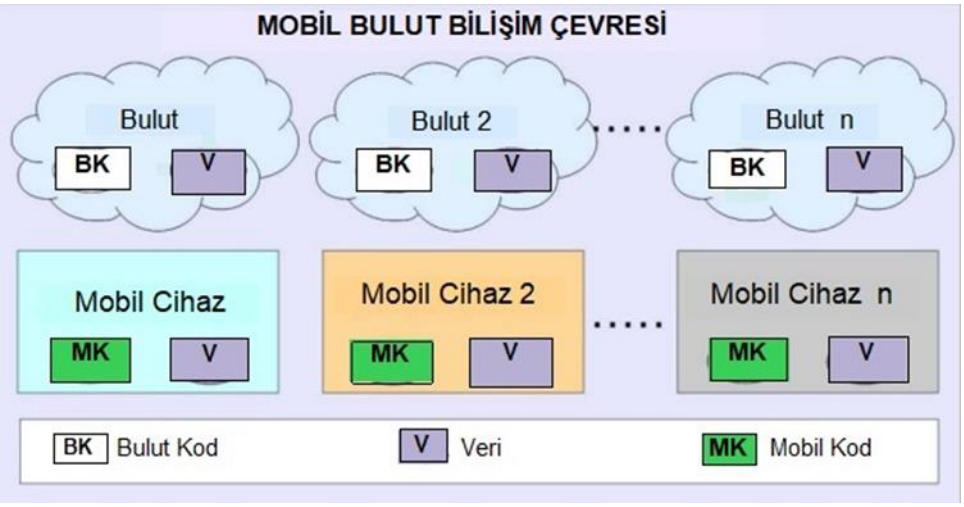
Mobil cihazların boyutları nispeten küçüktür. Bu yüzden çoğu uygulamada, durum çubukları, açılır menüler ve simgeler gibi birkaç statik ögeye sahip arabirimler kullanılmaktadır. Bu tür arabirimler kullanıcı dostu olmakla birlikte, statik ögeler içermeyen kolay arabirimler tasarlamak, çok daha fazla teknik bilgi gerektirmektedir. Başka bir dezavantaj ise ekran boyutu nedeniyle azalan yazma hızıdır (Allam ve diğerleri, 2017).

v. Heterojenlik:

Mobil bulut teknolojisinde, mobil cihazlar, bulutlar ve kablosuz ağlar kapsamında çeşitli donanım, mimari, altyapı ve teknolojileri sunulmakta; farklı kablosuz şebekelerin entegrasyonu, erişim teknolojileri, mimariler, protokoller, kullanıcı hareketliliği ve hizmet gereksinimlerindeki heterojenlik nedeniyle mobilite yönetimi oldukça zorlaşmaktadır. Mobil bulut bilişim, kablosuz ağ üzerindeki farklı arayüzlerden farklı kablosuz teknolojilere kadar uzanan heterojen bir ortamda yürütülmektedir. Bu heterojenliğin, mobil cihazların enerji kullanımında verimli olma, her zaman bağlı olma ve isteğe bağlı kablosuz bağlantının ölçeklenebilirliği gibi sunulması beklenen faydaların yerine getirilememesine neden olacağı değerlendirilmektedir (Allam ve diğerleri, 2017).

Çok sayıdaki heterojen mobil ve bulut işletim sistemi, programlama dili, API'ler ve veri yapıları, mobil bulut bilişimin etki alanını dağıtmakta ve çeşitli bilgi işlem varlıkları arasında taşıma içeriklerini yüklemektedir. Şekil 1.17'de, mobil bulut bilişimdeki, bulut bileşenlerinin bir buluttan diğer bulutlara ve mobil bileşenlerinin bir akıllı telefondan diğer akıllı telefonlara taşınması ile heterojen bulutlar arasındaki veri taşıma yöntemleri gösterilmektedir (Abolfazli ve diğerleri, 2015).

Şekil 1.17 Mobil Bulut Bilişimde Taşınabilirlik



Kaynak: Abolfazli ve diğerleri. 2015

Mobil cihazlar ve bulut sunucuları arasındaki donanım ile mimari heterojenlik, mobil cihazlarda bulut kaynakları ve hizmetlerinin doğrudan dağıtımını engellemekte ve aşağıdaki gibi bazı sorunlara yol açmaktadır;

- **Dengesiz kalite ve performans:** Bilgi işlem kaynaklarındaki ve uygulamalardaki zenginlik, bulut hizmetlerinin performansını ve kalitesini artırmaktadır. Bu tür bir varyasyon, hizmetlere yönelik iş rekabetini tetikleyip, çeşitli iyileştirilmelerin yapılmasını teşvik etse de bulut bilişim sağlayıcıları arasındaki ticari iş birliğini olumsuz etkilemekte ve kullanıcının mevcut seçenekler arasından en uygun satıcıyı seçme konusunda karar vermesini zorlaştırmaktadır.

- **Veri yönetimi ve bütünlük**: Çok büyük ölçekli, coğrafi olarak dağıtılmış veri ambarlarının artan sayısı ve veri yapılarının birbirine benzememesi, veri yönetimini zorlaştırmaktadır. Devasa büyüklükteki dağıtılmış verilerin entegre edilmesi ve mobil kullanıcılar için birleşik depolama sağlamak, mobil bulut bilişimde teknolojisindeki heterojenlik ile daha da karmaşık hale gelmektedir.

- **Taşınabilirlik:** Kodlar, teknolojideki heterojenlikten dolayı ana bilgisayarlarda kolayca taşınamamakta ve yürütülememektedir. Bu durum, geliştiricilerin "bir kez yaz, her yerde çalıştır" ayrıcalığını ellerinden almaktadır. Örneğin, dört çekirdekli işlemci için yazılan uygulama, mimari ve donanımsal farklılıklar nedeniyle çift çekirdekli işlemcide çalıştırılamamaktadır. Benzer şekilde ARM mimarisi için geliştirilen uygulamalar, kod değişikliği ve yeniden yapılandırma olmadan x86 üzerinde yürütülememektedir.

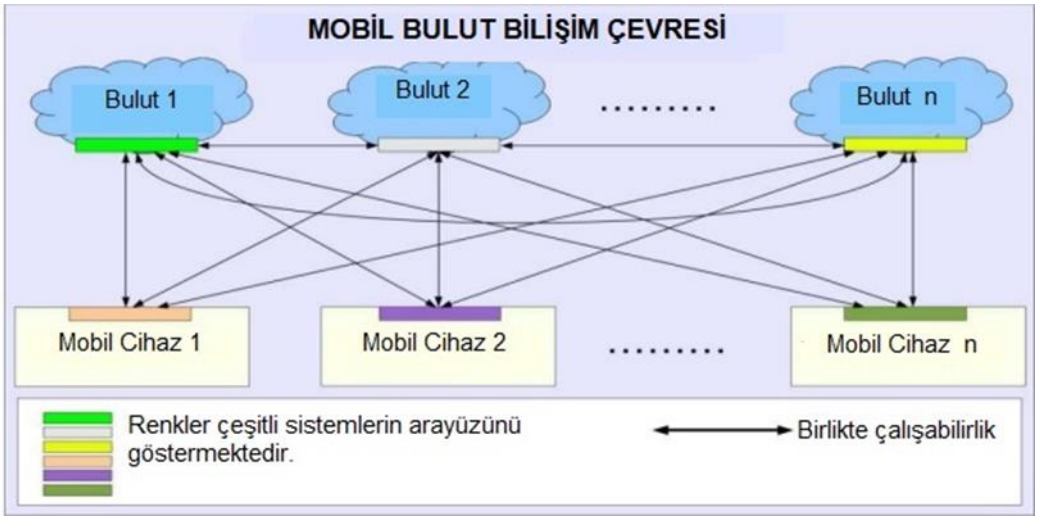
- **Platform heterojenliği:** Mobil bulut bilişim'de çeşitli işletim sistemleri, programlama dilleri ve veri yapıları bulunmaktadır. Hâlihazırda Google'ın Android'i ve Apple'ın iOS'u gibi her biri birden çok sürüme sahip çok sayıda heterojen mobil işletimleri, farklı programlama dili ve veri yapılarını desteklemektedir. Örneğin, Android Java dili, JNI ile yerel kod ve C/C++ sunarken, iOS Objective-C'yi desteklemektedir. Bu tür bir heterojenlik, bulut mobil kullanıcıları ve uygulama geliştiricileri için bir engel oluşturmaktadır. Bu nedenle, mobil bulut bilişim alanında taşınabilirlik ve veri bütünlüğü sorunları daha da artmaktadır. Bu durum, verileri farklı bulut ortamlarına taşımak için ek maliyetlerin ortaya çıkmasına neden olmaktadır. Bu maliyet, mevcut buluttan veri indirilmesini, gerekli değişiklikleri yapmayı ve dönüştürmeyi içermekte; ardından verilerin yeni buluta yüklenmesi sürecini kapsamaktadır. Özellikle kurumsal mobil kullanıcılar, hassas verilere sahip oldukları için heterojen bulutlar arasında büyük miktarda veri aktarımı yapmanın getirdiği maliyetli, zaman alıcı ve riskli zorluklarla

karşılaşabilmektedirler. Bir bulut veritabanında saklanan milyonlarca kayıt, dosya sistemleri ve şifreleme teknikleri arasında bir fark olduğunda, gizlilik ve bütünlükten ödün verilmek zorunda kalınabilmektedir (Sanaei ve diğerleri, 2014).

vi. Birlikte Çalışabilirlik Eksikliği

Şekil 1.18'de gösterilen mobil bulut bilişim'de birlikte çalışabilirlik; bulutlar arası, mobil cihaz-bulut ve mobil cihazlar arasındaki API ile veri yapılarıyla olan iş birliğini ifade etmektedir.

Şekil 1.18 Mobil Bulut Bilişimde Birlikte Çalışılabilirlik



Kaynak: Abolfazli ve diğerleri, 2015

Birlikte çalışabilirlik, mobil kullanıcıların bulutla etkileşime girmesi ve iletişim kurması gerektiğinde önemli bir sorun haline gelmektedir. Mobil kullanıcılar ve bulut arasındaki mevcut arayüz çoğunlukla web arayüzlerine dayanmaktadır. Ancak, web arayüzlerini kullanmak, mobil bulut bilişim için genellikle uygun olmamaktadır. Çünkü web arayüzü özellikle mobil cihazlar için tasarlanmamakta ve bu durumda arayüz çok daha fazla ek yüke sahip olabilmektedir. Ayrıca, web arayüzü ile mobil cihazlar arasında uyumluluk sorunu da çıkabilmektedir (Jalan ve Bhagat, 2014).

Mobil bulut bilişim alanında birlikte çalışabilirlik eksikliği, kullanıcı verilerini ve uygulamalarını belirli bir bulut içinde kilitleyen satıcı kilitleme (vendor lock-in) sorununu doğurmaktadır. Satıcı kilitleme sorunu, temel mimariler ve programlama dilleri arasındaki farklılıklar nedeniyle kodun ve verilerin bir buluttan diğerine taşınamadığı durumlarda ortaya çıkmaktadır.

Verilerin birlikte çalışması, farklı sistemleri birbirine bağlama (kablolu veya kablosuz tabanlı), coğrafi bilgi kaynaklarını anlama ve iki veya daha fazla heterojen sistem arasında bilgi alışverişi yapma yeteneğidir. Bununla birlikte, MCC altyapısındaki bulutlar arasındaki çeşitlilik, kablolu ve kablosuz şebeke donanım sistemleri, bulut ile mobil altyapılar arasındaki farklılıklar, arayüz standartlarının olmayışı veri entegrasyonu ve birlikte çalışma sorunları oluşturmaktadır (Sanaei ve diğerleri, 2014).

Kullanıcılar hizmet sağlayıcılarını değiştirdiğinde (genellikle kalite ve maliyet sorunları nedeniyle), içerik, kodlar ve verilerin taşınması ile bunların eski sağlayıcıdan yeni bulut sağlayıcısına iletilmesi yüksek maliyetlere neden olmaktadır. Ayrıca, dönüştürme ve iletim sırasında kod ve veri bozulması riskleri de MCC'deki bulut tüketicilerini tehdit etmektedir. MCC'de birlikte çalışabilirliğin sağlanabilmesi ve kesintisiz hizmetin sunulabilmesi için standart protokoller ile Açık Bulut Bilişim Arayüzü gibi ortak API'ler gerekmektedir (Abolfazli ve diğerleri, 2015).

vii. Mobil Bulut Yakınsama

Bulut bilişimi mobil dünyaya entegre ederek mobilite avantajı sağlayan mobil bulut bilişimde veri dağıtımı ana konudur. Mobil cihazların sınırlı bilgi işlem güçleri, görevlerin etkili bir şekilde dağıtılmasını önemli kılmaktadır. Çünkü mobil cihazların bilgi işlem gücü, ana bilgi işlem platformu olması için yeterince güçlü değildir. Mobil bulut yakınsaması performans artışı, daha uzun pil ömrü ve hesaplama gücü sorunlarına çözüm getiren bir yaklaşımdır. Temel prensip, uygulamanın bulutta daha fazla hesaplama gerektiren bölümlerde çalışmasını sağlamak ve kullanıcı arayüzü ile ilişkilendirilmiş kısımları mobil cihazda çalışacak şekilde bölümlere ayırmaktır. Bu yaklaşım, bir sürecin bölünmesiyle gerçekleştiği için, işlemler arası iletişim, bu

yakınsamayı başarmak için kritik bir rol oynamaktadır. Kablosuz teknolojiler, gelişmiş elektronik cihazlar ve interneti entegre ederek, bilgi işleminin yaygın ve her yerde erişilebilir olmasını sağlamaktadır (Chavan ve Rajani, 2013).

viii. Güvenlik ve Gizlilik

Mobil bulut bilişimin karşılaştığı en önemli sorunlardan biri veri güvenliğidir. Mobil cihazlarla ilgili fiziksel güvenlik kaybı, şifreleme ve şifre çözme anahtarlarının işlenmesi, sanal makinelerin güvenlik ve denetim sorunları ile çeşitli kaynakların hizmet platformu uyumsuzluğu da dâhil olmak üzere birtakım güvenlik endişeleri bulunmaktadır. Ayrıca, verilerin buluta aktarılması da veri güvenliği ve mahremiyetiyle ilgili çeşitli riskler barındırmaktadır (Allam ve diğerleri, 2017).

Mobil kullanıcıların bilgilerinin servis sağlayıcı tarafında bulunan bulutlarda saklanması ve işlenmesi; veri kaybı, veri ihlali, veri kurtarma, veri yerelliği ile veri gizliliği gibi önemli güvenlik riskleri barındırmaktadır. Özellikle gizlilik, mobil kullanıcıların verilerini veya uygulamalarını işlerken ve mobil cihazlardan heterojen dağıtılmış bulut sunucularına iletilirken, bulut hizmetlerini kullanmak için önemli bir zorluk olarak ortaya çıkmaktadır. Bulut sunucuları farklı yerlerde bulunmakta ve hizmet sağlayıcılar tarafından korunulmakta olup, gizlilik kaybından kullanıcılar sorumlu olmamaktadır. Öte yandan, kullanıcı verileri buluta aktarıldıktan sonra, bulut sağlayıcı tarafındaki yetkili kişilerin bu verilere sınırlı erişimi olacağına dair bir garanti olmalıdır. Müşterinin özel verilerine personel tarafından uygunsuz erişim, bulut verileri için potansiyel tehdit oluşturabilecek başka bir risk olarak yer almaktadır. Kullanıcılara veri güvenliği konusunda güvence vermek için uygulamalar, gizlilik politikaları ve prosedürleri mevcut olmalıdır.

Ayrıca kötü amaçlı yazılım da internet bağlantılarının kullanılabilirliğine yönelik bir tehdit olarak ortaya çıkmaktadır. Genel olarak, kötü amaçlı yazılım, spam ve e-posta kimlik avı dâhil olmak üzere internet güvenlik ihlalleri mobil bulut bilişimin gizliliğine yönelik en yaygın risklerdir. Bu kapsamda mahremiyeti korumak ve güvenliği sağlamak adına literatürde birçok çalışma yapılmıştır.

Mobil bulut bilişimdeki diğer bir güvenlik problemi ise boşaltma işleminde görülmektedir. Boşaltma işlemi, kullanıcı verilerinin ihlal edilmesi ve kişisel bilgilerin çalınma riski taşımakta, kişilerin önemli bilgilerinin sabote edilmesi veya çalınması amacıyla gerçekleştirilen kasıtlı müdahalelere dair endişelere neden olmaktadır (Allam ve diğerleri, 2017). Ayrıca bu işlem, kablosuz ağlar aracılığıyla buluta erişim gerektirmekte, ancak mobil kullanıcıların bu boşaltma işlemleri üzerinde erişimi veya kontrolü bulunmamaktadır. Dolayısıyla bu durum yüklenen içeriğe yetkisiz erişim riskini artırmaktadır.

Bununla birlikte boşaltma işleminin, içerik bütünlüğünü ve gizliliğini ihlal etme, bölümleme sırasında veri, uygulama ve mobil cihaz arasında sıkışma ile bulut hizmetlerinin kullanılabilirliğini tehdit etme potansiyeli de bulunmaktadır. Bunun nedeni, boşaltma içeriğine ilişkin yürütme işlemlerinin mobil cihaz yerine bulutta yapılmasıdır. Güvenli boşaltma süreçleri sağlayarak, bu riskleri azaltmak için mobil bulut bilişime uyarlanabilir bir uygulama bölümleme ve güvenli boşaltma algoritmaları önerilmiştir (Al-Janabi ve diğerleri, 2017).

2 MOBİL BULUT BİLİŞİMİN KULLANILDIĞI SEKTÖRLER VE ÖRNEK UYGULAMALAR

Günümüzde depolama, öğrenme ve eğitim, sosyal ağlar gibi birçok alanda kullanılan bulut bilişim uygulamaları mobil kullanıcılar tarafından kullanılmaktadır. Bulut tabanlı geliştirilen bu uygulamalar, mobil kullanıcı taleplerini ve mobil cihaz kapasitesini karşılamak için üretilmektedir. Bu uygulamaların temel amacı, mobil kullanıcılara, sınırlı kaynaklı mobil cihazlardan bile buluttaki mevcut hizmetlere erişim sağlamaktır.

Bir mobil uygulamayı buluta boşaltmak için uygulamanın parçalara bölünmesi gerekmektedir. Bu bölümler, ihtiyaçlarına göre istemci tabanlı, istemci bulut tabanlı ve bulut tabanlı modeller olmak üzere üç ana türe ayrılmaktadır. İstemci tabanlı modelde, uygulamanın yürütmesini tutmaktan mobil cihaz sorumludur. İstemci-bulut tabanlıda ise uygulama bileşenlere bölünerek; bu bileşenler, mobil cihaz ve uzak bulut tarafından yürütülmektedir. Ayrıca bulut, uygulamanın çalışabileceği, işleyebileceği ve depolayabileceği bir uygulama parçası olarak tanımlanmaktadır (Al-Janabi ve diğerleri, 2017).

Geleneksel mobil bilgi işlem teknolojilerinden farklı olarak, mobil bulut bilişimdeki kaynaklar sanallaştırılmakta ve yerel bilgisayarlar veya sunucular yerine çok sayıda dağıtılmış bilgisayar grubuna atanmaktadır. Google Gmail, mobil telefonlarda kullanılan haritalar ve navigasyon sistemleri, Apple iCloud, Microsoft Live Mesh ve Motorola Motoblur gibi mobil bulut bilişim tabanlı birçok uygulama geliştirilerek kullanıcıların hizmetine sunulmuştur (Gupta ve Gupta, 2012).

2.1 Mobil Bulut Bilişimin Kullanım Alanları

Son yıllardaki şebeke teknolojilerindeki gelişmeler her yerde bilgi işlem hayalini gerçeğe dönüştürmüştür. Bu teknolojik gelişmeler, e-öğrenme, e-ticaret, e-sağlık ve internet oyunları gibi ortaya çıkan bir dizi e-uygulama için itici bir güç sağlamış; kullanıcılar, mobil cihazlarının da bilgisayar sistemlerinde çalışan benzer

uygulamalarla aynı performans düzeyinde çalışmasını beklemişlerdir. Ancak, mobil cihazlar, aynı düzeyde kullanıcı deneyimi sağlayamayan, kaynakları kısıtlı cihazlardır. (Ahmed ve diğerleri, 2015).

Mobil şebekelerin ve cihazların kullanımının artması, şebeke kapasitesinde bir artışa yol açmış ve mobil cihazlar önemli hesaplama yeteneklerine ulaşmıştır. Diğer taraftan, mobil bulut bilişim alanındaki artan gelişmelerle de mobil uygulamalar, küresel mobil pazarda artan bir pay kazanmıştır. Mobil bulut bilgi işlem uygulama alanlarından bazıları aşağıda yer almaktadır.

2.1.1 Ticaret Sektörü

M-Ticaret, mobil cihazlar üzerinden ticaret yapılan bir iş modelidir. Kablosuz teknoloji ile ticaret yapabilme olanağı sağlamak için geliştirilmiş olup, genel olarak m-ticaret uygulamaları finans, bankacılık, alışveriş ve reklamcılığı içeren birkaç kategoriye ayrılmaktadır (Aery, 2016).

Günümüzde kişiler finansla ilgili faaliyetleri genellikle akıllı telefonlarından yürütmeyi tercih etmektedir. Mobil bulut, güçlü bilgi işlem kaynaklarıyla donatılmış olması nedeniyle, para transferi ve banka ödemesi gibi çeşitli finansal davranışları destekleyebilmektedir. Dünya çapındaki birçok banka mobil çevrim içi bankacılığı uygulamaya koymuştur. Mobil bankacılık uygulamaları, kullanıcılarının, hesap bakiyesini kontrol etmelerine, tek seferlik güvenlik giriş kodu oluşturmalarına veya ödeme/banka havalesi yapmalarına olanak tanımaktadır (Au, 2017).

M-ticaret sayesinde bankalar ve diğer finansal kuruluşlar, kullanıcılarının hesap bilgilerine erişmesi, hisse senedi satın alması, para ödemesi vb. işlemleri gerçekleştirmesine olanak tanımaktadır. Mobil reklam, cep telefonlarına gönderilen reklamlar olmakla birlikte, şirketler, mobil pazarlama kampanyaları yoluyla geleneksel kampanyalara göre daha iyi yanıt aldığını bildirmiştir. Bu durum gelecekte mobil reklamcılığın, sektöründeki yerini sağlamlaştıracağını göstermektedir (Aery, 2016).

2.1.2 Sağlık Sektörü

Sağlık hizmetleri ortamlarında mobil bilgi işlem cihazları, verilere daha hızlı ve daha basit erişim sağlayarak hastalara daha iyi bakım sağlanmasına yardımcı olmaktadır. Mobil sağlık hizmeti (m-sağlık), kablosuz teknoloji ile hastaların her zaman, her yerde izlenmesini sağlamakta ve bazı mobil cihazlar, acil durum sistemini uyarmak için nabız hızı ile kan basıncını algılayabilmektedir. Ayrıca m-sağlık hizmetleri, hastaların veya diğer sağlık hizmeti kuruluşlarının mevcut ve geçmiş tıbbi verilere kolaylıkla erişilmesine de olanak tanımaktadır. Mobil bilgi işlem cihazları, elektronik sağlık sistemleriyle bağlantı kurarak daha fazla hizmetin daha verimli ve daha düşük hata oranıyla erişilmesine izin verirken, daha fazla boş alan, daha az karmaşa ve daha düşük maliyetler sunmaktadır (Aery, 2016).

Mobil bulutun tıbbi uygulamalarda kullanım amacı, geleneksel uygulamaların sınırlamalarını (küçük fiziksel depolama alanı, güvenlik, mahremiyet ve tıbbi hatalar gibi) en aza indirmektir. M-sağlık, kullanıcıların hasta sağlık kayıtları gibi kaynaklara kolay ve verimli bir şekilde erişmeleri için yardım sağlamaktadır. Ayrıca m-sağlık'ta, yerel sunucularda yer alan bağımsız uygulamalar yerine hastanelere ve sağlık kuruluşlarına bulut üzerinde isteğe bağlı çeşitli hizmetler de sunulmaktadır. Mobil sağlık hizmetlerinin sunduğu beş ana avantaj aşağıda yer almaktadır.

- Genişbant kablosuz iletişim yoluyla sağlık izleme hizmetleri, hastaların her zaman ve her yerde izlenmesini sağlamaktadır.
- Akıllı acil durum yönetim sistemleri ile kazalardan veya olaylardan gelen çağrıları alırken acil durum araçları kolayca yönetilebilmekte ve koordine edebilmektedir.
- Mobil cihazlar ile nabız hızı, kan basıncı ölçülerek, acil durumlarda sağlık görevlilerine haber verilebilmektedir.
- Sağlık bilgilerine kapsamlı erişim ile hastaların veya sağlık hizmeti sağlayıcılarının mevcut ve geçmiş tıbbi bilgilere erişmesine izin verilebilmektedir.
- Sağlık harcamalarını ödemek veya ilgili masrafları otomatik olarak yönetmek için kullanılabilmektedir.

Bir m-sağlık örneği olarak, Tayvan'da özellikle hipertansiyon ve diyabetli hastalar için katılımcıları izlemek üzere tele-tıp evde bakım yönetim sistemi uygulanmıştır. Sistemde 300 katılımcı izlenmiş ve 4736'dan fazla kan basıncı ve şeker ölçümü kaydı bulutta depolanmıştır. Kullanıcı kan şekeri/basınç ölçümü yaptığında, ölçülen parametreler otomatik olarak sisteme iletilmiştir. Ayrıca kullanıcı mobil cihazları üzerinden kısa mesaj servisi (SMS, Short Message Service) ile söz konusu verileri de gönderebilmiştir. Ek olarak buluta kaydedilen kullanıcı sağlık verileri bilgileri toplanıp analiz edilmiş ve analiz sonuçları gösterilmiştir. Ancak kişisel sağlıkla ilgili toplanan ve yönetilen bilgilerin hassas olması nedeniyle güvenliğin sağlanması, veri koruması ve mahremiyet konuları büyük önem taşımaktadır (Dinh ve diğerleri, 2011). İlgili konular çalışmanın 4. bölümünde ele alınmaktadır.

2.1.3 Oyun Sektörü

Mobil oyun (m-oyun), servis sağlayıcılar için gelir sağlayan, gelişen bir pazardır. Mobil oyun, grafik işleme gibi büyük bilgi işlem kaynakları gerektiren oyun motorunun buluttaki sunucu ile tamamen serbest bırakılarak oyuncuların yalnızca mobil cihazlarındaki ekran arabirimiyle etkileşim kurmasına olanak tanımaktadır. Böylece mobil cihazların enerji tüketiminin azaltılarak, mobil cihazlarda oyun oynama sürelerini arttırmak ve kullanıcı deneyimini en üst düzeye çıkarmak hedeflenmektedir (Aery, 2016).

Mobil oyun uygulamaları görsel/ses efekti ve karmaşık tasarımı, akıllı telefonun pilini ve hafızasını ciddi şekilde tüketmektedir. Mobil bulutun yardımıyla, oyun motoru ya da efekt/yükseltme paketleri tamamen buluta aktarılabilmekte ve bulut, büyük hesaplamalı maliyet algoritmalarını (örneğin, grafik işleme) çalıştırmak için kullanılabilmektedir. Mobil bulut ayrıca, eski sürümün bulutta saklanabilmesi ve yedeklenebilmesi anlamında, mobil kullanıcıların sürüm güncellemesi için daha az depolama alanı tüketmesini sağlayabilmektedir. Ek olarak, bulut tabanlı oyunlar, çevrim içi çok oyunculu arayüzü desteklemekte, böylece birden fazla oyuncu, farklı

fiziksel konumlarda olsalar da aynı oyunda birbirleriyle rekabet edebilmektedir (Au ve diğerleri, 2017).

Mobil oyunlar, servis sağlayıcılar için potansiyel gelir kaynağı olan bir Pazar oluştururken, bulut bilişimin kullanımı büyük bilgi işlem kaynağı gerektiren oyun motorunun yükünü tamamen boşaltarak, kullanıcılara buluttaki sunucu üzerinden cihazlarının sadece ekran arayüzünü kullanarak oyun oynama imkânı sunmaktadır.

Hesaplama boşaltma ile mobil cihazlar için enerji tasarrufu sağlanarak oyun oynama süresi artırılabilmektedir. Ayrıca 3N şebekesi ve WiFi ile oyun uygulamalarında kullanılan enerjinin değerlendirilmesi için birtakım araştırmalar yapılmıştır. Bu kapsamda mobil kodların bir buluta ince taneli (fine-grained), enerji farkındalı olarak boşaltılmasını sağlayan bir sistem olan bellek aritmetik birimi ve arayüzü (MAUI, Memory Arithmetic Unit and Interface) önerilmiştir. MAUI, uygulama kodlarını analiz ederek işlenmek üzere olan tüm kodları buluta boşaltmak yerine, şebeke bağlantısı verildiğinde enerji tasarrufunu en üst düzeye çıkarmak için mobil cihazdaki şebeke iletişimi ve işlemci maliyetlerine dayalı olarak uygulama kodlarını bölümlere ayırmıştır. Deney sonuçlarına göre, MAUI'nin sadece mobil cihazlarda önemli ölçüde (video oyunlarında %27 ve satranç için %45) enerji tasarrufu sağlamakla kalmayıp, aynı zamanda mobil uygulamaların performansını da artırdığı görülmüştür. Özellikle oyunun yenileme hızı gibi faktörlerde olumlu iyileştirmeler gözlemlenmiştir. M-oyun ile iletişim ve bilgi işlem maliyetleri göz önüne alınarak kullanıcı deneyiminin en üst düzeye çıkarılması hedeflenmektedir (Dinh ve diğerleri, 2011).

2.1.4 Eğitim Sektörü

Hareketliliğe dayalı olarak tasarlanan mobil öğrenmede (m-öğrenme), geleneksel uygulamaların teknoloji açısından yüksek maliyeti, düşük şebeke aktarım hızı ve kısıtlı eğitim kaynakları gibi sınırlamaları bulunmaktadır. Bu kısıtları çözebilmek için bulut tabanlı m-öğrenme uygulamaları ele alınmaktadır. Örneğin, büyük depolama kapasitesine ve güçlü işleme yeteneğine sahip olan bulut bilişimi kullanan uygulamalar, öğrencilere büyük veri (bilgi) boyutu, daha yüksek işlem hızı ve daha

uzun pil ömrü gibi çok daha zengin hizmetler sağlamaktadır. Örneğin, öğrenciler ve öğretmenler arasındaki iletişim kalitesini artırmak için makine öğrenimi ile bulut bilişim birleştirilebilmektedir. Bunun için istemcilere açık kaynaklı JavaME UI ve Jaber uygulamalarına dayalı bir akıllı telefon yazılımı kullanılmıştır. Google Apps Engine üzerinde oluşturulmuş bir web sitesi aracılığıyla öğrenciler, öğretmenleriyle her an iletişim kurabilmekte, ayrıca öğretmenler, öğrencinin dersle ilgili bilgi düzeyi hakkında bilgi edinebilmekte ve öğrencilerin sorularını zamanında cevaplayabilmektedir. Ek olarak, mobil artırılmış gerçeklik ortamında etkileşim platformuna dayalı bulut tabanlı bir m-öğrenme sistemi, öğrencilerin öğrenme kaynaklarına uzaktan erişmesine de yardımcı olmuştur. (Dinh ve diğerleri, 2011).

2.1.5 Diğer Kullanım Alanları

Mobil bulut bilişim, mobil kullanıcıların Facebook, Twitter, Instagram gibi popüler sosyal ağ sitelerindeki kişilerle fotoğraf ve video paylaşmasına da yardımcı olmaktadır. Ayrıca mobil kullanıcılara trafik yoğunluk durumu veya yakındaki restoranları bulma gibi konuma dayalı hizmetler sağlayan harita ve diğer navigasyon uygulamalarında da mobil bulut hizmetleri kullanılmaktadır (Aery, 2016).

Mobil bulut bilişim kullanımına başka bir örnek olarak, mobil kullanıcıların gerçek zamanlı deneyimlerini (seyahat, alışveriş ve etkinlik gibi) otomatik bir blog aracılığıyla bulutlar üzerinden paylaşmalarını sağlayan MeLog uygulaması verilmektedir. Mobil kullanıcılar, haritaları gösterme, güzergâh kaydetme, resim ve video depolama gibi çeşitli bulut hizmetleri tarafından desteklenmektedir.

Amazon Web Services bulutu üzerinde çalışan ve çevrim içi çeviri hizmeti sunan One Hour Translation da başka bir mobil bulut bilişim uygulamasıdır. Bu uygulama, mobil kullanıcıların cihazları aracılığıyla kendi dillerine çevrilmiş bilgileri almalarına yardımcı olmaktadır. Mobil kullanıcılar arama hizmetlerine (örneğin, bilgi, konum, görüntü, ses veya video klip arama) ihtiyaç duyduklarında bulut üzerinden yapılan çeviri hizmeti en etkili araç haline gelmektedir (Dinh ve diğerleri, 2011).

Mobil bulut bilişime odaklanan bir senaryoda, doğal afet sonrasında bu teknolojinin kullanımı ele alınmıştır. Örneğin, 2004 yılında meydana gelen Hint Okyanusu tsunamisi gibi bir doğal afetin ardından, acil durum hizmetlerinin sağlanmasının büyük bir öneme sahip olduğu görülmüştür. Bu hizmetler arasında ise kayıp şahısların aranması en kritik ve en zorlu görevlerden biri olarak yer almıştır. Böyle bir kaotik durumda, altyapı yok olmuş, bilgisayarlara ve verilere erişim kısıtlanmış; böylece kayıp şahısların aranması daha da zorlaşmıştır. Bu tarz zorlukların üstesinden gelinebilmesi için, bulunan her kişinin fotoğraflanması, tüm görüntülerin merkezi bir yerde toplanması ve kayıp kişilerin görüntüleriyle arama ile eşleştirme işlemleri yapılması önerilmiştir. Ancak afet sonrası sınırlı insan ve makine kaynakları göz önüne alındığında bu yaklaşım çok gerçekçi olmamıştır. Dağıtık hesaplama ve toplu algılama ile mobil bulut kullanımı çerçevesinde oluşturulan senaryoda gerekli görüntüleri nasıl ve kimin çekeceği, bu görüntülerin nasıl toplanacağı, toplanan görsellerin nasıl işleneceği sorularına değinilmiştir (Fernando ve diğerleri, 2012).

İlk soru, iyi kalitede bir kameralı cep telefonuna sahip olan herkesin buna katkıda bulunabileceği şeklinde cevaplanabilirken, ikinci ve üçüncü sorular verinin toplanması ile işlenmesini kapsadığından cevaplanması daha zordur. Elde edilen verilerin uzak bir sunucuya yüklenmesi bir çözüm önerisi olarak sunulmakta ancak afet bölgeleri çoğunlukla bağlantı sorunu ile karşı karşıya kalmaktadır. Ayrıca, özellikle merkezi bir sunucu düğümü önceden kurulmamışsa, bu yöntem biraz zaman alabilmektedir. Görüntüler yerel olarak işlenebilmekte, ancak mobil cihazlar genellikle bu tür işlemleri (bireysel olarak) gerçekleştirmek için yeterli kaynağa sahip olmamaktadır. Belirtilen senaryo için yerel bir mobil bulut kullanma olasılığı ele alınmıştır. Bu durumda, çeşitli kişiler tarafından çekilen fotoğraflar, kayıp kişilerin eşleştirileceği verileri oluşturmaktadır. Afet bölgesinde birlikte çalışan yardım toplulukları, mobil cihazlarının depolama ve işleme kaynaklarını, kayıp kişileri tespit etmek için gereken görüntü işlemeyi etkili bir şekilde gerçekleştirebilecek bir yerel mobil buluta ödünç vermektedir. Buradaki temel zorluk, mevcut kaynakların sayısının ve türünün önceden bilinememesi veya tahmin edilememesidir. Kapasitenin nasıl verimli bir şekilde dağıtılabileceği ve yükün dengelenebileceği başka bir sorun olarak ortaya çıkmaktadır. Bu gibi durumlarda, cihazların tanıdık cihazlardan ziyade diğer bilinmeyen

düğümlerle karşılaşması muhtemeldir. Bu nedenle, mobil bulutun ön bilgi olmadan da performans artışı sağlayabilmesi önemlidir. Oluşturulan bu senaryo, mobil bulut bilgi işlem çerçevesine duyulan ihtiyacı göstermektedir (Fernando ve diğerleri, 2012).

Mobil bulut bilişimin kullanımına başka bir örnek olarak ise giyilebilir teknoloji alanı verilmektedir. Giyilebilir bilgi işlemlerin hesaplama yeteneklerinin kısıtlı olması ve yeterli pil gücüne sahip olmaması iki temel zorluk olarak yer almaktadır. Sensörler ve çevre birimleri kapsamlı kullanıcı deneyimini kolaylaştırırken, hesaplama işlemlerinin yerel mobil buluta yüklenmesi veya paylaşılması da ifade edilen bu temel problemleri çözmektedir. Ayrıca artırılmış gerçeklik alanındaki benzer sorunların çözülmesi için de mobil bulut kaynaklarının kullanılması önerilmiştir. Mobil bulut teknolojisi Vücut Alan Ağı (BAN, Body Area Network)'nı oluşturan giyilebilir tıbbi cihazların, hastaların verilerinin gerçek zamanlı olarak toplanmasını ve analiz edilmesini sağlayabileceği de ifade edilmiştir (Fernando ve diğerleri, 2012).

Bununla birlikte, mobil bulut bilişim kullanım alanları ve uygulamaları hizmet modellerine göre kategorize edilebilmektedir. Örneğin, MaaSC, en yaygın MCC hizmet modelidir. Çünkü mevcut mobil cihazların çoğu, hesaplama ve enerji kapasiteleri nedeniyle hâlâ kısıtlıdır. MaaSC hizmet türünde kullanılan CloneCloud, mobil cihazlar için hesaplama görevi boşaltma hizmeti sağlamaktadır.

CloneCloud'da akıllı telefon uygulamalarının çalışma hızını artırmak için yakındaki bilgisayarlar veya veri merkezleri kullanılmaktadır. Yaklaşımın temelinde tüm veri ile uygulamaları akıllı telefondan buluta klonlamak ve klonlar üzerinde bazı işlemleri seçici olarak yürüterek, sonuçları akıllı telefona yeniden entegre etmek yer almaktadır. Aynı akıllı telefon için birden fazla klon bulunabilmekte ve klonlar daha güçlü akıllı telefonlar gibi davranabilmektedir. Bu durumda mobil cihaz, diğer kullanıcılara hizmet sağlamak yerine yalnızca bulut tarafından sağlanan hizmetten yararlandığı için hizmet tüketicisi olarak tanımlanmaktadır. Ayrıca her uygulama, bir veya daha fazla mobil bulut bilişim hizmet modeli ve kullanım alanı kapsamında da ele alınabilmektedir. Ancak CloneCloud, yerel durumu (native state) taşıyamaması ve

benzersiz yerel kaynakları (unique native resources) uzaktan dışa aktaramaması nedeniyle bazı açılardan sınırlıdır (Jalan ve Bhagat, 2014).

Mobil bulut bilişim hizmetleri ve örnek uygulamaları aşağıda yer alan Tablo 2.1'de özetlenmektedir.

Tablo 2.1 Mobil Bulut Bilişim Hizmetleri ve Örnek Uygulamaları

KULLANIM ALANI	MCC UYGULAMASI	MCC HİZMET MODELİ		
		MaaSC	MaaSP	MaaSB
Mobil Bulut Hesaplama	CloneCloud	✓		
	MAUI	✓		
	ThinkAir	✓		
Mobil Bulut Depolama	Dropbox, iCloud, Google Drive, Skydrive	✓		
	WhereStore	✓		
	STACEE	✓	✓	
Güvenlik ve Gizlilik	CloudAI	✓		
	Zscaler	✓		
	Google Wallet	✓		
Bağlam Farkındalığı	Mobil Bulut Motoru (MCE)		✓	✓

Kaynak: Jeevan ve diğerleri, 2014

Mobil Bulut Hesaplama

Hesaplama-boşaltma, yoğun kaynak gerektiren hesaplama görevlerini gerçekleştirmek için internet bulutlarına güvenen mobil cihazlar için zorlu bir özelliktir. Enerji tüketimi, işlemci kullanımı ve ağ gecikmesi gibi çeşitli performans ölçütleri dikkate alındığında, hesaplama görevlerini bölümlendirmek ve bunları mobil cihazlar ile bulutlar arasında tahsis etmek, uygulama çalışma süresi boyunca çok verimsiz olabilmektedir. Hesaplama görevlerinin buluta verimli ve akıllı bir şekilde nasıl

yükleneceği, MCC'nin ana araştırma konularından biri olarak ele alınmaktadır. Bu bağlamda, CloneCloud ve MAUI bu alandaki iki öncü proje olarak yer almakta ve her ikisi de bilgi işlem görevlerini otomatik olarak buluta aktarabilmektedir.

CloneCloud, bir uygulama bölümleyicisi olmasının yanı sıra mobil uygulama yürütmelerinin bir kısmını mobil cihazlardan bulut sunucusuna sorunsuz bir şekilde boşaltmasına olanak tanıyan bir çalışma ortamı olarak da hizmet vermektedir. Boşaltma kararı, mobil cihazlar için yürütme süresi ve enerji kullanımı optimize edilerek verilmektedir. CloneCloud'un aksine MAUI ise mobil cihazların enerji tasarrufunu en üst düzeye çıkarmak için kodlama düzeyinde boşaltma uygulamalarının değiştirilmesine izin vermektedir. Mobil bulut hesaplamaya yönelik bir diğer uygulama olan Thinkair'de ise akıllı telefon sisteminin bir parçası olan bulutlarda, özel sanal makineler (VM'ler) talep edilmekte ve çevrim içi yöntem düzeyinde boşaltma yapılarak uygulamalar/girdi/çevre koşulları üzerindeki kısıtlamalar kaldırılmaktadır (Jeevan ve diğerleri, 2014).

Mobil Bulut Depolama

Depolama kapasitesi, mobil cihazların başka bir kısıtlaması olmakla birlikte bu cihazlar için Dropbox, iCloud, Google Drive ve Microsoft Skydrive gibi birçok mevcut depolama hizmeti bulunmaktadır. Dosyaları veya verileri buluta elle yüklemenin yanı sıra, mobil bulut depolama hizmetlerinin istenen bir özelliği de mobil cihazlar ile bulut arasında otomatik senkronizasyon olmasıdır. Mobil cihazlar tarafından üretilen multimedya verileri, istikrarlı ve yüksek oranda kullanılabilir bir depolama çözümü gerektirmektedir. Bu yüzden birçok akıllı telefon işletim sistemi multimedya veri senkronizasyon özelliğini yerel olarak (iOS için iCloud, Windows Phone için Skydrive, Android için Google Drive vb.) yerleştirmektedir. Ayrıca, konum izleri, tarama geçmişi, kişiler ve tercih ayarları gibi mobil kullanıcıların davranış verilerinin güvenilir ve korumalı bir depolama alanında tutulması da gerekmektedir. Bu bağlamda, mevcut ticari bulut depolama çözümlerinin çoğu, internet bulutları için uygun olan merkezi bir veri merkezi üzerine kuruludur.

Depolama hareketliliği, giderek güncel bir araştırma odağı haline gelmektedir. Bu kapsamda, araştırmacılar, WhereStore adlı akıllı telefonlar için konum tabanlı bir veri depolama çözümü önermektedir. Veri ögelerini akıllı telefonlar ve bulut arasında dağıtmak için her cihazın konum geçmişiyle birlikte filtrelenmiş çoğaltmayı (yakın gelecekte erişilmesi muhtemel veri öğeleri kümesini ifade eden bir filtre) kullanmaktadır. Bununla birlikte STACEE'de, mobil cihazlara bir P2P bulut depolama çözümü sağlanmakta ve QoS ise bir planlama sorunu olarak mobil depolamada ele alınmaktadır. (Jeevan ve diğerleri, 2014).

Güvenlik ve Gizlilik

Güvenlikle ilgili hizmetler sayesinde bulut aracılığıyla veri güvenliğinin korunması amaçlanmaktadır. Mobil cihazların güvenliği, bulut tabanlı güvenli proxy, uzaktan antivirüs, uzaktan tasdik vb. dâhil olmak üzere bulut güvenlik mekanizmasının yardımıyla geliştirilebilmektedir. Bu doğrultuda, literatürde CloudAV, bir bulut içi güvenlik hizmeti olarak antivirüs sağlayarak bilgisayarlar için kötü amaçlı yazılım tespitinde kullanılan bulut tabanlı güvenlik modeli yer almaktadır (Jeevan ve diğerleri, 2014).

Güvenli web yönlendirme hizmetleri, bulut aracılığıyla virüsten koruma ve kimlik avı önleme hizmetlerini etkinleştirmektedir. Yönlendirme hizmetleri mobil kullanıcıların kimlik avı yapan web sitelerine erişmesini önlemek için bir mobil cihaz tarafından erişilen URL'lerin doğrulanması için güvenli bir arama motoruna bağlıdır. Bu kapsamda, mobil cihazlar için ilke tabanlı güvenli internet erişimi sağlayan ve ticari bulut tabanlı güvenlik şirketlerinden biri olan Zscaler, üç ana bileşen içeren bir bulut tabanlı güvenlik çözümü sunmaktadır. Bu çözümde, ZEN (proxy), merkezi otorite ve Nanologs sunucusu (kayıt sunucusu) bileşenlerine dayalı olarak çeşitli bulut tabanlı güvenlik hizmetleri oluşturulmaktadır. Örneğin, ByteScan adlı hizmet, virüsler, siteler arası komut dosyası çalıştırma (XSS, Cross-Site Scripting) ile bot ağları gibi kötü amaçlı eylemleri ve verileri engellemek için her ZEN'in web isteğinin, içeriğinin, yanıtların ve ilgili tüm verilerin her baytının taranmasına olanak tanımaktadır.

NanoLog hizmeti, yöneticilerin herhangi bir işlem günlüğüne gerçek zamanlı olarak erişmesini sağlamaktadır.

Google Wallet da güvenlik kapsamında hizmet sunan uygulamalardan biridir. Uygulama, bulut tabanlı kredi kartı işlemleri ve kullanıcı kimlik bilgisi yönetimi gibi uygulama düzeyinde güvenlikten sorumlu olup, Google Wallet özellikli mobil cihazın mobil cihazlara yönelik kötü niyetli saldırıları önlemek için kart üzerinde bulunan güçlü güven hesaplama öğeleri tarafından korunan bir bulut-mobil çift güven kök modeli üzerinde geliştirilmiştir. (Jeevan ve diğerleri, 2014).

Bağlam Farkındalığı

Günümüzde akıllı mobil cihazlar, kullanıcılar için genellikle e-postaları kontrol etme, internette gezinme, bankacılık işlemlerini yürütme, veri madenciliği ve makine öğrenimine dayalı davranış verilerini analiz etme gibi çeşitli kişiselleştirilmiş etkinlikleri içeren bir bilgi geçidi görevi görmektedir. Mobil bulut teknolojisi kapsamında yapılan bir çalışmada "Mobil Cihazların Algılama Özelliğine Yönelik Entegre Bulut Tabanlı Çerçeve" önerilmekte ve mobil cihazda, karar modülü, yayınla-abone ol modülü ve içerik farkındalığı modülü olmak üzere üç bileşen içeren özel bir mobil bulut motoru (MCE, Mobile Cloud Engine) kullanılmaktadır. Karar modülü, MCE'nin farklı bölümleri arasındaki işlemleri yönetmekte ve düzenlemektedir. Yayınla-abone modülü, mobil uygulama ile MCE arasındaki veri akışını oluşturmaktan sorumludur. Son olarak, bağlam farkındalığı modülü, uygulamaya bağlam bilgisi sağlamaktadır (Jeevan ve diğerleri, 2014).

2.2 Mobil Bulut Bilişim Teknolojisi Kapsamında Ülke Uygulamaları

Mobil bulut bilişime yönelik uygulamalar genellikle ülkelerdeki özel kurum ve kuruluşlar tarafından yürütülmektedir. Hâlihazırda kamuda bu teknolojiye ilişkin herhangi bir çalışma bulunmamakta olup; bu bağlamda ülkelerde yer alan teknoloji şirketlerinin sunmuş olduğu mobil bulut bilişim uygulamaları incelenmiştir.

2.2.1 Amerika Birleşik Devletleri

Mobil bulut bilişim hizmet sağlayıcıları genellikle Amerika Birleşik Devletleri (ABD) merkezli olup, ABD nezdindeki mobil bulut bilişim çalışmaları aşağıda ele alınmaktadır.

2.2.1.1 Amazon Web Services

Mobil bulut bilişim, mobil kullanıcıların kablosuz şebekeler aracılığıyla büyük verileri bulutta depolamasını ve bu verilere erişmesini sağlamak için geliştirilmiştir. Dosya depolama hizmetini destekleyen Amazon Simple Storage Service (Amazon S3) mobil bulut bilişimin kullanımının bir örneği olarak yer almaktadır. Bu mobil fotoğraf paylaşım hizmetinde, mobil kullanıcıların görüntüleri çekildikten hemen sonra bulutlara yüklenmektedir. Kullanıcılar tüm görüntülere herhangi bir cihazdan erişebilmekte, tüm görüntüler bulutlarda gönderilip işlendiğinden, kullanıcılar mobil cihazlarında önemli miktarda enerji ve depolama alanı tasarrufu yapabilmektedir (Dev ve Baishnab, 2014).

Uzak mobil olmayan bulut örneği Amazon Elastic Compute Cloud (Amazon EC2)'da Amazon Machine Image (AMI), Microsoft Windows'un yanı sıra Amazon Linux 2, Ubuntu, Red Hat Enterprise Linux, CentOS, SUSE ve Debian'ın da aralarında bulunduğu Linux dağıtımlarını içerirken, bu işletim sistemleri ile önceden yapılandırılmıştır.

AWS'de ön uç web ve mobil uygulama geliştiricilerinin iş akışlarını desteklemek için çok çeşitli araçlar ve hizmetler sunmaktadır. AWS altyapısının hızı ve güvenilirliği ile uygulamalar ihtiyaç duyulan ölçekte geliştirebilmektedir. Bu kapsamda, aşağıda yer alan AWS hizmetleri ve kaynakları kullanılmaktadır;

- **AWS Amplify:** Amplify'da yerel iOS/Android, React Native ve JavaScript geliştiricileri için iş akışlarını destekleyen geniş bir araç ve hizmet kümesi sunulmaktadır. Ön yüz geliştirme (front-end) yapılıp, kimlik doğrulama ve

depolama gibi özellikler eklenebilmekte ve gerçek zamanlı veri kaynaklarına bağlanılabilmektedir. Öte yandan, AWS altyapısının sağladığı hız ile milyonlarca kullanıcıya kadar otomatik olarak, kimlik doğrulama, depolama, analiz ve yapay zekâ yetenekleri barındıran ölçeklenebilir uygulamalar oluşturulabilmektedir. AWS Amplify aracılığıyla ön uç web ve mobil geliştiricilerine yönelik hizmetler sunulurken; AWS sayesinde bulut işlevine sahip uygulamaların oluşturması kolaylaştırılmakta ve böylece pazara daha hızlı giriş yapılabilmektedir. Hizmetin sunmuş olduğu araçlar arasında, gerçek zamanlı ve çevrim dışı uygulamaları daha hızlı oluşturulmasına yardımcı olmak için mobil ve web uygulamaları ile AWS bulutundaki veritabanı arasındaki verileri otomatik olarak senkronize eden bir cihaz üzeri depolama motoru olan Amplift DataStore da bulunmaktadır. Bu depolama motoru, uygulama geliştirmenin hızlanması için veri modelinin ilişkilerle tanımlamak amacıyla görsel veya kod tabanlı bir arayüz kullanılmasına izin vermektedir. Ayrıca fotoğraflar, videolar gibi kullanıcı tarafından oluşturulan içeriklerin cihazda veya bulutta güvenli bir şekilde saklanıp yönetilmesini sağlayan AWS Amplify Storage modülü de bulunmaktadır. Bu modül oluşturulan uygulama için genel, korumalı veya özel depolama paketlerindeki kullanıcı içeriğinin yönetilmesine yönelik basit bir mekanizma sağlamaktadır. Uygulamanızı prototipten üretime kolayca taşıyabilmesi için bulut depolamadan yararlanırken; aynı zamanda modül Amazon S3 tarafından da desteklenmektedir (Amazon, 2023a).

- **AWS Amplify Hosting:** Sunucu tarafından oluşturulan, ölçeklenebilir, hızlı, statik ve güvenilir uygulamalara yönelik CI/CD (sürekli entegrasyon/sürekli teslimat, teslimat continuous integration/continuous delivery) ve barındırma hizmetidir. Bu doğrultuda, React, Angular, Vue, Next.js, Gatsby, Hugo, Jekyll gibi modern web çerçeveleri desteklenmektedir. Hizmet kapsamında, ön uç ve arka uç değişiklikleri, tek bir iş akışında otomatik olarak dağıtmak için yazılım geliştirme süreçlerinde kullanılan kontrol sistemi olan Git'teki dallara (branch) bağlanılabilmektedir. Uygulamalara ilişkin barındırma ölçümlerini gerçek zamanlı olarak izlenebilmekte ve ayarlanan ölçüm eşiği aşıldığında bildirim

gönderen özel alarmlar kurulabilmektedir. Doğrulama ile özel bir alan adı alınarak; özel ve özel olmayan alan adları için ücretsiz bir SSL sertifikası edinilebilmektedir (Amazon, 2023a).

- **AWS Device Farm**: Bu uygulama hizmeti, test altyapısı tedarik etme ve yönetme ihtiyacı olmadan çok çeşitli masaüstü tarayıcılarda ve gerçek mobil cihazlarda test yapma olanağı sağlamaktadır. Bu minvalde, web ve mobil uygulamalarının kalitesinin artırılması amaçlanmaktadır. Bu hizmet, testlerin birden fazla masaüstü tarayıcıda veya gerçek cihazda eş zamanlı olarak çalıştırılmasını desteklemekte ve uygulamadaki potansiyel sorunların hızlı bir şekilde tespit edilmesine yardımcı olmak için videolar ve günlük dosyalar oluşturmaktadır. Ayrıca, fiziksel cihazlardaki bellek, CPU kullanımı, konum ve üretici tarafından yapılan değişiklikler gibi faktörleri göz önünde bulundurarak, kullanıcılar ile uygulama arasındaki etkileşimi anlamak için önemli bilgiler sağlamaktadır. Bu sayede konum, şebeke bağlantısı ve uygulama verileri yapılandırılarak, gerçek dünya müşteri koşullarını simüle etmek için önkoşul uygulamaları yükleyerek test ortamı hassas bir şekilde ayarlanabilmektedir (Amazon, 2023b).

- **Amazon Chime SDK:** Bu hizmet sayesinde oluşturucular, makine öğrenimiyle desteklenen gerçek zamanlı ses, video, mesajlaşma ve masaüstü özelliklerini uygulamalarına kolayca ekleyebilmektedir. Çeşitli alanlarda kullanım örnekleri mevcuttur. Örneğin, tıbbi ve sağlık uygulamalarına gerçek zamanlı iletişim özelliği ekleyerek, günübirlik tedavilerde veya yatılı bakımlarda uzaktan konsültasyon için, sohbet ve video aracılığıyla tıp uzmanları ile hastalar arasında bağlantı sağlanabilmektedir. Bir başka örnekte ise e-eğitim uygulamalarında yüksek kaliteli ses, video ile ekran paylaşımı sunularak, eğitmenlerin karmaşık kavramları açıklamasına ve eğitimin kalitesinden ödün verilmeden daha fazla sayıda uzaktan öğrenciye ulaşılmasına yardımcı olabilmektedir.

Bir sağlık teknolojisi girişimi olan CareMonitor'de Amazon Chime SDK kullanılarak; klinik yönetim sistemler, tıbbi cihazlardan ve hastalardan verileri gerçek zamanlı olarak toplanıp, tek bir görünümde birleştiren ve bu verileri modern şifreleme standartlarıyla koruyan birleşik sağlık yönetimi platformu oluşturulmuştur. Uygulamada aynı zamanda yerleşik risk sınıflandırma araçları, bakım planı şablonları, hayati değerlerin sürekli izlenmesi, akıllı algoritmalar ve veri analitiğiyle akıllı sağlık hizmetleri de sağlanmıştır. Hâlihazırda bu telesağlık platformu, hastaneler, sağlık sigortacıları ve sağlık klinikleri de dâhil olmak üzere birçok sağlık kurumunda 10.000'den fazla hastaya hizmet vermektedir (Amazon, 2020).

- **AWS Wavelength**: Mobil bulut bilişimdeki en son yeniliklerden biri ise AWS işlem ve depolama hizmetlerini 5N şebekelerine yerleştiren AWS Wavelength'dir. Bu hizmet, ultra düşük gecikmeli uygulamalar geliştirmek, dağıtmak ve ölçeklendirmek için mobil uç bilgi işlem altyapısı sağlamaktadır. Bu kapsamda, yüksek çözünürlüklü canlı video akışı, yüksek kaliteli ses ve artırılmış/sanal gerçeklik (AR/VR, Augmented Reality/Virtual Reality) uygulamaları sunulurken; tıbbi tanılama, perakende ve akıllı fabrika ortamlarına yönelik 5N uygulamaları hızlandırmak için uçta yapay zekâ (AI, Artificial Intelligence) ile makine öğrenimi (ML, Machine Learning) destekli video ve görüntü analizleri sağlanmaktadır (Amazon, 2023c).

2.2.1.2 Google Cloud

Google Cloud, mobil uygulamalarına güçlü bulut altyapısı ve araçlar sağlamaktadır. Bu kapsamda sunulan hizmetler şu şekildedir;

- App Engine ve Cloud Run: Bu sunucusuz platformlar, geliştiricilerin mobil uygulama arka uçlarını verimli bir şekilde oluşturmasına ve dağıtmasına, kullanıcı istekleri ile veritabanı etkileşimlerini sunucuların yönetilmesine gerek kalmadan kullanılmasına olanak tanımaktadır.

- Bulut İşlevleri: Anlık bildirimler, kimlik doğrulama veya veri işleme gibi olay odaklı görevler için ölçeklenebilir bir çözüm sunulmaktadır.
- Cloud SQL: MySQL ve PostgreSQL gibi çeşitli veritabanı seçenekleri bulunmakta olup, uygulama verileri güvenli şekilde barındırılmaktadır.
- Bulut Depolama: Kullanıcı dosyaları, medya içeriği ve diğer uygulama verileri ölçeklenebilirlik ve yüksek kullanılabilirlik ile depolanmakta ve yönetilmektedir.
- Firebase Analytics: Ayrıntılı analizlerle kullanıcı davranışı izlenebilmekte ve uygulama kullanım desenleri ortaya çıkarılabilmektir.
- Bulut Günlüğü: Kullanıcı eylemlerini anlamak, hata ayıklamak ve uygulama kararlılığını artırmak için uygulama günlükleri analiz edilebilmektedir.
- Vertex AI: Mobil uygulamalara, gelişmiş işlevler için görüntü tanıma, doğal dil işleme veya özel modeller gibi makine öğrenimi özellikleri entegre edilebilmektedir.
- Firebase Cloud Messaging: Etkileşimi artırmak ve mobil uygulama özelliklerini tanıtmak için kullanıcı hedefli ve kişiselleştirilmiş anlık bildirimler gönderilebilmektedir.
- Firebase Kimlik Doğrulaması: Kullanıcı kaydı, oturum açma ve sosyal kimlik doğrulama işlemleri basitleştirilerek güvenli hale getirilmektedir.
- Bulut Kimlik ve Erişim Yönetimi: Mobil uygulamaların arka uç kaynakları için kullanıcı erişimi ve izinlerin güvenli bir şekilde yönetilmesi sağlanmaktadır.

Google Cloud, bu özelliklerinin yanı sıra kullanıcılarına mobil bulut uygulamaları sunmaktadır. Bunun bir örneği olarak bulut uygulamalarında olabilecek sorunların mobil cihaz üzerinden giderilmesine ve yönetilmesine yardımcı olan Google Cloud mobil uygulaması verilmektedir. Yukarıda değinilen özelliklere uygulama üzerinden direkt erişilebilmekte ve kullanılabilmektedir (Google Cloud, 2024).

2.2.1.3 Microsoft Azure

Microsoft Azure platformu, kullanıcılarına mobil bulut bilişim uygulamaları sunarken, geliştiricilere ise bulut temelli mobil uygulamalar oluşturmaları için çeşitli araçlar ve hizmetler sağlamaktadır. Bu kapsamda aşağıda yer alan hizmetler sunulmaktadır;

- Azure Mobile App Service: Bu platform, arka uç geliştirmeyi basitleştirerek kimlik doğrulama, anlık bildirimler, veri depolama ile API yönetimi sunmayı ve geliştiricilerin mobil uygulama oluşturmasını kolaylaştırmayı hedeflemektedir.
- Xamarin: Microsoft'un platformlar arası çerçevesi, geliştiricilerin C# koduyla yerel iOS, Android ve Windows uygulamaları oluşturmasına olanak tanıyarak uygulama geliştirme süresini ve maliyetlerini azaltmaktadır.
- Azure Uygulama Merkezi: Bu paket, sürekli entegrasyon ve teslimat (CI/CD), test, tanılama ve analiz için araçlar sunarak mobil geliştirme yaşam döngüsünü kolaylaştırmaktadır.
- Azure Cosmos DB: Küresel olarak dağıtılan bu NoSQL veritabanı, mobil uygulama veri depolaması için yüksek performans, ölçeklenebilirlik ve çevrim dışı özellikler sunmaktadır.
- Azure Blob Depolama: Kullanıcı dosyaları ile diğer uygulama verileri ölçeklenebilirlik ve yüksek kullanılabilirlikle depolanmakta ve yönetilmektedir.
- Azure Bilişsel Hizmetler: Görüntü tanıma, konuşma tanıma, metin analizi gibi önceden oluşturulmuş yapay zekâ modelleri mobil uygulamalara entegre edilebilmektedir.
- Azure Machine Learning: Mobil uygulamada kişiselleştirilmiş öneriler, sahtekârlık tespiti veya duyarlılık analizi gibi görevler için özel makine öğrenimi modelleri oluşturulmasını sağlamaktadır.
- Azure Bildirim Hub': Mobil cihaz kullanıcılara kişiselleştirilmiş anlık bildirimler gönderilmesi sağlamaktadır.

- Azure Active Directory: Oturum açma ve yetkilendirme için mevcut kimliklerden yararlanarak kullanıcı erişiminin ve izinlerinin güvenli bir şekilde yönetilmesi amaçlanmaktadır.
- Azure App Service Kimlik Doğrulaması/Yetkilendirme: Yerleşik kimlik doğrulama ve yetkilendirme özellikleri ile kullanıcı yönetimi basitleştirilmekte ve güvenli erişim kolaylaştırılmaktadır (Microsoft, 2023).

2.2.1.4 IBM Cloud

IBM Cloud sunduğu olanaklarla, kimlik doğrulama ve ölçeklendirme sıkıntısını hafifleterek, yerel, hibrit veya web tabanlı mobil uygulamalar oluşturulmasına ve bakımının yapılmasına yardımcı olmaktadır.

Mobil arka uç yazılım geliştirme IBM Cloud tarafından yürütülmekte olup, mobil uygulamaların daha kolay ve hızlı dağıtımı sağlanmaktadır. Ayrıca hava durumu verileri, nesnelerin interneti aygıtlarıyla entegrasyon ve yapay zekâ ile mobil uygulamaların özellikleri genişletilmektedir. Bununla birlikte verilerin korunması kapsamında, mobil uygulamalara kimlik doğrulama güvenliği eklenmekte ve arka uç hizmetleri içinse kullanıcıların özel hesaplarla veya mevcut sosyal hesaplarla oturum açmasına izin verilmektedir. Böylece nerede barındırıldıklarına bakılmaksızın veri kaynaklarına güvenli bir şekilde erişilmektedir. Öte yandan, çevrim dışı senkronizasyon ile şifreli cihaz içi depolama kullanılarak kurumsal mobil uygulamalar hem çevrim dışı hem de çevrim içi modlarda sorunsuz bir şekilde çalışmakta ve arka uç veritabanlarıyla veri eşzamanlaması otomatikleştirilmektedir.

IBM Cloud tarafından sağlanan diğer bir özellik ise sunucusuz mobil uygulamaların otomatik olarak ölçeklendirilmesidir. Böylece altyapı kısıtlamaları ortadan kaldırılarak geliştirme engelleri çözülmektedir (IBM, 2023a).

IBM Cloud'un mobil bulut bilişim kapsamında sunduğu çözümler şu şekildedir;

- IBM Cloud App ID: Bu özellik, web uygulamalarına ve mobil uygulamalara kolayca kimlik doğrulama eklemesini sağlamaktadır. Kimlik için altyapı kurulması, coğrafi kullanılabilirliğin sağlanması ve uyumluluk düzenlemelerinin onaylanması gibi konulardaki endişeler ortadan kaldırılarak, uygulamalar çok faktörlü kimlik doğrulama ve tek oturum açma gibi güvenlik özellikleriyle geliştirebilmektedir (IBM, 2023b).

- IBM Push Notifications (Anlık Bildirim): IBM Push Notifications hizmeti, bildirimleri yapılandırmak, izlemek ve göndermek için sezgisel bir kullanıcı arabirimi, istemci yazılım geliştirme kiti ve temsili durum transferi (REST) API'lerini kullanmakta ve böylece mobil ve web anlık bildirimlerin gönderilmesi ile yönetilmesine olanak tanımaktadır. Ayrıca kayıtlı cihazlardaki kullanıcı verileri izlenerek bu bilgiler analiz edilebilmektedir (IBM, 2023c).

- IBM Cloud App Configuration (Uygulama Yapılandırması): IBM Cloud App Configuration, ortam yapılandırmalarının ve uygulama özelliklerinin anında değiştirilmesine yardımcı olarak, merkezi bir yapılandırma deposu sunmaktadır (IBM, 2023d).

- IBM API Connect: Bu hizmet, API'lerin tutarlı bir şekilde oluşturulmasına, yönetilmesine ve güvenliğinin sağlanmasına yardımcı olarak, dijital dönüşümün güçlendirilmesini destekleyen API yönetimi çözümüdür. Uygulamalar ve veriler bulunduğu her yerde (bulutta, şirket içinde veya herhangi bir hibrit ortamda) esnek bir şekilde dağıtılabilmektedir. Ayrıca OAuth, OpenID Connect ve üçüncü taraf hizmetleri kullanılmasıyla API'lere erişim güvenli hale getirilerek kontrol edilmektedir (IBM, 2023e).

- IBM Cloudant: Hızla büyüyen web ve mobil uygulamalar için optimize edilmiş, dağıtılmış bir veritabanı olan IBM Cloudant, bir IBM Bulut hizmeti olarak sunulmaktadır. Cloudant ile uygulama gereksinimlerinin karşılanması

için üretim kapasitesi ve veri depolama esnek bir şekilde ölçeklendirilmektedir. Ayrıca isteğe bağlı kullanıcı tanımlı şifreleme anahtarı yönetimiyle tüm veriler şifrelenmektedir (IBM, 2023f).

Mobil cihazlar, masaüstü bilgisayarlar veya kurumsal sunuculara kıyasla çok daha az işlem gücüne ve belleğe sahiptir. Bu kısıtlamalar, özellikle web uygulamalarına yönelik geleneksel yazılım geliştirirken nispeten sınırsız kaynaklarla çalışanlar için önemli bir zorluk gibi görünebilmektedir. Bu yüzden sınırlı mobil platform kaynaklarının, uygulama tasarımı için ayarlanması gerekmektedir. Ayrıca mobil uygulamalarda kullanıcı deneyimi de çok önemlidir. Örneğin mobil uygulama için kullanıcı arayüzü bir masaüstü uygulama arayüzünden daha basit olmalıdır. Ancak genellikle mobil uygulamalar tipik bir mobil platformun destekleyebileceğinden daha fazla işlem gerektirmektedir. Bu kapsamda uygulamanın yürütülmesi buluta taşınmaktadır. IBM Cloud API'leri kullanılarak, uygulama yavaşlatılmadan veya üzerinde çalıştığı cihazı zorlamadan gelişmiş işlevselliğin sağlanması için uygulamaları bulut tabanlı hizmetlere ve veritabanlarına bağlamaktadır. Bunlara ek olarak, veri depolama ve önbelleğe alma yükü de bulut tabanlı bir sunucuya aktarılarak cihazda çok az veri bırakılabilmektedir. Mobil uygulamaların geliştirmesine yardımcı olabilecek anlık bildirimler, IBM Watson destekli yapay zekâ analitiği, akıllı cihaz entegrasyonu gibi özellikleri de entegre etmek için API'lerden yararlanılabilmektedir (IBM, 2023f).

IBM'in sunduğu MaaS360 Mobil Cihaz Yönetimi (SaaS), akıllı telefonların ve tabletlerin görünürlüğünü ve denetimini sağlayan bir kurumsal mobilite yönetimi (EMM) platformudur. IBM MaaS360 yazılımı iPhone, iPad, Android ve Windows Phone gibi aygıtları desteklemektedir. Hizmetin özellikleri arasında belge düzenleyici de bulunmakta ve böylece bulutta yer alan belgeleri doğrudan mobil cihazda düzenlemektedir. Ayrıca Maas360, Uç Nokta Tehdit Yönetimi (ETM)'ni de sunmaktadır. Yönetilen cihazlar ve kurumsal veriler gelişmiş güvenlik tehditlerine karşı korunarak, şüpheli etkinlikler tanımlanmakta ve güvenlik tehditlerine gerçek zamanlı olarak yanıt vermek amacıyla cihazlar izlenmektedir. Bir tehdit algılandığında, MaaS360 önceden tanımlanmış bir düzeltme eylemi başlatmakta ve

tehdit bilgisini MaaS360 Portal ile paylaşmaktadır. Böylece örneğin bir güvenlik yöneticisi, kuruluşunun tehdit bilgisini bir gösterge tablosunda inceleyebilmektedir (IBM, 2023g).

IBM, bir enerji şirketi olan ExxonMobil ile iş birliği yaparak, şirketinin sadakat programının avantajlarını mobil ödeme uygulaması ile birleştiren ExxonMobil Rewards+ uygulamasını oluşturmuştur. Ayrıca IBM, Amerika Açık Tenis Turnuvası için de mobil bulut bilişim temelli bir uygulama geliştirmiştir. Uygulamanın geliştirilmesinde IBM'in yapay zekâ programı olan Watson da kullanılmıştır. Amerika Açık Tenis Turnuvasına dijital bir deneyim kazandırılırken, maçların çoğu televizyonda yayımlanmadığından ve herhangi bir sözlü yorum bulunmadığından, Sandstone adlı güçlü ve büyük bir dil modelini temel alan üretken bir yapay zekâ çözümü geliştirilmiştir. Bu yapay zekâ çözümü tenis maçını tam olarak anlatabilmek için tenis verileri üzerinden eğitilmiştir. Ayrıca model, söz konusu verileri, anlamlı içgörülere dönüştürmek için gelişmiş veri analitiğini ve doğal dil işlemeyi de kullanarak yapay zekâ destekli bilgi formları oluşturmuştur (IBM, 2023a). Bu çerçevede, mobil bulut bilişim teknoloji sayesinde mobil cihaz kapasitesi bir engel olarak düşünülmeden yapay zekâ ve doğal dil işlemenin kullanıldığı bir mobil uygulama geliştirilmiştir.

2.2.2 Çin Halk Cumhuriyeti

Bu başlık altında, Huawei ve Alibaba şirketlerinin mobil bulut bilişim hizmetlerine yer verilmiştir.

2.2.2.1 Huawei Mobile Cloud

Çin menşeli ve çok uluslu bir şirket olan Huawei tarafından, mobil cihaz kullanıcılarının fotoğraflarını, videolarını, rehberdeki kişilerini, notlarını ve diğer önemli bilgilerini depolamaları ve yedeklemeleri için Mobile Cloud geliştirilmiş; ayrıca hizmet kapsamında, internet tarayıcı, harita, cihaz bulma gibi özellikler de sunulmuştur.

Sunulan hizmet kapsamında yer alan Huawei Drive ile mobil cihazdaki fotoğraflar, sesler, videolar, belgeler veya uygulamalar bulutta kaydedilirken; depolanan verilerin herhangi bir cihazdan yönetilmesi içinse Huawei ID adı verilen bir Huawei kimliği verilmektedir. Bu doğrultuda, kişi bilgisi, notlar, fotoğraflar, görüntülenebilmekte, cihazın konum bilgisine erişilebilmekte veya cihazın kaybedilmesi/çalınması durumlarında telefon verileri uzaktan silinerek kişisel verilerin çalınması önlenebilmektedir. Ayrıca kullanıcı verilerinin bir bulutta yedeklenmesi, cihaz kaybedilse bile veri kaybının önlenerek, kişilerin verilerini istedikleri zaman, istedikleri yerde yeni bir cihaza rahatça aktarabilmelerine olanak tanımaktadır. Bununla birlikte fotoğraflar ve videolar herhangi bir mobil cihazdan güvenli bir şekilde ve otomatik olarak senkronize edilebilmektedir (Huawei, 2023a).

Huawei Mobile Cloud'da veriler işlenirken şu şekilde bir yöntem izlenmektedir; kullanıcı bilgileri ilk önce cihazda sıkıştırılıp şifrelenmekte, ardından şifreleme anahtarıyla birlikte şifreli bir kanal üzerinden buluta iletilmektedir. Ayrıca yüz tanıma ve akıllı fotoğraf gibi görüntü işleme özellikleri yalnızca mobil cihazda gerçekleştirildiği için bulut hizmeti sağlayıcısı da dâhil hiç kimse kullanıcı bilgilerine erişememektedir. Bununla birlikte, veriler, ağ işlemlerinde ve ödemelerde yaygın olarak kullanılan bir şifreleme kanalı olan HTTPS protokolü aracılığıyla iletilmektedir.

Huawei Mobile Cloud'un; veri güvenliği kapsamında CSA STAR Sertifikası, CSA C-STAR Sertifikası, ISO/IEC 27001 Bilgi Güvenliği Yönetimi Sertifikası, ISO/IEC 27018 Kişiyi Tanımlayan Bilgilerin Güvenliğinin Yönetimi Sistemi, MIIT TRUCS Sertifikası, DJCP MLPS Seviye III Bilgi Güvenliği, CNITSEC Bilgi Güvenliği Servisi Niteliği ve ISCCC Bilgi Güvenliği Servisi Nitelik Sertifikası gibi çeşitli sertifikaları bulunmaktadır (Huawei, 2023b).

2.2.2.2 Alibaba Cloud

Alibaba Cloud, mobil uygulama geliştirme, test, bakım ve operasyon için buluttan uca, tek noktadan çözüm sağlayan MPaaS hizmeti sunmaktadır. Hizmet, geliştiriciler mobil uygulama oluştururken ortaya çıkan teknik engellerin azaltılmasına, Ar-Ge maliyetlerinin düşürülmesine ve verimliliğinin artırılmasına yardımcı olmaktadır.

MPaaS hizmeti, Kylin, HTML5 ve Mini olmak üzere üç yerel yazılım iskeleti barındırmaktadır. Ayrıca ağ geçidi hizmeti, olay izleme analizi, kullanıcı geri bildirimi, mesaj gönderme, çevrim dışı paket yönetimi gibi yirmiden fazla işlevsel bileşen ile AntUI ve AntMobile dâhil olmak üzere yüzden fazla kullanıcı arayüzü kontrolüne sahiptir. Bununla birlikte, mobil uygulama geliştirmenin her aşamasını kapsayan birçok yüksek performanslı bileşen de içermektedir. Söz konusu bileşenler, yeni uygulamaların hızla geliştirilmesi için yazılım iskeletiyle birlikte kullanılabilmekte veya mevcut bir uygulamaya bağımsız olarak entegre edilebilmektedir (Alibaba, 2023).

Alibaba Cloud, bu hizmete yönelik çeşitli özellikler barındırmaktadır;

- Her bir iş modülü, beyaz ekran hataları ve yükleme hataları gibi performans sorunlarını en aza indirmek için konteynerlarla izole edilmektedir.
- Birden fazla cep telefonuyla entegre olan mPaaS, mesaj dağıtım ayarlarının özelleştirilmesine ve uygulama kullanıcılarıyla etkileşimde bulunulmasına olanak tanımaktadır.
- MPaaS sistemi karmaşık istemcilerle uyumlu olmakla birlikte, uygulamaların zayıf ağ koşullarında çalışmasına da yardımcı olmaktadır.
- Tersine mühendisliği önlemek amacıyla mobil uygulamalar için istikrarlı, kullanışlı ve etkili güvenlik çözümleri sunulmaktadır.

Alibaba MPaaS platformunun sunduğu hizmet bileşenleri şu şekildedir (Alibaba, 2023);

- Mobile Delivery Services (Mobil Dağıtım Hizmeti): Mobil Dağıtım Hizmeti, MPaaS platformunun temel hizmet bileşenlerinden biridir. Sürüm yükseltme

paketleri ve HTLM5 çevrim dışı paketleri için yönetim ve yayımlama hizmetleri sağlamaktadır. Bununla birlikte, gelişmiş filtreleme özelliği sayesinde resmi sürümden önce, uygulamanın ya da sürüm yükseltme paketinin beklentileri karşılayıp karşılamadığının anlaşılabilmesi için belirli bir kullanıcı grubuna (örneğin: yalnızca şirket içi personele) sunulabilmektedir.

- Message Push Services (Mesaj Gönderme Hizmeti): Mesaj Gönderme Hizmeti, kişiselleştirilmiş gereksinimleri karşılamak üzere farklı senaryolar için çeşitli gönderme türlerini desteklemektedir. Anlık iletilen mesajların varış oranının iyileştirilmesi için Huawei, Xiaomi ve diğer satıcıların anlık işlevleri, Mesaj Gönderme Hizmeti'ne entegre edilmektedir. Böylece, kullanıcılarla etkileşimi sürdürmek için mesajlar mobil cihazlara hızlı bir şekilde iletilmekte ve kullanıcı deneyimi iyileştirilmektedir.

- **Mobile Sync Service (Mobil Senkronizasyon Hizmeti):** Mobil Senkronizasyon Hizmeti MPaaS platformunun temel bir iş bileşenidir. Bu bileşen, İletim Kontrol Protokolü (TCP, Transfer Control Protocol) ve Güvenli Yuva Katmanı (SSL, Secure Sockets Layers) tabanlı güvenli bir veri kanalı sağlamaktadır. Bu veri kanalı ile bilgiler sunucudan mobil uygulamaya zamanında, doğru ve düzenli bir şekilde aktif olarak senkronize edebilmektedir.

- **Mobile Gateway Services (Mobil Ağ Geçidi Hizmeti):** Mobil Ağ geçidi hizmeti, mobil istemciyi ve sunucuyu birbirine bağlayan MPaaS tarafından sağlanan bir bileşendir. Bu bileşen, mobil terminal ile sunucu arasındaki veri protokolünü ve iletişim protokolünü basitleştirerek, geliştirilmesini ve ağ iletişim verimliliğini önemli ölçüde artırmaktadır. Söz konusu hizmet, çeşitli terminallere uyum sağlamakta ve heterojen arka uç hizmetlerini basit yapılandırmayla birbirine bağlamaktadır.

- **Mobile Security Armor (Mobil Güvenlik Zırhı):** Hizmet, mobil uygulamaların genel güvenliğin artırarak istikrarlı, basit ve etkili güvenlik koruması sağlamaktadır. Hem Android hem de iOS işletim sistemleri için yüksek güvenlik ve yüksek uyumluluk sağlarken, düşük hata oranı da sunmaktadır. Ayrıca HTML5 uygulamalarına yönelik sabit dize şifreleme, kod sıkıştırma, hata ayıklama önleme gibi güvenlik güçlendirme yetenekleri de bulunmaktadır (Alibaba, 2023).

Alibaba Cloud sunmuş olduğu MPaas Platformu kapsamında çeşitli projeler de hazırlamıştır. Örneğin, Shenzhen Rural Commercial Bank ile finans alanına yönelik bir proje yürütülmüştür. Proje kapsamında, bankanın MPaaS kullanılarak geliştirilen mobil uygulamasının yeni bir sürümünü yayımlandıktan sonra mobil uygulama performansı büyük ölçüde iyileşmiştir. Bu doğrultuda kullanıcı etkileşimi artmış ve mobil bankacılık uygulaması üzerinden ödeme oranları yükselmiştir. Bankaya ise kullanıcı davranışlarına yönelik analizler iletilerek, pazarlamaya yönelik yeni stratejiler oluşturmasına yardımcı olmuştur (Alibaba, 2023).

2.2.3 Birleşik Krallık

Birleşik Krallık merkezli Starling Bank, mobil cihazların sunduğu rahatlığı, bankacılık hizmetleriyle birleştirmiş ve 2017 yılında hem iOS hem de Android telefonlar için bulut tabanlı mobil uygulamasını kullanıma sunmuştur.

Yalnızca mobil cihazlar üzerinden hizmet veren ve fiziki şubesi bulunmayan bankanın, yaklaşık 3,6 milyon kullanıcısı bulunmaktadır. Starling Bank, bulut tabanlı mobil uygulamasını kullanıma sunarken AWS ve Google'ın bulut hizmetlerinden yararlanmıştır. Bu kapsamda, Google'ın sunucusuz veri ambarı olan BigQuery'den çok büyük miktardaki müşteri verisinin analiz edilmesi amacıyla faydalanılmış, hesapların nasıl ve ne sıklıkla kullanıldığının belirlenmesi için bankacılık hizmetlerine ilişkin anonimleştirilmiş veriler toplanmıştır. Ayrıca bulutlar arası dayanıklılık oluşturmak ve herhangi bir bulut sağlayıcısına bağımlılığı ortadan kaldırmak için açık kaynaklı Kubernetes ve Google Kubernetes Engine üzerinden konteynerli

uygulamalar çalıştırılarak, Google Cloud'un barındırma hizmetlerinden istifade edilmiştir (Google Cloud, 2023a).

Bununla birlikte Starling Bank altyapısını oluştururken AWS'yi kullanmıştır. Amazon'un bulut hizmetleri kapsamında sunduğu Amazon EC2 aracılığıyla güvenli sanal sunucu barındırma, Amazon RDS ile tam olarak yönetilen, ölçeklenebilir veritabanı motoru, Amazon EKS ile Kubernetes yönetimi, Amazon S3 ile veri gölü AWS Lambda aracılığıyla sunucuları tedarik etmeden veya yönetmeden kod çalıştırma özelliklerinden yararlanılmıştır.

Bir MSaaS örneği olan Starling Bank'ta uygulama güvenliği gerçek zamanlı anlık bildirimler, biyometrik tanımlamalar, şifreler ile sağlanmaktadır. Bununla birlikte, kişisel verilerin korunması kapsamında UK GDPR ile uyumlu olması için gereken kontroller yapılmaktadır (Starling Bank, 2023).

2.2.4 Birleşik Arap Emirlikleri

Birleşik Arap Emirlikleri'nde de birçok bulut temelli mobil uygulama bulunmaktadır. Bunlardan biri olarak Orta Doğu ve Kuzey Afrika'nın önde gelen araç çağırma platformu Careem verilmektedir. Careem üzerinden sadece araç çağrılmamakta aynı zamanda yemek siparişi verilebilmekte veya alışveriş yapılabilmektedir. Careem ölçeklenebilir ve güvenli altyapısı nedeniyle Google Cloud Platform'u (GCP) kullanmaktadır. Yolculuk eşleştirme, ödeme işleme ve gerçek zamanlı takip gibi temel özellikleri çalıştırmak için sanal makineler sağlayan Compute Engine'den yararlanırken, bulut depolama sayesinde çok miktarda kullanıcı verisi, sürücü bilgisi ve sürüş geçmişi saklanmaktadır. Bulut bilişimin sunduğu ölçeklenebilirlik özelliği sayesinde Careem, çeşitli bölgelerdeki milyonlarca eş zamanlı yolculuk talebinin karşılanmasına olanak tanıyarak sorunsuz çalışmaktadır.

Careem mobil uygulamasında da temel işlevler için bulut hizmetlerinden yararlanılmaktadır. Bulut algoritmaları, sürücüleri uygun seçeneklerle anında

buluşturmak için mevcut sürücüleri, konumları ve talepleri analiz etmekte, yapay zekâ ise geçmiş verilere ve gerçek zamanlı talebe dayanarak artış fiyatlandırmasını belirlemektedir. Ayrıca bulut tabanlı haritalama ve trafik verileri, rotaları en kısa seyahat süresi ve yakıt verimliliği için optimize etmektedir.

Ayrıca Careem veri güvenliğini sağlamak için çeşitli önlemler almaktadır. Bu kapsamda, kullanıcının kişisel bilgileri, seyahat ayrıntıları ve ödeme bilgileri gibi hassas veriler hem depolamada hem de aktarım sırasında şifrelenmektedir. Güvenlik açıklarını belirlemek için düzenli güvenlik denetimleri ile sızma testleri gerçekleştirilmekte ve iki faktörlü kimlik doğrulama uygulanmaktadır. Bununla birlikte, GDPR ve Birleşik Arap Emirlikleri Kişisel Verilerin Korunması Yasası gibi faaliyet gösterilen bölgelerdeki ilgili veri gizliliği düzenlemelerine uyumlu hizmetler yürütülmektedir. Tüm bunlara ek olarak, Careem yalnızca gerekli olan verileri toplayıp saklamakta, böylece tuttukları hassas bilgi miktarını en aza indirmektedir (Careem, 2023).

Başka bir örnek olarak ise Birleşik Arap Emirlikleri merkezli bir dijital banka olan Liv Bank verilmektedir. Liv Bank, bulut teknoloji sağlayıcılarından Microsoft Azure ile ortaklık yürütmektedir. Bu bağlamda, büyük miktardaki müşteri verisinin yönetilmesi, işlemler, bildirimler ile gerçek zamanlı olayların takip edilmesi, güvenli kimlik doğrulaması ve erişim kontrolünün sağlanması için sunulan hizmetlerden faydalanılmaktadır. Yalnızca mobil cihazlara yönelik dijital bankalardan biri olan platformun mobil bulut uygulamasında anında para transferleri, finans yönetimi, yapay zekâ destekli bütçeleme araçları ile parmak izi veya yüz tanıma yoluyla güvenli oturum açma ve işlem yetkilendirmesi yapılabilmektedir (Microsoft, 2021).

Platformda veri güvenliği kapsamında, çok faktörlü kimlik doğrulama, biyometrik kimlik doğrulama, kişisel veriler depolanırken ve aktarımı esnasında şifreleme gibi tedbirler alınmaktadır. Ayrıca erişim kontrolleri ile kullanıcı verilerine yetkili personelin ve sistemlerin erişimi kısıtlanmaktadır. Bununla birlikte, Birleşik Arap

Emirlikleri Kişisel Verilerin Korunması Yasası gibi veri gizliliği düzenlemelerine de uyumlu hizmetler sunulmaktadır (Liv, 2024).

2.2.5 Almanya

Almanya merkezli Open Telekom Cloud, şirket içi, özel bulut ve genel bulut hizmetlerinin tamamını destekleyerek, sorunsuz bir arada çalışmasına olanak sağlayan hibrit bulut hizmeti vermektedir. Bu kapsamda ise barındırma, depolama, olağanüstü durum kurtarma, güvenlik, konteyner ve veri analizi gibi çözümler sunmaktadır. IaaS ve PaaS hizmetleri veren şirket, mobil bulut bilişim kapsamında ise depolama çözümü sağlamaktadır. Ayrıca Open Telekom Cloud'un bulut bilişime yönelik çeşitli güvenlik önlemleri de bulunmaktadır. Bu doğrultuda, DDoS saldırılarına yönelik Anti DDoS, SQL enjeksiyonu için çeşitli güvenlik araçları, web sunucusuna giden HTTP ve HTTPS tabanlı ağ trafiğinin izlendiği güvenlik duvarı, anahtar yönetim ve şifreleme hizmetleri uygulanan güvenlik tedbirleri arasındadır. Bununla birlikte, güvenlik testleri (sızma testleri) de yapılmaktadır.

Tüm bunlara ek olarak, Open Telekom Cloud'da gizli bilgi işlem gerçekleştirilmekte ve hassas verilerin yerleşim adı verilen özel olarak korunan, şifrelenmiş bir ortamda işlenebilmesi sağlanmaktadır. Böylece verilere, bulut sağlayıcısı veya yetkisiz üçüncü şahıslar tarafından değil, yalnızca kullanıcı tarafından erişilebilmektedir. Bekleme ve aktarım sırasındaki şifreleme ise ana bellekte çalışan yazılımı ve işlenen verileri kapsayan şifrelemeyle tamamlanmaktadır. Bulut bilişim kapsamında birçok sertifikası bulunan şirket, GDPR ve AB Bulut Davranış Kurallarına uyumlu çalıştığını da belirtmektedir (Open Telekom Cloud, 2023).

Almanya'da yer alan başka teknoloji şirketi IONOS da küçük ve orta ölçekli işletmelere yönelik web barındırma ve bulut hizmetleri sağlamaktadır. Özellikle IaaS'a yönelik çalışmaları olan şirket, dijital bir çözüm portföyü sunmaktadır. Şirketin bulut bilişim kapsamında, Kubernetes, makine öğrenimi platformu, büyük veri analizi, hizmet olarak güvenlik duvarı, veri yedekleme ve felakat kurtarma gibi çözümleri de bulunmaktadır.

IONOS, mobil bulut bilişime yönelik de hizmet vermektedir. IONOS mobil uygulaması ile kişiler hesabını doğrudan kullanabilmekte ve ürünlerine masaüstü veya dizüstü bilgisayarla aynı erişimi sağlamaktadır. Kullanıcılar web siteleri ile ilgili bildirimlere ve mesajlara ulaşabilirken, sitelerin düzenlemesini mobil cihazlar üzerinden yapamamaktadır. Mobil uygulama iki faktörlü kimlik doğrulama ile IONOS hesabını güvence altına almakta ve hesap erişimi yalnızca iki farklı kimlik bilgisi girildikten sonra mümkün olmaktadır (IONOS, 2023).

2.2.6 Kanada

Kanada merkezli çok uluslu e-ticaret şirketi olan Shopify, 2018 yılında kendi veri merkezlerinden Google Bulut'a geçiş yapmıştır. Hâlihazırda Google Kubernetes Engine'i kullanan şirket, Google Bulut'a geçerek 400'den fazla özelliğe erişmiş ve Kubernetes'teki tüm üretim hizmetlerini birleştirmek amacıyla bir hizmet olarak platform (PaaS) oluşturmuştur. Öte yandan şirket AWS'den de bulut barındırma hizmeti almıştır (Shopify, 2023a).

Mobil cihazlar için optimize edilen bulut tabanlı uygulaması ile de kullanıcıların, internet bağlantısı olan herhangi bir mobil cihazdan işletmelerine erişebilmeleri ve her yerden yönetebilmeleri sağlanmaktadır. MSaaS örneği olan uygulaması, çok kiracılı bir mimariye dayanmakta olup, kişisel veriler, uygulama düzeyindeki kontrollerle ayrıştırılmaktadır. Kullanıcılar çok faktörlü kimlik doğrulamayı etkinleştirebilmekte ve son oturum açma etkinliği de dâhil olmak üzere etkinlik günlüklerini görüntüleyebilmektedir. Ayrıca kullanıcı rollerine göre erişim düzeyleri de ayarlanabilmektedir. Bunlara ek olarak, ödeme, vitrinler ve yönetici sayfaları için Güvenli Hiper Metin Aktarım Protokolü (HTTPS, HyperText Transfer Protocol Secure) kullanılmaktadır. Operasyonel veri depolarındaki kredi kartı ayrıntıları ve diğer hassas bilgiler, kullanımda değilken de şifrelenmektedir. Kullanıcılara ve mağazalara olan tüm bağlantıları güvence altına almak amacıyla bir şifreleme protokolü olan Aktarım Katmanı Güvenliği (TLS, Transport Layer Security) kullanılmaktadır. Potansiyel güvenlik zayıflıklarını tespit etmek ve gidermek amacıyla

üçüncü taraf güvenlik açığı taramaları ve sızma testleri de düzenli olarak gerçekleştirilmektedir (Shopify, 2023b).

Ayrıca Kanada merkezli telesağlık hizmeti olan Maple de başka bir mobil bulut bilişim uygulaması olarak yer almaktadır. Şirket, bulut bilişim servis sağlayıcılarından AWS ile çalışmaktadır. AWS'nin sunmuş olduğu hizmetleri kullanarak, hasta verilerinin güvenli bir şekilde saklanarak, mevzuata uygunluğun sağlanması ve kullanıcı verileri ile randevu bilgilerinin verimli bir şekilde yönetilmesi hedeflenmektedir. AWS güçlü güvenlik önlemlerinin yanı sıra sağlık hizmeti veri gizliliği düzenlemeleriyle uyumlu hizmetler de sunmaktadır.

Maple mobil uygulamasında da bulut teknoloji hizmetlerinden yararlanılmaktadır. Bulut algoritmaları, hastaların ihtiyaçlarını ve tıbbi geçmişini analiz ederek kişileri uygun doktorlara gerçek zamanlı olarak bağlamaktadır. Ayrıca elektronik reçeteler eczanelere güvenli bir şekilde gönderilerek fiziksel kopya ihtiyacı ortadan kaldırılmaktadır. Özellikle mobil uygulama sayesinde sağlık hizmetlerine erişim kolaylaşarak uzak bölgelerden gelen veya hareket kabiliyeti kısıtlı hastalar doktorlarla rahatça bağlantı kurabilmektedir.

Maple platformu, AWS'nin sunduğu güvenlik önlemleriyle beraber tehditlere karşı düzenli olarak taranmakta ve iki yılda bir harici sızma testleri gerçekleştirilmektedir. Depolanan verilerin güvenliğini sağlamak için AES 256 bit şifreleme kullanılmakta, kullanıcı kredi kartı bilgileri işlenmemekte veya saklanmamaktadır. Ayrıca iki faktörlü kimlik doğrulama ve hesap etkinliğinin izlenmesi gibi özellikler de bulunmaktadır (Maple, 2024).

2.2.7 Hindistan

Hindistan merkezli ve 2010 yılında başlatılan teknoloji platformu Zomato, müşterileri, restoran sahiplerini ve teslimatçıları birbirine bağlayarak kişilerin çeşitli ihtiyaçlarına hizmet etmektedir. Kullanıcılar, restoranları aramak, müşteri tarafından oluşturulan yorumları okuyup yazmak, fotoğrafları görüntülemek ve yüklemek, yemek siparişi

vermek, masa rezervasyonu yapmak ve restoranlarda yemek yerken ödeme yapmak için platformu kullanmaktadır.

Bulut bilişim kapsamında AWS ile iş birliği yapan şirket, zengin bir kullanıcı deneyimi yaşatmayı amaçlamaktadır. Bu doğrultuda, AWS tarafından sunulan Amazon EC2, Amazon S3, Amazon RDS, Amazon CloudFront, Amazon Route 53 gibi araçlardan yararlanılmaktadır. Platform, bilgi işlem kapasitesinin ölçeklendirilmesi, verilerin depolanması, ilişkisel veritabanının yönetilmesi, güvenilir DNS hizmetinin sunulması, gerçek zamanlı sipariş takibi, içeriğin kullanıcılara yerel sunucularda ya da en yakın yerel sunucuda önbelleğe alınarak içeriği indirmek için erişim hızını artıran küresel proxy sunucu ağının sağlanması kapsamında AWS'den faydalanmaktadır (Medium, 2023). Ayrıca şirket, arama işlemini daha kapsayıcı ve etkileşimli hale getirmek amacıyla alana özgü arama sistemlerini, tek amaç tipi sorgular için optimize etmiş ve bu kapsamda doğal dil işleme kullanarak, Google'ın eğittiği Word2Vec'den yararlanmıştır.

Bununla birlikte Zomato'nun bulut tabanlı mobil uygulaması da bulunmaktadır. Mobil uygulamasında kullanıcının mevcut konumunun yakınında rastgele bir restoran önerilmesi veya restoranlara ilişkin tavsiyeler alınması gibi GPS tabanlı özellikler bulunmaktadır. Genel olarak mobil uygulamada, web sitesi üzerinden ulaşılabilecek her şey yapılabilmektedir. Mobil bulut bilişime dayalı bu uygulama ile kullanıcılar, kolaylıkla restoranları arayabilmekte, menüler ile fotoğrafları görüntüleyebilmekte, yorumları okuyabilmekte ve ayrıca bir restoran için yorum yazıp resim yükleyebilmektedir (Zomato, 2011).

Hindistan merkezli e-ticaret şirketi olan Flipkart da bulut bilişimden yararlanmaktadır. Ölçeklenebilir ve güvenli altyapı sunması nedeniyle Google Cloud ile iş birliği yapan şirket, temel uygulamaları çalıştırmak için sanal makineler sağlayan Compute Engine, kullanıcı davranışlarını ve satış verilerini analiz etmek için ise BigQuery gibi hizmetlerden faydalanmaktadır. Mobil bulut bilişim örneği olan mobil uygulamasında BigQuery'den yararlanarak veri analizi ve yapay zekâ destekli kişiselleştirilmiş öneriler sunulmakta, gerçek zamanlı ürün güncellemeleri ile siparişin lojistik durumu

kullanıcıya yansıtılmaktadır. Ayrıca Google Cloud, Flipkart mobil uygulaması üzerinde kullanıcılarına güvenli ödeme ağ geçitleri ve sahtekârlık tespit araçları sunmakta, güvenli ödeme yapmalarını sağlamaktadır. Flipkart, mobil bulut bilişimden yararlanarak, kullanıcılarına kişiselleştirilmiş ve güvenli bir mobil alışveriş deneyimi sunmayı hedeflemektedir (Google Cloud, 2023b). Bu kapsamda sanal makine, bilgi işlem, depolama ve veritabanı çözümleri kullanmak için sadece Google Cloud'dan değil aynı zamanda AWS ve Microsoft Azure gibi diğer bulut servis sağlayıcılarından da hizmet almaktadır.

2.2.8 Japonya

Japonya'nın önde gelen e-ticaret şirketlerinden biri olan Rakuten, platformunu ve mobil uygulamasının temelini büyük ölçüde bulut bilişime dayandırmaktadır. Microsoft Azure, AWS ve Rakuten Cloud gibi çeşitli bulut bilişim servis sağlayıcıları ile çalışan Rakuten, çoklu bulut stratejisi ile her özel ihtiyaç veya bölge için en iyi bulut sağlayıcısını seçebilmekte, maliyette verimliliği sağlamakta ve farklı bulut bilişim sağlayıcılarının hizmet ve özelliklerine erişebilmektedir. Temel altyapısı için AWS'yi kullanan şirket, ürün listeleme, arama motoru ve sipariş işleme gibi temel uygulamaları barındırmak için sanal makinelerden yararlanırken; büyük miktardaki ürün görseli, kullanıcı verisi ile işlem bilgisini verimli bir şekilde yöneterek depolamaktadır.

Rakuten mobil uygulaması, çeşitli işlevler için bulut hizmetlerinden yararlanmaktadır. Bu doğrultuda, yapay zekâ algoritmaları ile kişiselleştirilmiş önerilerde bulunmak için kullanıcı tercihleri ve satın alma geçmişleri analiz edilmektedir. Bununla birlikte, sipariş durumu ve teslimat bilgileriyle ilgili gerçek zamanlı güncellemeler, hızlı arama sonuçları ile çeşitli kriterlere göre ürün filtreleme kapsamında da bulut bilişimden yararlanılmaktadır.

Platform, veri güvenliğini sağlamak için kullanıcı bilgileri, finansal ayrıntılar ile satın alma geçmişi gibi hassas verileri depolarken şifrelemekte ve bu verilere erişimi yetkili personel ve sistemlerle sınırlandırmaktadır. Bununla birlikte, güvenlik açıklarını

belirlemek için düzenli denetimler gerçekleştirmektedir. Ayrıca faaliyet gösterdiği bölgelerde GDPR ve APAC veri gizliliği yasaları gibi ilgili düzenlemelere uygun hizmet vermektedir. Ek olarak bulut bilişim sağlayıcılarının sunduğu güvenlik hizmetlerinden de faydalanılmaktadır (Rakuten, 2024).

Japonya'da yer alan diğer bir mobil bulut bilişim uygulaması olan taksi çağırma platformu JapanTaxi, mobil uygulamasındaki farklı işlevler için AWS, Microsoft Azure ve Google Cloud'dan yararlanarak hibrit bir bulut yaklaşımı kullanmaktadır. Bulut teknolojisi kapsamında sunulan hizmetler sayesinde kullanıcı yönetimi, yolculuk rezervasyonu ve ödeme gibi temel işlevler ile birlikte gerçek zamanlı konum takibi gibi özelliklerle için kullanılmaktadır. Ayrıca BigQuery ile taksi konum bilgileri, kullanım süresi, kullanıcı bilgileri gibi JapanTaxi hizmetleriyle ilgili çeşitli verileri yönetilmekte ve hızlı bir şekilde işlenmektedir.

JapanTaxi uygulamasının veri güvenliğini sağlamak bulut hizmet sağlayıcılarının sunmuş olduğu güvenlik hizmetleri, şifreleme, iki faktörlü kimlik doğrulama, erişim kontrolleri, potansiyel güvenlik açıklarını belirlemek için düzenli iç ve dış güvenlik denetimleri gibi önlemlerden yararlanmaktadır (Google Cloud, 2019).

2.2.9 Lihtenştayn

Lihtenştayn, bilte teknolojileri, elektronik kimlik ve turizm alanlarında mobil bulut bilişim uygulamaları kullanmaktadır. Bahse konu uygulamalar siber güvenlik açısından ağ ve bilgi sistemlerinin yüksek düzeyde güvenliğinin sağlanması amacıyla alınacak önlemleri belirleyen Siber Güvenlik Kanunu'na tabidir. Bunun yanı sıra, kamu makamları arasında ve kamu kurumları ile bireyler arasında elektronik ticari işlemleri düzenleyen elektronik kimlik E-Devlet Yasası kapsamında değerlendirilmektedir (Sualname, 2023). Ancak söz konusu Kanun'da direkt olarak mobil bulut bilişim özelinde maddeler yer almamaktadır.

Ülkede mobil bulut bilişime ilişkin Avrupa Birliği genelinde ağ ve bilgi sistemlerinin yüksek düzeyde ortak güvenliğine yönelik tedbirlere ilişkin (AB) 2016/1148 sayılı

Direktifi, Avrupa Siber Güvenlik Sanayi, Teknoloji ve Araştırma Yetkinlik Merkezi ve Ulusal Koordinasyon Merkezleri Ağını kuran (AB) 2021/887 sayılı Tüzük ve ISO/IEC 27002:2022; ISO/IEC 27017:2020; BSI C5 2020 standartları kullanılmaktadır (Sualname, 2023).

Mobil bulut bilişimde ülkede, veri koruma ve veri egemenliği gerekliliklerine sürekli uyum sağlamak için bulut bilişime ilişkin kılavuzlar kullanılmaktadır. Bu bağlamda, kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımına ilişkin olarak referans alınan veya kullanılan yönetmelik veya standartlar şu şekildedir (Sualname, 2023):

- 27 Nisan 2016 tarihli ve 2016/679 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (AB),
- Kişisel verilerin suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai yaptırımların infazı amacıyla yetkili makamlar tarafından işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin 27 Nisan 2016 tarihli ve 2016/680 sayılı Avrupa Parlamentosu ve Konsey Direktifi
- ISO/IEC 27002:2022; ISO/IEC 27017:2020; BSI C5 2020

2.2.10 Türkiye

Ülkemizdeki bazı işletmeciler ile sözlü anket yapılarak mobil bulut bilişim uygulamalarına yönelik aşağıdaki bilgiler derlenmiştir.

Mobil bulut bilişim kapsamında, Turkcell Grup Şirketleri çatısı altında yer alan Lifecell Bulut Çözümleri A.Ş. tarafından Suit Drive markası ile kurumsal dosya yedekleme ve yönetim servisi, Lifebox markası ile bireysel bulut uygulaması hizmeti verilmektedir. Şirket, Microsoft Azure, Amazon Web Service ile Huawei Cloud bulut ürünleri ve bu firmalarla yapılan iş birlikleri çerçevesinde kurumsal müşterilerine çeşitli hizmetler sunmaktadır. Ayrıca Turkcell Bulut ürün çatısı altında sanal veri

merkezi, yedekleme ve replikasyon servisleri de verilmekte olup, söz konusu hizmetlerin ISO 27001 ve ISO 27017 standartları da bulunmaktadır.

Turkcell Grup Şirketleri bünyesinde yer alan şirketler tarafından çoklu bulut ürün yönetimi altında yer alan Microsoft Azure, Amazon Web Service ve Huawei Cloud bulut ürünleri, bayilik (reseller partner) sıfatı ile kurumsal müşterilere sunulmaktadır. Bununla birlikte, "reseller partner" sıfatını haiz Turkcell gibi işletmeler bulut hizmet sağlayıcısı olmadığından bu iş birlikleri kapsamında bulut hizmet sağlayıcılarına özgü güvenlik sertifikaları ve uluslararası standartları almamaktadır. Örneğin, Almanya'daki bulut bilişim standardı olan Cloud Computing Compliance Criteria Catalogue ya da ABD'de kurulan Cloud Security Alliance tarafından verilen CSA STAR, CSA CCM gibi sertifikasyonlar gerekli durumlarda bulut bilişim sağlayıcıları tarafından alınmaktadır.

Mobil bulut bilişim hizmeti sunan işletmelerden bir diğeri olan Vodafone'un bu kapsamdaki servisleri şu şekildedir;

- Microsoft 365: Core Office ürünleri ve Lisanslamalarını içeren bir üründür.
- Web Hosting: İnternet barındırma ürünü olup, kullanıcılarına web sitesi barındırma hizmeti sağlamaktadır.
- Domain Registration: Müşterilere alan adı hizmeti sağlamaktadır.
- Vodafone Drive: Bulut ortamındaki güvenli depolama ve uzaktan ortak çalışma ürünüdür.
- Smarter e-Mail: Fiziksel altyapı gerekliliği duymadan bulut ortamı üzerinden sağlanan bir e-posta ürünüdür.
- Public Cloud: Paylaşımlı sanal iş yüklerinin barındırma platformudur.
- Private Cloud: Tek bir kuruluşa tahsis edilmiş bir bulut bilişim ortamıdır.
- Container Platform: Paylaşımlı sanallaştırma üzerinde konteyner barındırma hizmetidir.
- Disaster Recovery: Felaket sonrası kritik bilgi teknolojileri altyapısının, yazılımının ve sistemlerinin operasyonlarını kurtarmak veya sürdürmek için kullanılan politikalar, araçlar ve süreçlerden oluşan bir portföydür.

- VMware Cloud Director Availability: Hizmet olarak olağanüstü durum kurtarma çözümüdür.

Türk Telekom tarafından ise mobil bulut bilişim kapsamında aşağıda yer alan çözümlerin sunulduğu belirtilmiştir;

- Bireysel Dijital Depo: Fotoğraf, video, çalışma dosyası gibi veriler bulut ortamında saklanmakta ve paylaşılabilmektedir.
- Kurumsal Dijital Depo: İşletmeler mobil uygulama üzerinden kurumsal verilerini bulut ortamında depolayabilmektedir.
- TT-posta: Kobiler, büyük şirketler ve kamu kurumları için mevzuata uygun olarak geliştirilen, Türk Telekom veri merkezi üzerinden bulut tabanlı hizmet veren yerli e-posta servisidir.
- Microsoft 365: Word, Excel, PowerPoint, Outlook, Exchange, Teams, OneDrive gibi birçok Microsoft ürününün tek bir yerden yönetilebilmesini sağlayan bir hizmettir. Bulut tabanlı olması nedeniyle tüm veriler bulutta depolanmakta ve her yerden, her cihazdan erişilebilmesine imkân tanınmaktadır.

Bununla birlikte ilgili şirketler, bulut bilişim hizmet sağlayıcısı olarak veri işleyen veya veri sorumlusu sıfatını haiz olduğu tüm faaliyetlerde Kişisel Verilerin Korunması Kanunu hükümlerine ve ikincil düzenlemelere uymakla mükelleftir.

3 KİŞİSEL VERİLERİN KORUNMASI ALANINDA ULUSLARARASI VE ULUSAL DÜZENLEMELER

Kişisel veri, bir bireyi doğrudan veya dolaylı olarak tanımlayan ya da başka verilerle birleştirilerek tanımlayabilme potansiyeli olan ve kişinin bulunmasına olanak sağlayan verilerdir (Schwartz, 2013). Başka bir deyişle, kişisel veri, bireylerin kimliklerini belirli hale getirmeye elverişli olan her türlü bilgiyi içermektedir. Bu kapsamda, kişinin kimlik, iletişim, sağlık ve mali bilgileri ile özel hayatına ilişkin bilgiler de kişisel veri olarak nitelendirilmektedir (Çelik, 2017). Bu tür veriler, dijital çağda büyük öneme sahiptir. Veri, alınıp satılabilen bir araç olarak görülmekte ve özellikle pazarlama şirketleri ile büyük kuruluşlar, müşteri verilerini kullanarak kendilerini geliştirmekte, müşteri beklentilerine uygun planlamalar yapmaktadır.

Ancak, kişisel verilerin işlenmesi konusu büyük bir dikkat gerekmektedir. Bu veriler, birçok düzenlemede özel hayatın gizliliği kapsamında anayasal güvence altına alınmış önemli bilgiler olmakla birlikte, mahremiyete zarar verebilecek potansiyel riskleri içermektedir. Kişisel verilerin işlenmesi sırasında mevcut yasal düzenlemelere uyulması, genel kurallara dikkat edilmesi, gerekli güvenlik önlemlerinin alınması ve kişilerin verilerinin işlenmesi konusunda açık ve anlaşılır şekilde bilgilendirilmesi de gerekmektedir. Veri işleme amacı için başka bir hukuki dayanak bulunmuyorsa, kişisel veriler ancak kişilerin açık rızası alınarak işlenebilmektedir (Paşaoğlu ve Cevheroğlu, 2020). Bu prensiplere uygun olarak hareket edilmesi, kişisel verilerin güvenli ve etik bir şekilde işlenmesini sağlayarak bireylerin gizliliği ile ilgili haklarını korumaktadır.

3.1 Kişisel Verilerin Korunması Hakkındaki Düzenlemelerin Tarihsel Gelişimi

Uluslararası hukuktaki kişisel verilerin korunması kavramının tarihsel gelişimi, bireylerin özel hayatlarına ve mahremiyetlerine saygı gösterilmesi gerekliliği üzerine ortaya çıkan bir değişim sürecini yansıtmaktadır. Bu gelişim, çeşitli uluslararası belgeler, sözleşmeler ve düzenlemeler aracılığıyla gerçekleşmiştir.

Bu sürecin ilk adımı, 1948'de kabul edilen İnsan Hakları Evrensel Beyannamesi ve 1950'de imzalanan Avrupa İnsan Hakları Sözleşmesi ile atılmıştır. Bu belgeler,

bireylerin özel hayatlarına saygı gösterilmesi gerektiğini vurgulayarak kişisel verilerin korunmasına dair temel prensipleri ortaya koymuştur. 1980 yılında kabul edilen OECD Sözleşmesi, kişisel verilerin otomatik işleme tabi tutulmasını düzenleyen ilk uluslararası belge olmuştur. Bu sözleşme, veri koruma ilkelerini belirlese de bağlayıcı bir karakter taşımamıştır (Paşaoğlu ve Cevheroğlu, 2020).

Daha sonra, Avrupa Konseyi tarafından 1981'de kabul edilen 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" ile kişisel verilerin otomatik işleme tabi tutulmasında bireylerin mahremiyetinin korunması amaçlanmıştır. Bu kapsamda, sözleşmeyi imzalayan ülkelere söz konusu anlaşmanın iç hukuka aktarılması yükümlülüğü getirilmiştir. Anılan sözleşme ile uyrukları ne olursa olsun bireylerin mahremiyet hakkına saygı gösterilerek, kişisel verilerin otomatik olarak işlenmesinde de bu mahremiyete saygı gösterilmesi hedeflenmiştir. Sözleşmede kişisel veri, otomatik veri işleme, denetleyici (kontrolör) gibi terimlerin tanımları yapılarak sözleşmenin amaç ve kapsamı belirtilmiştir (Paşaoğlu ve Cevheroğlu, 2020).

Birleşmiş Milletler ise 1990 yılında "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Denetlenmesine İlişkin Rehber İlkeleri" kabul etmiştir. Bu rehber ilkeler ile üye devletlere kişisel verilerin korunması için asgari standartları belirleme çağrısında bulunulmuştur.

Avrupa Birliği (AB) ise 1995 yılında 95/46/AT sayılı "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif"i kabul etmiştir. Bu Direktif, AB ülkelerinde kişisel verilerin işlenmesi ve serbest dolaşımı konusunda temel esasları belirlemiştir. Söz konusu Direktifin yürürlük tarihinden itibaren AB ülkeleri, Direktifte belirtilen kişisel veri koruma standartlarını kendi iç hukuklarına entegre etmeye başlamıştır. Bu süreç ile AB üye ülkelerinin kişisel veri işleme faaliyetlerini daha tutarlı ve koruma odaklı hale getirmeleri amaçlanmıştır.

Direktifin 29'uncu maddesi kapsamında oluşturulan Article 29 Data Protection Working Party adlı çalışma grubu ise veri koruma konusundaki genel yasal

düzenlemeleri ve yükümlülükleri analiz ederek, tavsiye kararları, rehberler ve raporlar yayımlamaktadır. Söz konusu dokümanlar, Avrupa Ekonomik Alanı'ndaki veri sorumlularının, müşterisi bulunan servis sağlayıcıların ve müşterilerin kişisel veri koruma konusundaki sınırlamaları anlamalarına, gerekli teknik ve idari önlemleri almalarına yardımcı olmakta, öte yandan hem işletmelerin hem de bireylerin kişisel verilerin güvenli bir şekilde işlenmesi konusunda uygun önlemleri alabilmeleri için önemli bir kılavuz niteliği taşımaktadır.

Sonraki yıllarda AB ülkelerindeki veri koruma kanunları arasındaki farklılıkların neden olduğu zorluklar ve teknolojideki hızlı gelişmeler, kişisel verilerin daha etkili bir şekilde korunması için birleşik bir yasal çerçevenin gerekliliğini ortaya çıkarmıştır. Bu ihtiyaç doğrultusunda, Avrupa Parlamentosu, 25 Mayıs 2016 tarihinde, kişisel verilerin korunması konusunda son yirmi yılın en kapsamlı düzenlemesi olarak kabul edilen Genel Veri Koruma Tüzüğü'nü (GDPR) onaylamıştır. Bu tüzük, 25 Mayıs 2018 tarihinde, 95/46/AT sayılı AB Veri Koruma Direktifi'ni sona erdirerek yürürlüğe girmiştir. GDPR ile AB veri koruma düzenlemeleri güncellenerek bireylerin verilerinin daha etkin bir şekilde korunması sağlanmıştır (Paşaoğlu ve Cevheroğlu, 2020).

Ülkemizde 24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun tarihçesi ise oldukça uzun bir süreci kapsamaktadır. Bu süreç, hem ulusal hem de uluslararası düzeydeki gelişmeleri içermekte ve kişisel veri koruma konusundaki ihtiyaçları ele almaktadır. 1989 yılında, Türkiye'nin 108 sayılı Avrupa Konseyi Sözleşmesini imzalayan ilk ülkelerden biri olmasının yanı sıra Avrupa Birliği müzakereleri sürecinde kişisel verilerin korunması alanında kanuna ihtiyaç olduğu vurgulanmış ve bir komisyon kurulmuştur. Ancak, bu dönemde hazırlanan taslaklar sonuçlandırılamadan çalışmalar durmuştur. 2004 yılına gelindiğinde ise yeni bir komisyon oluşturularak tasarı hazırlık çalışmalarına devam edilmiştir. Fakat tasarı, seçimlerin gündeme gelmesi nedeniyle yasalaşamamış ve hükümsüz sayılarak 2006’da Başbakanlığa geri gönderilmiştir.

2012 ve 2014 yıllarında, Adalet Bakanlığı bünyesinde yeni bir çalışma grubu kurularak, önceki tasarı, yapılan öneriler ve eleştiriler göz önünde bulundurulmuş ve yeniden ele alınmıştır. Ancak, tekrar seçim süreci nedeniyle tasarı hükümsüz sayılmıştır. Bu aşamadan sonra, Türkiye'de kişisel verilerin korunması konusundaki hukuki boşluğu doldurmak amacıyla yeni bir kanun yapma süreci başlatılmıştır. Bu çerçevede hazırlanan tasarı, 9 Şubat 2016 tarihinde Türkiye Büyük Millet Meclisi (TBMM) Adalet Komisyonu'nda, 24 Mart 2016 tarihinde ise TBMM Genel Kurulu'nda görüşülerek kabul edilmiş ve 7 Nisan 2016 tarihinde "Kişisel Verilerin Korunması Kanunu" yürürlüğe girmiştir. Ayrıca "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetin Sağlanması Hakkında Yönetmelik" ile sağlık alanındaki kişisel veriler, "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" ile de elektronik haberleşme sektörü kapsamında işlenen kişisel veriler üzerine tanımlamalar yapılmıştır (Paşaoğlu ve Cevheroğlu, 2020).

Kişisel Verilerin Korunması Kanunu, Türkiye'deki bireylerin kişisel verilerinin işlenmesini düzenleyen, bu verilerin gizliliğini ve güvenliğini sağlayan, aynı zamanda bu verilere ilişkin hak ve özgürlükleri güvence altına alan bir çerçeve sunmaktadır. Kanun, Türkiye'nin kişisel veri koruma standartlarının uluslararası normlarla uyumlu hale getirilmesi ve bireylerin dijital mahremiyetinin güçlendirilmesi amacını taşımaktadır. Bu kapsamda, "Türkiye Cumhuriyeti Anayasası", "Türk Ceza Kanunu" ve "Kişisel Verilerin Korunması Kanunu"nun ilgili maddelerince belirli yaptırımlar uygulanabilmektedir (Paşaoğlu ve Cevheroğlu, 2020).

Kişisel verilerin korunması kavramının gelişimi, bireylerin mahremiyet haklarına ve kişisel verilerin işlenmesinde şeffaflık ilkesine verilen önemin arttığı bir süreci yansıtmaktadır. Bu gelişmeler, kişisel veri koruma standartlarını yükseltmeyi ve toplumun bu konudaki duyarlılığını artırmayı amaçlamaktadır.

3.2 Kişisel Verilerin Korunmasına Yönelik Uluslararası Düzenlemeler

Bu bölümde uluslararası alandaki kişisel verilerin korunmasına yönelik düzenlemeler ele alınmaktadır.

3.2.1 Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Birleşmiş Milletler Rehber İlkeleri

Birleşmiş Milletler, kişisel verilerin korunması hakkını, 23 Mart 1976 tarihinde yürürlüğe giren Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'sinde "mahremiyet hakkı" altında değerlendirmiştir. Ancak, teknolojik gelişmeler ve bilgisayar kullanımının yaygınlaşması, "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler"in (BM Rehber İlkeleri) yayımlanmasını zorunlu kılmıştır. 14 Aralık 1990 tarihinde yayımlanan bu ilkeler, Birleşmiş Milletler tarafından yapılan ilk doğrudan kişisel veri koruma düzenlemesi olmaları bakımından büyük önem taşımaktadır.

Birleşmiş Milletler, BM Rehber İlkeleri'nde aşağıdaki ilkeleri düzenleyerek önemli bir adım atmıştır:

- Hukuka uygunluk ve dürüstlük ilkesi,
- Doğruluk ilkesi,
- Amacın belirliliği ilkesi,
- İlgili kişinin verilerine erişim hakkının bulunması ilkesi,
- Verilerin güvenliği ilkesi,
- Ayrımcılık yasağı ilkesi,
- Denetim ve yaptırım ilkesi,
- Sınır ötesi veri akışı ilkesi.

Bu ilkeler ile asgari standartlar oluşturularak, üye ülke mevzuatlarında yer alması gereken temel prensiplerin belirlenmesi amaçlanmıştır (Dülger, 2019).

3.2.2 OECD Düzenlemeleri

OECD (Ekonomik İşbirliği ve Kalkınma Teşkilatı), dünya genelindeki ekonomik kalkınma ile ilgili politika analizi ve deneyim paylaşımını teşvik etmek amacıyla 1961 yılında kurulan uluslararası bir kuruluştur. Üye ülkeler arasında ekonomik politikaların koordinasyonu, bilgi paylaşımı, kalkınma politikalarının geliştirilmesi gibi konularda faaliyet göstermektedir.

OECD, ekonomik politika, ticaret, istihdam, eğitim, enerji, çevre, vergilendirme ve bilim gibi geniş bir konu yelpazesinde çalışmalar yürütmekte ve üye olmayan ülkelerle de iş birliği yapmaktadır. OECD'nin rehberlik ettiği ilkeler ile standartlar, uluslararası ticarette ve ekonomik ilişkilerde önemli bir referans kaynağı olmaktadır (Dülger, 2019).

Bu çerçevede, OECD, 23 Eylül 1980 tarihinde "Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler"i (OECD Rehber İlkeleri) kabul ederek uluslararası alanda kişisel verilerin korunması konusunda ilk adımı atmıştır. OECD Rehber İlkeleri, kişisel verilerin korunması konusunda önemli bir referans kaynağı olmuştur. Bu ilkeler, ülkeler arasında benimsendikçe uluslararası alanda bir standart oluşturmuş ve kişisel veri koruma konusundaki temel prensipleri belirlemiştir.

Öte yandan, bu ilkeler bağlayıcılık taşımamakla birlikte tavsiye niteliğinde olup; bu tür kurallar, yumuşak hukuk kuralı (soft law) olarak adlandırılmaktadır. Her ne kadar doğrudan bir bağlayıcılığı olmasa da bu kuralların birçok ülke tarafından benimsenmesiyle birlikte ilgili alanda temel bir başvuru kaynağı olmaktadır (Dülger, 2019). Ayrıca, çevrim içi ve çevrim dışı ortamlarda sınır ötesi veri akışlarının gereksiz kısıtlamalarının önlenmesine katkıda da bulunmaktadır (OECD, 2002).

OECD Rehber İlkeleri'nde ana prensip olarak, veri toplamanın sınırlı olması ilkesi, veri niteliği ilkesi, amacın belirli olması gerektiği ilkesi, kullanımın sınırlanması ilkesi,

veri güvenliği ilkesi, açıklık ilkesi, bireyin katılımı ilkesi, hesap verme zorunluluğu ilkesi yer almaktadır.

Öte yandan, OECD Rehber İlkeleri'nin günümüzde yetersiz kalmasının temel sebebi, bu ilkelerin teknolojideki ilerlemelerin daha az olduğu bir dönemde kabul edilmiş olmasıdır. Örneğin, bireylerin sosyal medya hesaplarından pek çok kişisel bilgiyi ve görseli dünya genelinde erişime açık olarak paylaşmadıkları bir zamanda bu ilkeler belirlenmiştir. Günümüzdeki gelişen teknoloji ve artan internet kullanımı, o zamanlarda öngörülemeyen yeni riskleri ortaya çıkarmıştır (Develioğlu, 2017).

Ayrıca, ilkelerin asıl düzenlenme amacının üye devletlerin ekonomik alanda gelişmesini destekleme odaklı olması, bireylerin kişisel verilerinin korunmasıyla ilgili tüm yönlerin kapsamlı bir şekilde ele alınmamasına neden olmuştur. Bu durum, teknolojinin ve dijital yaşamın hızla evrim geçirmesiyle birlikte ortaya çıkan yeni sorunları ve ihtiyaçları karşılamada zorluklar da oluşturmuştur (Dülger, 2019).

3.2.3 Avrupa Konseyi

Merkezi Strazburg olmak üzere 1949 yılında kurulan ve mevcutta 46 üyesi olan Avrupa Konseyi de kişisel verilerin korunması alanında önemli hukuki metinler yayımlamıştır.

3.2.3.1 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

1960'lı yıllarda bilişim teknolojilerinin ortaya çıkmasıyla birlikte, kişisel verilerin korunmasını sağlamak için daha detaylı düzenlemelere ihtiyaç duyulmuştur. Bu ihtiyacı karşılamak amacıyla Avrupa Konseyi, 28 Ocak 1981 tarihinde 108 No'lu "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ni kabul etmiştir (Council of Europe, 1981).

Bu sözleşme, kişisel verilerin korunması alanında bağlayıcı nitelikteki ilk uluslararası sözleşme olması bakımından büyük bir öneme sahiptir. Sözleşme ile bireyleri kişisel verilerinin işlenmesinden kaynaklanabilecek zararlardan korumanın yanı sıra sınır ötesi veri akışlarının düzenlemesi de amaçlanmaktadır (Giakoumopoulos ve diğerleri, 2018).

108 No'lu Sözleşme hem kamu sektöründe hem de özel sektörde gerçekleştirilen her türlü veri işleme faaliyetlerini kapsamaktadır. Ayrıca kolluk ve adli makamların gerçekleştirdiği veri işleme etkinliklerini de içermektedir. Sözleşme, bu özelliği sebebiyle Avrupa Birliği Genel Veri Koruma Tüzüğü'nden ayrışmaktadır.

Sözleşme ile otomatik işlemeye tabi olan kişisel verilere yönelik, "adil bir biçimde ve yasal yoldan elde edilip işlenmesi", "belirli ve meşru amaçlar için kaydedilmesi ve bu amaçlara aykırı kullanılmaması", "kaydedilmelerinin amaçlara uygun ve yerinde olması ve aşırı olmaması", "doğru olmaları ve gerektiğinde güncellenmeleri gerektiği", "ilgili kişilerin kimliklerini belirlemeye, kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkân verecek bir biçimde saklanması" ilkeleri düzenlenmiştir (Council of Europe, 1981). Bunlara ek olarak, özel veri kategorilerine giren bireylerin ırksal kökenlerini, siyasi düşüncelerini, dinlerini veya diğer inançlarını ortaya koyan kişisel veriler ile sağlık veya cinsel hayatları ve ceza mahkûmiyetleriyle ilgili kişisel veriler, iç hukuka uygun güvenceler sağlanmadıkça otomatik işleme tabi tutulmamaktadır (Giakoumopoulos ve diğerleri, 2018).

Sözleşme kapsamındaki haklar, 9'uncu madde uyarınca iki şekilde sınırlandırılabilmektedir. Bu sınırlamalar, yalnızca taraf devletin kanunlarında öngörülmüş olması durumunda ve demokratik bir toplumda, devlet güvenliğinin korunması; yani kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi ya da ilgili kişinin hak ve özgürlüklerinin korunması için gerekli bir önlem oluşturması hallerinde yapılmaktadır. Ayrıca, sözleşme ile taraf devletler arasında kişisel verilerin serbest aktarımınında, yasal düzenlemelerin bu sözleşme ile getirilen koruma

seviyesini sağlamadığı durumlarda devletlere veri aktarılmasına ilişkin bazı sınırlamalar da getirmektedir (Giakoumopoulos ve diğerleri, 2018).

8 Kasım 2001 tarihinde, 108 No'lu Sözleşme'deki eksikliklere çözüm getirmek amacıyla sözleşmeye ek olarak "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Ötesi Veri Akışına İlişkin Protokol" kabul edilmiştir. Bu Protokol ile taraf olmayan devletlere yönelik sınır ötesi veri akışı ve yerel denetleyici makamların kurulmasının zorunlu hale getirilmesi gibi konular düzenlenerek, 108 No'lu Sözleşme'deki eksikliklere çözüm sunulması amaçlanmıştır (Dülger, 2019).

3.2.3.2 Kişisel Verilerin İşlenmesinde Bireylerin Korunmasına İlişkin Sözleşmede Değişiklik Yapılmasına Dair Protokol (108+)

18 Mayıs 2018 tarihinde kabul edilen "Kişisel Verilerin İşlenmesinde Bireylerin Korunmasına İlişkin Sözleşmede Değişiklik Yapılmasına Dair Protokol" ile 108 No'lu Sözleşme, bilişim teknolojilerinin getirdiği yeniliklere uyumun sağlanması, dijital alanda gizliliğin korunması ve sözleşmenin takip mekanizmalarının güçlendirilmesi amacıyla modernize edilmiştir (Dülger, 2019). Ek Protokol kapsamında, daha etkili bir veri koruma mekanizması öngörülerek; 108 sayılı Sözleşme'de bulunmayan yeni tanımlar eklenmiş ve özel nitelikli veri kategorisi genişletilerek, genetik ve biyometrik verilerin de bu kategoriye dâhil olduğu vurgulanmıştır (KVKK Blog, 2023).

3.2.4 Avrupa Birliği

Avrupa Birliği, kişisel veri koruma alanındaki gereksinimleri karşılamak için geniş bir veri koruma düzenlemesi çerçevesi oluşturmuştur. Bu kapsamda, bu başlık altında Avrupa Birliği'nin kişisel verilerin korunmasına ilişkin politikaları ele alınmıştır.

3.2.4.1 Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin 24 Ekim 1995 tarihli ve 95/46/AT Sayılı Avrupa Parlamentosu ve Konsey Direktifi

95/46/AT sayılı Direktif, Avrupa Parlamentosu ve Avrupa Konseyi tarafından, 24 Ekim 1995 tarihinde kabul edilmiştir. Direktif, Avrupa Birliği'nde kişisel verilerin işlenmesi ve serbest dolaşımı konusunda bireylerin korunmasına yönelik temel yasal düzenleme olarak yer almıştır. Ancak bu Direktif, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesiyle birlikte mülga olmuştur.

Direktif, birçok Üye Devletin iç hukuklarında veri korumasıyla ilgili düzenlemeler yaptığı bir dönemde ortaya çıkmış ve kişisel verilere yönelik daha güçlü bir koruma sağlaması hedeflenmiştir. Aynı zamanda Üye Devletlerin iç hukuklarını uyumlaştırması ve kişisel verilerin serbest dolaşımını kolaylaştırması ihtiyacı da doğmuştur. Direktiflerin doğrudan tüm AB ülkelerine uygulanamaması sebebiyle, yer alan kuralların bu ülkelerin ulusal hukuklarına aktarılması gerekmiştir. Bu kapsamda, Üye Devletlere takdir yetkisi verilmiş; dolayısıyla, Direktif farklı ülkelerde çeşitli şekillerde yorumlanmış ve iç hukuka yeknesak bir şekilde aktarılamamıştır. Sonuç olarak, Direktif, AB'de kişisel verilerin korunmasında tutarlılığı sağlama konusunda başarısız olmuştur (Dülger, 2019).

Genel olarak, Direktif, 108 No'lu Sözleşme ve ulusal hukuklarda bulunan ilkeleri yansıtmakta ve çoğunlukla bu ilkeleri detaylandırmaktadır. Direktif, temel olarak meşruluk ve adillik ilkelerini benimsemekte; kişisel verilerin açık, belirli ve meşru amaçlar için toplanması; şeffaflık, orantılılık, güvenlik ve veri işleme süreçlerinin denetime tabi olması gibi ilkeleri içermektedir. Direktif ve 108 No'lu Sözleşme arasında bir etkileşim de bulunmaktadır. Bu etkileşim, her iki belgeyi de kişisel verilerin korunması açısından olumlu bir şekilde etkilemektedir (Giakoumopoulos ve diğerleri, 2018). Ayrıca 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun hazırlanmasında Direktif önemli bir rehber olmuştur.

3.2.4.2 Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin 12 Temmuz 2002 Tarihli ve 2002/58/AT Sayılı Avrupa Parlamentosu ve Konsey Direktifi (E-Gizlilik Direktifi)

12 Temmuz 2012 tarihinde kabul edilen e-Gizlilik Direktifi, elektronik haberleşme alanında kişisel verilerin güvenliğini, kişisel veri ihlallerinin bildirimini ve bu haberleşmelerin gizliliğiyle ilgili kuralları düzenlemektedir.

E-Gizlilik Direktifi, 95/46/AT sayılı Direktife sıkça atıf yaparak, temelde söz konusu Direktifi tamamlayıcı bir nitelik taşımaktadır. Ayrıca, bu Direktif, üye devletlere ilgili kuralları iç hukuklarına aktarmaları konusunda da yükümlülük getirmektedir (Dülger, 2019).

3.2.4.3 Avrupa Birliği Kurumlarına Yönelik Veri Koruma Tüzükleri

95/46/AT sayılı Direktif, sadece üye devletler için geçerli olması sebebiyle AB kurumları tarafından gerçekleştirilen veri işleme faaliyetlerini düzenlemek amacıyla "Topluluk Kurum ve Organları Tarafından Kişisel Verilerin İşlenmesine İlişkin Olarak Bireylerin Korunması ve Bu Tür Verilerin Serbest Dolaşımına İlişkin 18 Aralık 2000 Tarihli ve (AT) 45/2001 Sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (45/2001 sayılı Tüzük)" kabul edilmiştir. 45/2001 sayılı Tüzük ile genel olarak AB veri koruma rejiminin temel ilkeleri benimsenmiş ve özellikle Birlik organları ile kurumları tarafından işlenen kişisel verilere odaklanılmıştır. Bu doğrultuda, Tüzük çerçevesinde kişisel verilerin işlenmesiyle ilgili standartlar belirlenerek; veri sahiplerinin haklarını korunması ve veri güvenliğinin sağlanması adına önemli düzenlemeler yapılmıştır. Ayrıca, Tüzük kapsamında Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor) adlı bağımsız bir denetim makamı da kurulmuştur. Avrupa Veri Koruma Denetçisi'nin görevleri arasında, veri koruma hukukuyla ilgili düzenlemelerde Birliğe danışmanlık sağlamak, kurumlarda veri koruma hukukunun etkin bir şekilde uygulanmasını sağlamak, denetlemek ve koordinasyonu sağlamak bulunmaktadır (Giakoumopoulos ve diğerleri, 2018).

GDPR'ın yürürlüğe girmesiyle birlikte, 2018 yılında 45/2001 sayılı Tüzük ilga edilmiş ve yerine GDPR ile uyumlu düzenlemeler içeren "Kişisel Verilerin Birlik Kurumları, Organları, Ofisleri ve Ajansları Tarafından İşlenmesine İlişkin Olarak Gerçek Kişilerin Korunması ve Bu Tür Verilerin Serbest Dolaşımına İlişkin 23 Ekim 2018 Tarihli ve (AB) 2018/1725 Sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (2018/1725 sayılı Tüzük)" kabul edilmiştir. Bu yeni Tüzükte, GDPR ilke ve esasları doğrultusunda, kamu sektörünün veri işleme özellikleri dikkate alınarak, AB kurumları ve yetkililerinin işlediği verilere yönelik uyarlamalar yapılmıştır. Tüzükte, genel olarak GDPR hükümleri benimsenmiş ve AB'deki kurumların işleyeceği verilere ilişkin bazı istisnai haller düzenlemiştir. Bu bağlamda, 2018/1725 sayılı Tüzük ile AB veri koruma reformunun önemli bir aşaması tamamlanarak, veri koruma hukukunda daha tutarlı ve modern bir yapıya kavuşulmuştur (Dülger, 2019).

3.2.4.4 Kişisel Verilerin İşlenmesine İlişkin Olarak Gerçek Kişilerin Korunması ve Bu Tür Verilerin Serbest Dolaşımına İlişkin 27 Nisan 2016 Tarihli ve (AB) 2016/679 Sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (GDPR)

95/46/AT sayılı Direktif, bilgi ve iletişim teknolojilerinin görece daha az gelişmiş olduğu bir dönemde kabul edilmiş olması sebebiyle AB, kişisel verilerin korunması alanındaki gereksinimlerin karşılanması ve birlik içinde yeknesaklığın sağlanması amacıyla 2012 yılında bir tüzük çalışması başlatmıştır. Bu çalışmaların sonucunda, 25 Mayıs 2018 tarihinde yürürlüğe giren GDPR ile 95/46/AT sayılı Direktif ilga edilmiştir (KVKK Blog, 2023). GDPR; 11 bölüm, 99 madde ve 173 gerekçeden oluşmaktadır.

GDPR'da kişisel veri; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır. Bu kapsamda, kişinin adı, kimlik numarası, konum verisi veya kişiyi çevrim içi veya fiziksel olarak tanımlayabilen genetik, zihinsel, ekonomik, kültürel veya sosyal bilgiler kişisel veri kavramına girmektedir. Bununla birlikte,

> "*Bu Tüzük kişisel verilerin tamamen veya kısmen otomatik araçlarla işlenmesine ve otomatik olmayan bir dosyalama sisteminin bir parçasını oluşturan veya oluşturması amaçlanan kişisel verilerin otomatik araçlar dışında işlenmesine uygulanmaktadır*."

şeklindeki madde ile de GDPR'ın kapsamı belirlenmektedir (GDPR, 2018).

Ayrıca GDPR çerçevesinde veri işleme faaliyeti, veri sorumlusu ve veri işleyen tanımları da yapılmıştır. Veri işleme, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen herhangi bir toplama, kaydetme, yapılandırma, düzenleme, uyarlama, saklama veya değiştirme gibi faaliyetlerin gerçekleştirilmesi şeklinde tanımlanmıştır. Bununla birlikte; veri sorumlusu, kişisel verilerin işlenmesine ilişkin amaçlar ile yöntemleri belirleyen gerçek veya tüzel kişi, kamu makamı ya da kuruluş olarak ifade edilirken; veri işleyen ise, veri sorumlusu adına kişisel verileri işleyen bir gerçek veya tüzel kişi, kurum ve diğer herhangi bir kuruluş olarak Tüzük'te yer almıştır (GDPR, 2018).

GDPR'da ilk olarak Avrupa Birliği sınırları içerisinde faaliyet gösteren veri sorumluları ve işleyenleri ele alınsa da AB dışında faaliyet gösterenlere de Tüzüğün uygulama alanı bulunmaktadır. Bu bağlamda, bir veri sorumlusu veya işleyen şirketin merkezi ya da faaliyet alanı AB dışındaysa ve bu şirket AB topraklarında bir mal veya hizmet sunumunda bulunuyorsa, olası bir kişisel veri ihlali durumunda GDPR hükümleri uygulanabilmektedir (Dülger, 2019). Böylece GDPR'ın uygulama sınırları oldukça genişlemiştir.

Öte yandan, AB dışında merkezi bulunan sosyal medya şirketlerine yönelik açık bir düzenleme de yer almaktadır. Buna göre, AB'deki veri sahiplerinin davranışlarının Avrupa Birliği içerisinde gerçekleşmesi ve izlenmesi durumunda GDPR uygulanabilmektedir. Bu nedenle AB sınırları içerisinde kullanıcılara sahip olan ve çevrim içi davranışsal reklamcılık faaliyetlerinden yararlanan tüm sosyal medya veya arama motoru şirketleri bu düzenleme sayesinde GDPR'a tabi olmaktadır (Dülger, 2019).

GDPR, Avrupa Birliği ülkeleri genelinde etkili bir kişisel veri koruma standartı oluşturarak, bireylerin verilerini daha iyi kontrol etmesini ve korumasını sağlamayı hedeflemektedir. Bu düzenleme, şirketlere, kurumlara ve diğer veri işleyenlere daha fazla sorumluluk yüklemekte ve bireylere kendi kişisel verileri üzerinde daha fazla hak ve kontrol tanımaktadır. GDPR ile Avrupa'daki kişisel veri koruma düzenlemeleri bir adım ileriye taşınarak, bireylerin mahremiyetinin güçlendirilmesi amaçlanmaktadır.

GDPR'ın kişisel verilerin işlenmesine yönelik temel ilkeleri aşağıda yer almaktadır;

- **Hukuka Uygunluk, Dürüstlük ve Şeffaflık İlkesi:** Hukuka uygunluk, dürüstlük ve şeffaflık kavramları ayrı ilkeler olmasına rağmen, birbirleriyle bağlantılı ve iç içe geçmiş bir yapıya sahiptir. Bu sebeple tek bir ilke gibi görünebilmektedir. İlk defa GDPR ile düzenlenmiş olan şeffaflık ilkesi, ilgili kişinin işlenen kişisel veriler, veri sorumlusu vb. hususlarda anlaşılır ve kolay erişilebilir şekilde bilgilendirilmesini gerektirmektedir.

- **Amacın Sınırlandırılması İlkesi:** Amaçların sınırlandırılması ilkesinde, kişisel veriler açık ve meşru amaçlar doğrultusunda toplanarak söz konusu amaçlara uygun bir biçimde işlenmesi ele alınmaktadır.

- **Veri Minimizasyonu İlkesi:** Bu ilkeye göre kişisel veriler; yeterli, ilgili ve işlendikleri amaç için gerekli olanla sınırlı olmalıdır .

- **Doğruluk İlkesi:** İlke çerçevesinde, kişisel veriler doğru olmalı ve gerekli olduğunda güncel olarak tutulmalıdır. Bu bağlamda, işlenme amaçları göz önünde bulundurularak yanlış olan kişisel veriler gecikmeksizin silinmesini veya düzeltilmesini sağlamak için her türlü makul adım atılmalıdır.

- **Sınırlı Süre Saklama İlkesi:** Sınırlı süre saklama prensibi, kişisel verilerin yalnızca ilgili amacın gerektirdiği süre boyunca tutulmasını belirtmektedir.

İşleme sebeplerinin ortadan kalkması halinde kişisel veriler silinmeli veya anonim hale getirilmelidir.

- **Bütünlük ve Gizlilik İlkesi:** Bu ilkeye göre kişisel veriler; uygun teknik veya idari önlemler alınarak yetkisiz veya yasa dışı işlemeye karşı ve kazara kayıp, imha veya hasara karşı koruma dâhil olmak üzere kişisel verilerin uygun güvenliğini sağlayacak şekilde işlenmelidir.

  Hesap Verebilirlik İlkesi: Veri sorumlusu, Tüzükte düzenlenmiş ilkelere göre davranmalı ve bu uygunluğu gösterebilmelidir. Bu amaçla, veri sorumlusu tarafından uygun teknik ve idari tedbirler alınarak, yapılan tüm işlemler kayıt altında tutulmalıdır (Hukuk ve Bilişim Dergisi, 2022), (GDPR, 2018).

GDPR kapsamında veri sorumlusunun; veri işleme faaliyetlerini gerçekleştirirken uygun teknik ve idari tedbirleri almasına ilişkin birtakım yükümlülükleri aşağıda yer almaktadır;

i. Veri Koruma Politikaları Oluşturulması

Veri sorumlularının oluşturduğu veri koruma politika kuralları, kişisel verilerin işlenme amaçlarını, sorumluluklarını, ana ilkeleri ve terimlerin tanımları ile ilgili konulardaki denetleyici otoriteleri içermektedir. Bu kapsamda, uygun veri politikaları söz konusu sorumlular tarafından uygulanmaktadır (Bhatia, 2023).

ii. Gizlilik Bildirimi

Kişisel verilerin işlenmesiyle ilgili her türlü bilgilendirme, veri sorumlusu tarafından kısa, öz, şeffaf ve kolayca erişilebilir bir biçimde veri sahibine sunulmalıdır. Veri toplama durumunda, veri sahibine, veri sorumlusunun kimlik ve iletişim bilgileri, veri koruma görevlisinin iletişim bilgileri, veri işlemenin yasal dayanağı, varsa meşru menfaat ile ilgili bilgiler, kişisel verilerin alıcıları, kişisel verilerin üçüncü bir

ülkeye/uluslararası kuruluşa aktarılıp aktarılmayacağı ve bu aktarımın güvenceleri hakkında bilgiler verilmelidir.

Ayrıca, kişisel verilerin saklama süresi, belirlenmiş bir süre yoksa kullanılan kriterler, verilerin taşınabilirliği, düzeltilmesi, kısıtlanması ve silinmesi ile ilgili açıklamalar, veri işleme rızasının geri çekilmesi hakkı, şikâyet hakkı gibi konularda da veri sahibine bilgilendirme yapılmalıdır (GDPR, 2018).

iii. Veri Saklama ve İşleme Kayıtları

Veri sorumlusunun, işlenen kişisel verilere ilişkin kayıtları yazılı veya elektronik formatta tutma yükümlülüğü bulunmaktadır. Bu kayıtlar içerisinde, veri sorumlusu ile veri koruma görevlisi bilgileri, veri işleme amaçları, veri sahibi ve kişisel veri kategorileri, yapılan veri aktarımları ve verilerin silinmesine ilişkin süre sınırları gibi açıklamalar yer almalıdır (Dülger, 2019).

iv. Veri Sahibi Rıza Formu

Veri işlemenin rızaya dayalı olduğu durumlarda, rıza talebi ayırt edilebilir, anlaşılır ve kolay erişilebilir bir şekilde, açık ve sade bir dil kullanılarak sunulmalıdır. Rıza, yazılı form dışında elektronik veya sözlü olarak da alınabilmektedir. Bununla birlikte internet sitesi ziyareti sırasında kutu işaretleme yöntemi gibi açık ve net bir şekilde ifade edilen rıza talepleri de geçerli olmaktadır. Ayrıca, her bir işlenen veri ayrı rıza gerektirmekte ve rıza verildiği durumlarda veri sorumlusu kullanıcının rızasının var olduğunu ispatlamalıdır (Dülger, 2019).

Çocuklar için rıza durumunda ise çocuğun en az 16 yaşında olması gerekmekte ve eğer veri sahibi 16 yaşından küçükse, rıza ancak velayet hakkı sahibi tarafından verilmişse veya çocuk tarafından verilip velayet hakkı sahibi tarafından onaylanmışsa geçerli olmaktadır. Bununla birlikte, geçerli bir çocuk rızası için üye devletler 13 yaşından küçük olmamak kaydıyla kanunla daha küçük bir yaş da belirleyebileceklerdir (GDPR, 2018).

v. Veri İşleme Antlaşması

Veri sorumlusu, veri işleme faaliyetinin kendi adına bir başkası tarafından gerçekleştirilmesini istediğinde, özel yazılı bir onay vermelidir. Onayın verildiği durumlarda, veri sorumlusu, veri işleyenin GDPR gereksinimlerini karşılamak üzere teknik ve idari tedbirleri uygulamasını talep etmektedir. Veri sorumlusu ve işleyen, bu tür durumlarda mevzuata uygun olarak, veri işlemenin konusu, süresini, verinin çeşidi gibi konularda yükümlü olmaktadır.

Veri sorumlusu adına gerçekleştirilen işlemin tamamlanmasıyla beraber, veri işleyen, ilgili mevzuatlara göre saklanması gerekmediği sürece, işlenen veriyi silmek veya bu veriyi temin ettiği yere iadeyle yükümlü olmaktadır (Dülger, 2019).

vi. Varsayılan Olarak ve Tasarım ile Veri Koruma (Data Protection By Design and By Default)

GDPR'da varsayılan olarak veri koruma ve tasarımla veri koruma dikkat çeken yenilikler arasındadır. Buna göre veri sorumlusu; teknolojinin geldiği noktayı, uygulama maliyetini ve işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hak ve özgürlüklerine yönelik olarak ortaya çıkardığı değişen olasılık ve ciddiyetteki riskleri dikkate alarak, hem işleme faaliyetine yönelik araçların belirlenmesi sırasında hem de işleme faaliyetinin kendisi sırasında veri minimizasyonu gibi veri koruma ilkelerini etkili bir şekilde uygulamak ve Tüzüğün gerekliliklerini karşılamak ve veri sahiplerinin haklarını korumak için gerekli güvenceleri işleme sürecine entegre etmek üzere tasarlanmış olan takma ad kullanımı gibi uygun teknik ve idari tedbirleri uygulamakla yükümlüdür (GDPR, 2018).

Bu doğrultuda GDPR'ın 25. maddesine göre;

> "*(1) Kontrolör, son teknoloji, uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli olasılıklar ve*

ciddiyetlere sahip riskleri dikkate alarak, hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında, verilerin en alt düzeye indirilmesi gibi veri koruma ilkelerinin etkili bir şekilde uygulanması ve bu Tüzük'ün gerekliliklerinin yerine getirilmesine yönelik olarak gerekli güvencelerin entegre edilmesi amacı ile tasarlanan takma ad kullanımı gibi uygun teknik ve düzenlemeye ilişkin tedbirler uygular ve veri sahiplerinin haklarını korur. (2) Kontrolör, olağan durumda, yalnızca her spesifik işleme amacı için gereken kişisel verilerin işlenmesini sağlamaya yönelik uygun teknik ve düzenlemeye ilişkin tedbirler uygular. Söz konusu yükümlülük toplanan kişisel veri miktarı, bunların işlenme derecesi, saklama süresi ve bunlara erişilebilirliğe uygulanır. Özellikle, söz konusu tedbirler, olağan durumda, bireyin müdahalesi olmaksızın kişisel verilerin belirsiz sayıda gerçek kişinin erişimine açılmamasını sağlar."

hükümleri ile özel ve olağan veri korumasına yönelik unsurlar yer almıştır.

vii. Veri İşlemenin Güvenliği

GDPR'da veri işlemenin güvenliğine yönelik kurallar ve veri işleme faaliyetlerine izinsiz müdahaleyi önlemek için alınması gerekli birtakım tedbirler de düzenlenmiştir. Bu çerçevede, teknolojinin geldiği noktayı, uygulama maliyetlerini ve işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlüklerine yönelik değişen olasılık ve ciddiyetteki riskleri dikkate alarak uygun güvenlik seviyesi sağlamak için veri sorumlularının ve veri işleyenlerin uygun olduğu ölçüde;

- Kişisel verilerde takma ad kullanımı ve şifreleme,
- İşleme faaliyetleri ve hizmetlerinin gizliliği, bütünlüğü, erişilebilirliği ve dayanıklılığının düzenli olarak sağlanması,
- Fiziksel ya da teknik bir problem olduğunda, kişisel verilere erişilebilirliğin gecikmeksizin eski haline getirilmesi,

- İşleme faaliyetinin güvenliğinin sağlanması amacıyla alınan tedbirlerin etkinliğini düzenli olarak test etmeye, değerlendirmeye ve ölçmeye yönelik bir süreç olması

dahil teknik ve idari tedbirler alması beklenmektedir.

viii. Veri İhlali Bildirimi

Kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir risk oluşturması durumunda, veri sorumlusu, kişisel veri ihlalini gecikmeksizin veri sahibine bildirmekle yükümlüdür. Ayrıca veri sorumlusu, ihlale yönelik bilgi aldığı andan itibaren en geç 72 saat içinde, kişisel veri ihlalini yetkili otoriteye bildirmelidir.

Bahse konu hükümler birlikte ele alındığında GDPR'ın mülga 95/46/AT sayılı Direktife kıyasla şeffaflık ve veri güvenliğini daha fazla vurguladığı ve daha güçlü bir veri koruma amaçladığı söylenebilmektedir.

3.3 Ülkemizde Kişisel Verilerin Korunmasına Yönelik Temel Hukuki Düzenlemeler

Kişisel verilerin toplanması, saklanması ve işlenmesi; teknolojik gelişmeler ile birlikte günümüzde oldukça önem kazanmıştır. Ulusal mevzuatımızda bu alanı düzenleyen hükümler ise Kişisel Verilerin Korunması Kanunu'ndan çok daha eskiye dayanmaktadır. Bu bölümde, kişisel verilerin korunmasına yönelik Anayasa, Kişisel Verilerin Korunması Kanunu, Türk Ceza Kanunu ve Elektronik Haberleşme Kanunu ele alınmaktadır.

3.3.1 Anayasa

Anayasa, normlar hiyerarşisinin tepesinde yer almasından dolayı kişisel verilerin korunması alanındaki tüm düzenlemelerin hukuki altyapısını oluşturmaktadır. 1982 Anayasası'nda; özel hayatın gizliliği hakkını düzenleyen 20'nci madde, haberleşmenin gizliliğini düzenleyen 22'nci madde, dini ve vicdani kanaatleri açıklamaya

zorlanamama hakkını düzenleyen 24'üncü madde ve düşünce ve kanaatleri açıklamaya zorlanamama hakkını düzenleyen 25'inci madde gibi kişisel verilerin korunmasına yönelik düzenlemeler yer almaktadır. Özel hayatın gizliliği hakkını düzenleyen 20'nci maddeye göre;

> *"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*
> *Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar."*

Maddenin birinci fıkrası ile kişilik hakkı çerçevesinde tüm vatandaşların özel ve aile hayatının gizliliği hakkı güvence altına alınırken; kişilik ve özel hayatın gizliliği haklarının kapsadığı unsurlar belirtilmemiştir. Bu durum, kişilik hakkı kavramının içerdiği değerlerin, kişilerin günlük yaşamlarındaki ihtiyaçlarının değişmesi ve/veya teknolojinin gelişmesi sonucunda farklılaşacağı gerçeğine dayanmaktadır (Kaya ve Tolun, 2020).

2010 yılında yapılan referandum ile Türkiye Cumhuriyeti Anayasası'nın 20'nci maddesine aşağıdaki üçüncü fıkra hükmü eklenmiştir;

> *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla*

> *işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."*

Anayasa değişikliği teklifinde bu fıkra için gösterilen gerekçede ise;

> *"Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği öngörülmektedir."*

hususuna yer verilerek kişisel verilerin korunmasına yönelik ihtiyacın önemi vurgulanmıştır (Anayasa, madde gerekçesi). Eklenen fıkra ile, bu madde kapsamında kişisel verilerin korunması hakkı, açık bir biçimde Anayasa'da yer almıştır. Ayrıca kişisel verilerin korunmasına ilişkin esasların, kanun ile belirleneceğine yer verilmiş olması da Kişisel Verilerin Korunması Kanunu'nun hukuki temelini oluşturmuştur.

Bu itibarla Anayasa'da, kişisel verilerin korunması hakkının temelini teşkil eden;

- Hukuk devleti ilkesi (m. 2),
- Bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı (m. 17),
- Özel hayatın gizliliği hakkı (m. 20),
- Konut dokunulmazlığı (m. 21),
- Haberleşmenin gizliliği (m. 22),
- Dini ve vicdani kanaatleri açıklamaya zorlanamama (m. 24),
- Düşünce ve kanaatleri açıklamaya zorlanamama (m. 25)

şeklindeki hükümler ile anayasal garantilerin yanı sıra kişisel verilerin korunması hakkına yönelik açık bir hüküm de Anayasa'da yer almıştır (Kılınç, 2012). Böylece

kişisel verilerin korunması hakkı doğrudan düzenleme altına alınmış ve kişilere; bilgilendirilme, verilere erişebilme, bu verileri düzeltebilme ve sildirebilme ile verilerinin ne için kullanıldığını öğrenebilme hakları da tanınmış ve hakkın kapsamı genişletilmiştir (Boz, 2014).

3.3.2 Kişisel Verilerin Korunması Kanunu

Ülkemizde kişisel verilerin korunmasına yönelik kanun çalışmaları, 1989 yılında başlamış ve bir komisyon oluşturulmuş ama bu komisyon çalışmalarını tamamlayamadan dağılmıştır (Aydın, 2014). Akabinde 2000 yılında yeni bir komisyon oluşturulmuş ve bu yeni komisyon kanun tasarısı hazırlamıştır (Korkmaz, 2016). Fakat hazırlanan taslak kanun çeşitli nedenlerle kanunlaşamamıştır. 2008 ve 2014 yıllarında Adalet Bakanlığı öncülüğünde yeni bir tasarı hazırlanıp TBMM'ye sunulmuşsa da yasama döneminin sona ermesi sebebiyle ilgili kanun teklifleri kadük kalmıştır. Nihai olarak ise 26 Aralık 2014 tarihinde TBMM Başkanlığı'na sunulan "Kişisel Verilerin Korunması Kanunu Tasarısı" 24 Mart 2016 tarihinde kabul edilmiştir. Söz konusu tasarı, 7 Nisan 2016 tarihinde Resmi Gazete'de yayımlanmış ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (6698 sayılı Kanun) olarak yürürlüğe girmiştir. Anılan Kanunun kabulü ile ülkemiz mevzuatı açısından önemli bir boşluk doldurulmuştur (KVKK, 2023a).

6698 sayılı Kanun;

- Kişisel verilere ilişkin bütüncül bir kanun bulunmaması ve konuya ilişkin hükümlerin farklı kanunlarda yer alması,
- Ülkemizde kişisel verilerin işlenmesi sürecine ilişkin denetleme ve düzenleme faaliyetlerini yerine getirecek bir kurumun bulunmaması ve bunun bir sonucu olarak, kişisel verilerin yeterli regülasyona ve kontrole tabi olmaksızın birçok kişi veya kurum tarafından kullanılması ve bu durumun bazı hak ihlallerinin yaşanmasına sebep olması,
- Ülkemizin, devam etmekte olan AB tam üyelik sürecinde müzakere fasıllarından bazılarının doğrudan kişisel verilerle ilgili olması,

- AB'nin; Türkiye'nin üyelik sürecine ilişkin olarak hazırladığı ilerleme raporlarında, ülkemizdeki veri koruma alanındaki kanuni boşluğa işaret etmesi,
- AB Kolluk Kuvvetleri İşbirliği Ajansı (Europol), AB Ceza Adaleti İşbirliği Ajansı (Eurojust) ve sair uluslararası kuruluşlar ile iş birliğinin sağlanması ihtiyacı

gibi sorunlara çözüm olmuştur (KVKK, 2018a). Şekil 3.1'de kişisel veri kapsamına giren bilgilere yer verilmektedir.

Şekil 3.1 Kişisel Veri Kabul Edilen Bilgiler

Kaynak: KVKK, 2016.

6698 sayılı Kanun incelendiğinde;

- Birinci bölümde; kişisel verilerin işlenmesinde başta mahremiyet olmak üzere temel hak ve özgürlüklerin korunması saikiyle, veri işleyen gerçek ve tüzel kişilerin uyması gereken yükümlülüklerin belirlenmesinin ve gerçek kişilere ait verilerin korunmasının amaçlandığı görülmektedir (m. 1). İlgili kanunda 3'üncü maddede ise tanımlara yer verilmektedir. Bu kapsamda, kişisel veri

"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi"; veri sorumlusu "*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi*"; veri işleyicisi ise *"veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi"* olarak tanımlanmaktadır.

- Kişisel verilerin işlenmesine ilişkin esasları içeren ikinci bölümde; işleme faaliyetinde uyulması gereken temel ilkelerden bahsedilmektedir (m. 4). Bu ilkeler şunlardır:

  "a) Hukuka ve dürüstlük kurallarına uygun olma.
  b) Doğru ve gerektiğinde güncel olma.
  c) Belirli, açık ve meşru amaçlar için işlenme.
  d) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
  e) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

  Bununla birlikte; ilgili kişinin açık rızasının veri işleme faaliyeti için şart koşulduğu ve açık rıza olmaksızın kişisel veri işlenmesine ilişkin belirtilen istisnaların sınırlı sayıda (numerus clausus olarak) belirlendiği (m. 5), özel nitelikli kişisel verilerin de sayma yöntemiyle belirtildiği ve bu verilerin işlenmesine dair ayrı bir madde ihdas edildiği (m. 6), veri işleme faaliyetini gerektiren sebeplerin son bulması hâlinde veya ilgili kişinin talebi üzerine kişisel verilerin silinme, yok edilme veya anonim hale getirilmesine dair usullerin 7'nci maddede, veri aktarımına ilişkin usullerin ise 8'inci ve 9'uncu maddelerde detaylandırıldığı görülmektedir.

- İlgili Kanun'un üçüncü bölümünde; verileri işlenen ilgili kişilerin hakları (m. 11) ile veri sorumlularına ve veri güvenliğine ilişkin yükümlülükler yer almaktadır (m. 10-12).

- Dördüncü bölümde ise ilgili kişinin yapacağı başvuru ve şikâyet yöntemleri belirlenerek veri sorumlularına, "Veri Sorumluları Sicili"ne kayıt olma şartı getirilmiştir (m. 13). Beşinci bölümde de kişisel verilere ilişkin suçlar bakımından Türk Ceza Kanunu hükümlerinin uygulanması düzenlenirken, bazı maddelerine ilişkin yükümlülüklerin ihlali hakkında idari para cezası verilmesi öngörülmüştür (m. 17-18). Öte yandan veri güvenliğine ilişkin yükümlülükler madde metninde şu şekilde düzenlenmiştir:

  "(1) Veri sorumlusu;

  a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

  b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

  c) Kişisel verilerin muhafazasını sağlamak,

  amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

  (2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

  (3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

  (4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

  (5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."

- Kişisel Verileri Koruma Kurumu'nun yapısı ve görevleri (m. 19-20), Kişisel Verileri Koruma Kurulu'nun yapısı ve görevleri (m. 21-22-23) ile personele

ilişkin hükümler (m. 24-25-26-27) ise Kanun'un altıncı bölümünde düzenleme altına alınmıştır.

3.3.3 Türk Ceza Kanunu

26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nda (TCK), kişisel verilerin işlenmesi hakkında birtakım suçlar düzenlenmiştir. Bu suçlar; Kanun'un özel hükümleri içeren ikinci kitabının, kişilere karşı işlenen suçlara dair hükümlere yer verilen ikinci kısmında yer alan "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünde yer almıştır. Ayrıca 6698 sayılı Kanun'un "Suçlar" başlığı altında yer alan 17'nci maddesi uyarınca da TCK'nın 135 ila 140'ıncı maddelerine atıfta bulunulmuştur.

TCK'nın ilgili bölümünde; haberleşme gizliliğinin ihlal edilmesi (m. 132), kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (m. 133), özel hayatın gizliliğinin ihlal edilmesi (m. 134), hukuka aykırı olarak kişisel verilerin kaydedilmesi (m. 135), hukuka aykırı olarak verilmesi veya ele geçirilmesi (m. 136) ve kanunların belirlediği süreler geçmiş olmasına rağmen kişisel verilerin yok edilmemesi (m. 138) suçlarına ilişkin cezalar yer almaktadır (Ülker, 2016).

TCK'nın topluma karşı işlenen suçlara dair hükümlere yer verilen üçüncü kısmının "Bilişim Alanında Suçlar" başlıklı onuncu bölümünün 243 ve 244'üncü maddelerinde ise bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları için çeşitli cezalar ile bu cezaların ağırlaştırıcı hallerine yer verilmektedir (Şahin, 2011). Ayrıca bahse konu suçlar için TCK 140 ve 246'ncı maddelerinde tüzel kişiler hakkında güvenlik tedbirleri uygulanacağı belirtilmektedir (KVKK, 2023a).

3.3.4 Elektronik Haberleşme Kanunu

10/11/2008 tarihli ve 27050 sayılı Resmî Gazete'de yayımlanan Elektronik Haberleşme Kanunu (EHK), elektronik haberleşme sektörüne yönelik kişisel verilerin işlenmesi ve gizliliğin korunması hakkında hükümler içermektedir.

Elektronik haberleşme ve elektronik haberleşme sektörü tanımlarına bakıldığında, elektronik haberleşme EHK'nın "Tanımlar ve kısaltmalar" başlıklı 3'üncü maddesinin h bendinde şu şekilde tanımlanmıştır:

> *"h) Elektronik haberleşme: Elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesini, gönderilmesini ve alınmasını,"*

Ayrıca elektronik haberleşme sektörü ise bahsi geçen 3'üncü maddenin l bendinde aşağıdaki şekilde tanımlanmıştır:

> "*l) Elektronik haberleşme sektörü: Elektronik haberleşme hizmeti verilmesi, elektronik haberleşme şebekesi sağlanması, elektronik haberleşme cihaz ve sistemlerine yönelik üretim, ithal, satış ve bakım-onarım hizmetlerinin yürütülmesi ile ilgili sektörü,"*

EHK'nın "Kurumun görev ve yetkileri" başlıklı 6'ncı maddesinin birinci fıkrasının (c) bendinde yer alan,

> *"Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak"*

hükmü ile de kişisel verilerin ve gizliliğin korunması, Bilgi Teknolojileri ve İletişim Kurumunun (BTK) görev ve yetkileri arasında sayılmıştır.

Yine, EHK'nın "İşletmeci hak ve yükümlülükleri" başlıklı 12'nci maddesinin ikinci fıkrasında yer alan,

> *"(2) Kurum, işletmecilere sektörün ihtiyaçları, uluslararası düzenlemeler, teknolojide meydana gelen gelişmeler gibi hususları gözeterek aşağıdaki hususlar başta olmak üzere, mevzuat doğrultusunda yükümlülükler getirebilir:*
> *…*
> *d) kişisel veri ve gizliliğinin korunması…"*

hükmü ile kişisel veri ve gizliliğin korunması hususu, sektörde faaliyet gösteren işletmecilere getirilebilecek yükümlülükler arasında sayılmıştır (EHK, 2008).

Öte yandan, AYM'nin 09.04.2014 tarihinde vermiş olduğu karar ile EHK'nın "Kişisel verilerin işlenmesi ve gizliliğin korunması" başlıklı 51'inci maddesi[4] iptal edilmiş ve Anayasa'nın 153'üncü maddesinin üçüncü fıkrası ile 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66'ncı maddesinin üçüncü fıkrası gereğince kararın Resmî Gazete'de yayımlanmasından başlayarak altı ay sonra yürürlüğe girmesine hükmedilmiştir. AYM kararında 51'inci maddenin iptal gerekçesine ilişkin olarak;

> *"Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisini Bilgi Teknolojileri ve İletişim Kurumuna veren itiraz konusu kural, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır."*

açıklamasına yer verilmiştir. Bu bağlamda, hukuki boşluğun oluşmamasını teminen, Anayasa hükmü gereği, elektronik haberleşme sektöründe kişisel veriler özelinde bir kanun hazırlanması ihtiyacı hâsıl olduğu, bu minvalde EHK'nın 51'inci maddesinin yeniden düzenlenmek suretiyle, 27/03/2015 tarihli ve 6639 sayılı Kanunun 32'nci maddesi ile yasama organı tarafından yasalaştırıldığı görülmektedir. Söz konusu madde ile elektronik haberleşme sektörüne özgü kişisel verilerin işlenmesi ve

[4] Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir.

gizliliğin korunmasına yönelik hususlara ilişkin çerçeve çizilmiştir. Maddenin yürürlük tarihi ise 26.01.2015 olarak belirlenmiştir. Ayrıca 19/07/2019 tarihli ve 30836 (Mükerrer) sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 7186 sayılı Kanun ile söz konusu 51'inci maddenin on birinci fıkrasında değişiklik yapılmıştır.

EHK'nın "Kişisel verilerin işlenmesi ve gizliliğin korunması" başlıklı 51'inci maddesi ile Kuruma, elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin kişisel verilerin işlenmesi ve gizliliğinin korunması ile ilgili olarak uyacakları usul ve esasları belirleme görevi verilmektedir. Ayrıca söz konusu maddede temel olarak;

- 6698 sayılı Kanun'da benzer şekilde yer alan ilkelerin veri işleme faaliyetlerinde dikkate alınması,
- Elektronik haberleşmenin ve ilgili trafik verisinin gizliliğinin sağlanması,
- Elektronik haberleşme şebekelerinde, haberleşmenin sağlanması dışında terminal cihazlarında kişisel verilerin saklanması veya bu verilere erişilmesinin ancak kapsamlı bilgilendirme ve açık rıza alınmak şartıyla yapılabileceği,
- İşletmeciler tarafından abonelerine veya kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak için gerekli teknik ve idari tedbirlerin alınması,
- Kanunun 49'uncu maddesi kapsamında veya kamu yararının sağlanması amacıyla Kurum tarafından işletmecilere getirilen yükümlülüklerin yerine getirilebilmesi için kişisel verilerin işlenebileceği,
- Kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak şartıyla, trafik ve konum verilerinin yalnızca ilgili kişilerin açık rızası alınması suretiyle yurt dışına aktarılabileceği,
- Trafik ve konum verilerinin açık rıza aranmaksızın hangi şartlarda işlenebileceği,
- Şikâyet incelemeleri ve denetim faaliyetleri kapsamında trafik ve konum verileri ile kişisel verilerin yapılan işlemle sınırlı olmak şartıyla işlenebileceği,
- Kanun kapsamında sunulan hizmetlerle ilişkin olarak veri saklama sürelerinin ne kadar olacağı,

- İşletmecilerin, tahsilata ilişkin riskin yönetilmesi ve kötü niyetli kullanımların önlenmesi amacıyla abonelerin elektronik haberleşme hizmetlerine yönelik fatura tutarı ve ödeme bilgileri ile sahtecilik, dolandırıcılık riski içeren şüpheli veya zarar doğurucu vakalara ve işlem hareketlerine ilişkin kayıtları işleyebileceği veya diğer işletmecilerle paylaşabileceği,
- Kanun kapsamında kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının temininden işletmecilerin sorumlu olacağı

hususlarının düzenlendiği görülmektedir (EHK, 2008).

3.4 Temel Hukuki Düzenlemeler Kapsamında Mobil Bulut Bilişim

Bulut bilişime yönelik düzenlemeler, ana bileşenlerinden biri olduğu mobil bulut teknolojisini de etkilemektedir. Bu bağlamda, mobil bulut bilişime ilişkin özel bir hukuki düzenleme olmamakla birlikte, yapılan değerlendirmeler bulut bilişim çerçevesinden ele alınmıştır.

3.4.1 Uluslararası Düzenleme Örnekleri

Bulut bilişim, günden güne yaygınlaşarak kullanıcı sayısını giderek artırmaktadır. Birçok kişi ve kurum, her yerden erişilebilirlik, düşük maliyet, ölçeklenebilirlik ve yüksek veri saklama kapasitesi gibi özelliklere sahip olması nedeniyle bulut bilişimi tercih etmektedir.

Bulut teknolojisi, kişisel verilerin korunmasına yönelik düzenlemeler göz önünde bulundurularak değerlendirildiğinde ise işlenen verilerin güvenliği ve mahremiyeti ile ilgili çeşitli sorunların ortaya çıktığı görülmüştür. Bu doğrultuda, bulut bilişim sistemleri ile ilgili uluslararası düzenlemelerin incelenmesi yerinde olacaktır.

a) ABD Bulut Yasası (Cloud Act)

ABD'de 2018 yılında yürürlüğe giren ve kısaca "Bulut Yasası" olarak da bilinen Verilerin Denizaşırı Ülkelerde Yasal Kullanım Şeklinin Netleştirilmesi (Clarifying

Lawful Overseas Use of Data -CLOUD- Act) Yasası ile ABD dışında tutulan verilere erişimin kolaylaştırılması amaçlanmaktadır. Bu yasa, uluslararası pazarda faaliyet gösteren Amerika menşeli şirketlerin işledikleri verilere ilişkin yapılan kamu soruşturmalarında bu verilerin talep edilmesini düzenlemektedir. Bulut Yasası, Amerikan şirketlerinin yurt dışında bulunan verilere daha etkin bir şekilde erişmelerini sağlayarak, hukuki süreçleri düzenlemekte ve uluslararası hukuki süreçlere uyumlu bir çerçeve oluşturmaktadır.

Bulut Yasası çerçevesinde, ABD ile diğer devletler arasında Uygulama Anlaşması (Executive Agreement) imzalanmakta ve böylece, taraf devletlere, sınırları içinde faaliyet gösteren şirketler hakkında doğrudan arama kararı verebilme yetkisi tanınmaktadır. Yasa kapsamında imzalanan Uygulama Anlaşması ile ülkeler, "kalifiye yabancı devletler" (qualifying foreign governments) statüsü kazanmaktadır. Bu yasa, uluslararası düzeyde bilgi paylaşımını desteklerken aynı zamanda veri gizliliği ve güvenliği konularında koruma sağlamayı da hedeflemektedir (Kalender, 2020).

Bulut Yasası yürürlüğe girmeden önce, bulut hizmet sağlayıcıları verilere erişim taleplerine itiraz etme hakkına sahip olduklarından, yurt dışındaki verilere erişim süreci ABD için zorlayıcı bir durum olmuştur. Bu kapsamda, Bulut Yasası'nın yürürlüğe girmesinin nedeni olarak Microsoft'un dâhil olduğu bir dava gösterilmiştir. Söz konusu dava, Microsoft'un veri depolama hizmeti olan Outlook kullanıcısının, ABD hükümetinin mahkeme kararıyla talep ettiği e-posta verilerini teslim etmeme kararı üzerine başlamıştır. Microsoft, kullanıcının e-posta verilerinin İrlanda'daki bir sunucuda depolandığını ve bu nedenle ABD mahkemesi kararının geçerli olmadığını savunmuştur. Microsoft tarafından, yurt dışındaki verilere ABD hükümetinin erişebilmesi için, ABD hükümetinin yabancı bir ülkeden veri talep etmesi ve bu talep doğrultusunda yerel hukuka uygun bir şekilde hareket etmesi gerektiği belirtilmiştir. Söz konusu davada Bulut Yasası'nın kabul edilmesiyle birlikte, ABD hükümeti yurt dışındaki verilere yönelik tekrar erişim talebinde bulunmuştur. Talebin yasal dayanağı olarak Bulut Yasası verilmiş ve Microsoft, yurt dışındaki verilerini ABD hükümetinin erişimine açmak zorunda kalmıştır (Maya, 2023).

b) AB Bulut Davranış Kuralları (EU Data Protection Code of Conduct for Cloud Service Providers)

GDPR'ın 40'ıncı maddesi kapsamında hazırlanan, Bulut Davranış Kuralları (Davranış Kuralları), bulut hizmet sağlayıcılarının GDPR ile uyumunu kolaylaştırmak amacıyla hazırlanmıştır.

Davranış Kuralları, GDPR'ın gerekliliklerini ve kişisel verilerin işlenmesi ile korunmasına yönelik kuralları açıklamaktadır. Bu doğrultuda kurallar, bulut hizmet sağlayıcının veri işleyen şeklinde ifade edildiği ve bulut kullanıcısının ise tüketici olmadığı durumlar için geçerli olmaktadır. Ancak, bulut hizmet sağlayıcının hem tüketici olduğu hem de kişisel veri işleme faaliyetlerinde veri sorumlusu olarak hareket ettiği durumlar için söz konusu kurallar geçerli olmamaktadır (EU Cloud, 2020).

Mobil bulut bilişimde, kişisel veri güvenliğinin sağlanması için ana bileşeni olan bulut teknolojisinin, yalnızca teknik açıdan ele alınması yeterli olmamakta ve bireylerin hakları hukuki yollarla da korunmalıdır. Bu bağlamda, yapılan gizlilik sözleşmeleri, bulut servis ana sözleşmelerinin bir parçası olduklarından, uygulanacak hukuk kuralları genellikle ana sözleşmede belirtilen hükümlere göre belirlenmektedir.

Bulut teknolojisindeki gizlilik sözleşmelerinde tarafların hangi ülkeye mensup olduğuna göre uygulanacak hukuki maddeler de değişmektedir. Eğer sözleşmede yer alan tarafların tabi olduğu hukuk aynı ise, uygulanacak kurallara ilişkin bir ihtilaf söz konusu olmamaktadır. Taraflar arasında farklı hukuk sistemlerinin uygulanması durumunda ise ülkelerden birinin yükümlü olduğu hukukun dışında kalan ve diğer ülkenin hukuk kurallarının geçerli olduğu bir yetki anlaşma yapılsa bile bu anlaşma geçersiz olmaktadır. Söz konusu anlaşma, taraflardan birinin diğer bir ülkenin hukukuna tabi olması halinde, taraflar arasında hangi ülkenin hukukunun öncelikli olacağı konusunda yapılabilmektedir. Bu kapsamda, AB Hukuku'nda bulut bilişim sözleşmelerinde taraflara istedikleri hukuku seçme hakkı tanınmış, ABD'de ise Bulut Yasası ile telekomünikasyon hizmet sağlayıcıları tarafından depolanan verilere ilişkin yasal çerçeve güncellenmiştir.

Ülkemizde ise kişisel verilerin ülke dışına transferi 6698 sayılı Kanun'un 9'uncu maddesinde düzenlemiştir. Söz konusu hüküm gereğince kişisel verilerin yurt dışına aktarılması için kişinin açık rızasının bulunması şart koşulmuştur (Tunç, 2020). Öte yandan ilgili maddenin 2'nci fıkrası çerçevesinde ise kişisel verilerin açık rıza olmaksızın yurt dışına aktarılabileceği durumlar yer almıştır. Buna göre verilerin aktarıldığı ülkede yeterli korumanın bulunması halinde (md. 9/2);

- Kanunlarda açıkça öngörülmesi,
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

hallerinde kişisel veriler yurt dışına aktarılabilmektedir. Ayrıca kişisel verilerin aktarılacağı ülkede yeterli korumanın bulunması halinde, kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri kanunda açıkça öngörülmesi halinde yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın yurt dışına aktarılabilmektedir (KVKK, 2023b).

Bulut bilişim, verilere kimlerin erişebileceği gibi sorular da dâhil olmak üzere kişisel bilgilerin mahremiyeti kapsamında önemli etkiler barındırmaktadır. Mobil bulut

bilişimde de gizlilik ve kişisel verilerin korunmasına ilişkin düzenlemelere uyulmaması; kullanıcı bilgilerinin sızması, verilerin kötüye kullanılması, kimlik hırsızlığı ve bilgi veya verilerin ifşa edilmesi gibi tehdit ya da saldırılara neden olabilmektedir (Alnajrani ve Norman, 2020).

3.4.2 Kişilerin Verilerin Korunması Kanunu'nun Bulut Bilişim Aktörleri Açısından İncelenmesi

Bulut hizmet sağlayıcılarının, sistemin kullanımına yönelik müşterilerine taahhüt ettiği belirli yükümlülükleri bulunmaktadır. Genellikle taahhüt edilen bu yükümlülükler, kullanıcı ile bulut hizmet sağlayıcı arasında imzalanan bulut bilişim sözleşmesinde yer almaktadır. Yapılan sözleşmede, rollerin açıkça belirtilmesi önerilmekte ve böylece taraflar arasında net bir anlaşma sağlanması hedeflenmektedir (EDPS, 2012).

Bu doğrultuda bulut bilişimde; hizmet sağlayıcısı ile müşteri arasındaki gizliliği ve veri koruma yükümlülüklerini tanımlayan gizlilik sözleşmesi büyük önem taşımaktadır. Gizlilik sözleşmesi ile kullanıcıların verilerinin güvenliği ve gizliliği garanti edilmekte ve hizmet sağlayıcısının, bu verileri kullanmasına veya üçüncü kişilerle paylaşmasına izin verilmeyeceği ortaya konulmaktadır (Gitmez, 2023).

Gizlilik sözleşmesi ile taraflar arasında hukuki bir güvence sağlanarak gizliliğin korunması amaçlanmaktadır. Bu bağlamda sözleşmeye taraf olanların, hangi bilgilerin gizli olduğu konusunda anlaşmaları ve bu bilgilerin üçüncü kişilerle paylaşılmaması için karşılıklı rıza uyumunun sağlanması beklenmektedir (Sias, 2008).

Bulut hizmet sağlayıcısı ile kullanıcı arasında yapılan gizlilik sözleşmesinde, sözleşmenin düzenleyicisi genellikle AWS, Microsoft Azure, Google Drive gibi veri sorumlusu olan küresel şirketlerden oluşurken karşı tarafta ise gerçek veya kamu/özel tüzel kişiler yer almaktadır. Sözleşmede, veri sorumlusu tarafından önceden belirlenmiş olan genel hükümler ile ücret, süre gibi konuları içeren tek taraflı hükümler bir araya getirilmektedir. Ancak, teknolojik hayatın gereklilikleri doğrultusunda, sözleşmenin tüm hükümleri veri sorumlusu tarafından karşı tarafla müzakere

edilmemektedir (Gitmez, 2023). Bu bağlamda, ortaya konulan düzenlemeler, standartlar veya yasalar ile kullanıcıların korunması büyük önem taşımaktadır.

Diğer taraftan, kişisel verilerin korunmasına yönelik yapılan düzenlemelerin de gerektiği biçimde uygulanabilmesi adına sözleşmelerde veri sorumlusu ve veri işleyenin yükümlülükleri ile kullanıcı haklarının net bir şekilde belirtilmesi gerekmektedir.

a) Veri Sorumlusunun ve Veri İşleyenin Yükümlülükleri

- **Aydınlatma Yükümlülüğü**: 6698 sayılı anun'da veri sorumlularının temel yükümlülüklerinden biri olarak şeffaflık ve hesap verebilirlik ilkelerinin yansıması olan aydınlatma yükümlülüğü yer almaktadır. Kanun'un 10'uncu maddesine göre;

  "Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;

  a) Veri sorumlusunun ve varsa temsilcisinin kimliği,

  b) Kişisel verilerin hangi amaçla işleneceği,

  c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,

  ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,

  d) 11 inci maddede sayılan diğer hakları,

  konusunda bilgi vermekle yükümlüdür."

Aydınlatma yükümlülüğü ifa edilirken açık ve yalın bir dil kullanılmalı ve muğlak ifadelere yer verilmemelidir. Bununla birlikte ilgili kişilere yanlış veya yanıltıcı bilgiler sunulmamalıdır (Çelikel, 2022).

- **Veri Güvenliği Sağlama Yükümlülüğü:** Veri güvenliğinin sağlanması ile kişisel verilerin korunması arasında yakın bir ilişki bulunmaktadır. İlerleyen teknoloji ve gelişmeler, veri güvenliğini sürekli sağlanması gereken bir yükümlülük haline getirmektedir. Veri güvenliğinin ihlal edilmesiyle, kişisel verilerin tehlikeli kişilerin eline geçmesi ve hukuka aykırı bir şekilde kullanılması durumunda, ilgili kişiler maddi ve manevi olarak zarar görebilmektedir. Bu nedenle 6698 sayılı

Kanun veri sorumlusu tarafından kişisel verilerin hukuka aykırı işlenmesi, erişilmesinin önlenmesi, muhafazasının sağlanması için gerekli olan her türlü teknik ve idari tedbirin alınmasını zorunlu kılmaktadır. Buna göre Kanun'un 12'nci maddesinde "veri güvenliğine ilişkin yükümlülükler" başlığı altında kişisel verilerin güvenliğine ilişkin hükümler bulunmaktadır (Maya, 2023).

- **Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Yükümlülüğü:** Veri sorumlusunun, işleme sebeplerinin kalkmasıyla birlikte, kullanıcının kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi yükümlülüğü ortaya çıkmaktadır. Bu yükümlülük, 6698 sayılı Kanun'un "Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi" başlıklı 7'nci maddesinde belirtilerek, konuya ilişkin usul ve esaslar 28/10/2017 tarihli ve 30224 sayılı Resmi Gazete'de yayımlanan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"te düzenlenmiştir. Genellikle bulut hizmet sağlayıcıları, işledikleri ve depoladıkları bilgileri veri kaybını önlemek amacıyla yedeklemektedir. İlgili taraflar arasında yapılan sözleşmelerde, verilerin yedeklenme sıklığı, bu verilere erişme yöntemleri, verilerin nerede saklanacağı gibi konulara ilişkin maddeler bulunmaktadır. Bu bağlamda, kullanıcının kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesine yönelik bir talebi olduğunda, yedeklenmiş kişisel veriler üzerinde de ilgili talebe uygun bir şekilde silme, yok etme ya da anonim hale getirme işlemi gerçekleştirilmektedir (Tunç, 2020 ve Maya, 2023).

- **Diğer yükümlülükler:** 6698 sayılı Kanun kapsamında bulut hizmet sağlayıcıları için önemli olan diğer bazı yükümlülükler de şu şekildedir;
  - Veri ihlalinin olması halinde veri ihlalini bildirme,
  - Veri işlemeye başlamadan önce veri sorumluları siciline (VERBIS) kaydolma,
  - Kanun kapsamındaki Kurul kararlarına uyma,
  - Veri koruma etki değerlendirmesi yapma (Maya, 2023).

Veri sorumlusu ile veri işleyenin sorumluluk alanı birbirlerinden farklı olmakla birlikte, Kanun'un 12'nci maddesi uyarınca, veri güvenliğine ilişkin önlemlerin alınmasında veri işleyen ile veri sorumlusunun ortak yükümlülüğü bulunduğu belirtilerek, veri işleyene ayrıca bir sorumluluk yüklenmemiştir.

b) İlgili Kişinin Hakları

6698 sayılı Kanun çerçevesinde, ilgili kişinin haklarının da güvence altına alınması amaçlanmaktadır. Kişisel verilerin korunması hakkı, kişilerin kendileriyle ilgili kişisel verilerinin işlenmesini kontrol edebilmelerini sağlamaktadır. Bu hak kapsamında, kişiler kendi verilerine erişebilmekte, bu verilerin düzeltilmesini veya silinmesini talep edebilmekte ya da veri işlemeye itiraz edebilmektedir (Küzeci, 2010).

İlgili kişi veri sorumlusuna başvurarak Kanun'un 11'inci maddesinde yer alan haklarını kullanabilmektedir. Anılan madde çerçevesinde ilgili kişi veri sorumlusuna başvurarak kendisi ile ilgili;

- "*Kişisel verilerinin işlenip işlenmediğini öğrenme,*
- *Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,*
- *Kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,*
- *Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,*
- *Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,*
- *Kişisel verilerin silinmesini veya yok edilmesini isteme,*
- *Kişisel verilerin düzeltilmesi, silinmesi veya yok edilmesine ilişkin işlemlerin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,*
- *İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme*
- *Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etm*e"

haklarına sahiptir (KVKK, 2016).

Kişisel verileri işlenen kişiler, bahse konu haklarına ilişkin başvurularını, Kişisel Verileri Koruma Kurumunun 10/03/2018 tarihli ve 30356 sayılı "Veri Sorumlusuna Başvuru Usul ve Esaslar Hakkında Tebliğ"inde yer alan usul ve esaslara göre yapabilmektedir.

Genel olarak bakıldığında, bulut bilişim hizmetleri kapsamında gerçekleştirilen tüm kişisel veri işleme faaliyetleri 6698 sayılı Kanuna uygun şekilde olmalıdır. Bu kapsamda, bulut hizmet sağlayıcı, veri sorumlusu veya veri işleyen olduğu tüm durumlarda Kanun'daki yükümlülükleri eksiksiz şekilde yerine getirmelidir. Veriler elde edilme anından itibaren Kanun'daki temel ilkelere uygun şekilde işlenmeli, aydınlatma yükümlülüğü yerine getirilerek, kişisel verilerin güvenliğinin sağlanmasını teminen gerekli teknik ve idari tedbirler alınmalıdır. Örneğin, Kişisel Verileri Koruma Kurulu tarafından hazırlanan Kişisel Veri Güvenliği Rehberi'nde bulut bilişim sistemlerindeki kişisel verilerin; kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması, kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerektiği ifade edilmiştir.

Bununla birlikte, bulut bilişim sistemleri üzerindeki kişisel veri işleme faaliyetlerinde, işleme amacına, sınırlarına ve kapsamına karar veren taraf genellikle bulut bilişim hizmet sağlayıcı olmadığından, bulut bilişim hizmet sağlayıcıları çoğunlukla veri sorumlusu değil, veri işleyen niteliğindedir. Nitekim Kişisel Verileri Koruma Kurulu tarafından yayımlanan "Veri Sorumlusu ve Veri İşleyen Rehberi"nde de bulut bilişim sistemlerinde, tüzel kişiler tarafından toplanan verilerin işlenmesi durumunda bulut bilişim hizmet sağlayıcısının veri işleyen, tüzel kişi kullanıcının ise veri sorumlusu olduğu ifade edilmiştir (KVKK, 2018b).

Bu hususa Kişisel Verileri Koruma Kurumu tarafından yayımlanan "Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler" başlıklı rehberde de ayrıca yer verilmiştir. Söz konusu rehberde, uygulama sağlayıcısının her durumda veri sorumlusu olarak kabul edilemeyeceği, bazı durumlarda veri işleyen sıfatını haiz

olabileceği belirtilmiştir. Örneğin; uygulama sağlayıcısı ve geliştiricisinin ayrı kuruluşlar olduğu bir durumda, uygulama sağlayıcısı ile geliştiricisi arasındaki sözleşmeye göre uygulama geliştiricisinin kişisel veri işlemede yalnızca teknik bir rol üstlenmesi ve kendi amaçları doğrultusunda kişisel veri işlememesinin güvence altına alınmasında uygulama geliştiricisinin veri işleyen olarak nitelendirilmesi söz konusu olabilecektir. Mobil uygulamalardan toplanan kişisel veriler genellikle bulutta depolanmakta olup, uygulama geliştiricisi tarafından kullanılan bulut hizmetleri söz konusu olduğunda da veri işleyen sıfatının ortaya çıkması ihtimali gündeme gelebilecektir (KVKK, 2023c).

Bu kapsamda, ülkemizdeki bulut bilişim hizmet sağlayıcıları veri işleyen veya veri sorumlusu sıfatını haiz olduğu tüm faaliyetlerde 6698 sayılı Kanun hükümlerine uymakla mükelleftir.

4 MOBİL BULUT BİLİŞİM KAPSAMINDA KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEHDİTLER VE ALINABİLECEK TEDBİRLER

Veri depolama ve işleme çoğu zaman mobil cihazların dışında gerçekleştiği için mobil bulut teknolojisi, mobil cihazlar aracılığıyla bulut hizmetlerinin kullanımı olarak tanımlanabilmektedir. Bulut sunucuları, teorik olarak sonsuz bir depolama alanı, yüksek hızlı bilgi işlem ve mevcut herhangi bir mobil cihaza göre daha yüksek bir güvenlik sunabilmektedir. Ancak uygulamaların bulut sunucularında yürütülmesi ve kullanıcı verilerinin sahibinin koruma alanından çıkıp buluta girmesi güvenlik ile veri gizliliği açısından birçok zorluğu da beraberinde getirmektedir. Ayrıca, internet hizmetlerin kullanımının artması, kişisel verilerin istismarına yönelik siber saldırılarda da büyük bir artışa neden olmaktadır. Mobil bulut bilişim hem bulut teknolojisine hem de mobil bilgi işleme dayalı olduğundan, hizmet sağlayıcıların güvenli bir ortam sağlamak için mobil cihaz, şebeke ve bulut bilişim güvenliğine yönelik tehditlerin ele alınması gerekmektedir.

Bununla birlikte, pazara giriş engellerinin oldukça az olması nedeniyle, kısa zaman dilimlerinde giderek daha fazla mobil uygulama tasarlanmaktadır. Bu durum, yazılımcıların ürün geliştirme aşamalarında uygulamanın güvenlik yönünü ihmal etmesine yol açabilmektedir. Piyasada bulunan çok çeşitli donanım cihazları nedeniyle geliştiriciler için yazılım yaması oluşturmak zor olduğundan, geliştiricilerin ana odak noktası işletim sistemi için yama altyapısı geliştirmek yerine ana işlevselliği sağlamaya devam etmektedir. Ayrıca Android platformunun esnekliği mobil uygulamalarda saldırı olasılığını artırmaktadır. Çeşitli virüsler, güvenlik açıkları, kimlik avı saldırıları, sahtecilik ve diğer kötü niyetli faaliyetler uygulama pazarını bozmakta ve kullanıcı güvenliğini etkilemektedir (Gu ve Guirguis, 2014).

Finans, sağlık ve oyun gibi çevrim içi sektörler için de mobil buluta dayalı uygulamaların güvenliği büyük bir endişe kaynağıdır. Günlük hayatımız için gerekli olan uygulamalarda, küçük bir güvenlik sorunu hem işletmeler hem de bireyler için paha biçilemez ekonomik ve itibar kaybına neden olabilir. Bu sorun, mobil

uygulamaların geliştirilmesi veya piyasaya sürülmesine ilişkin ulusal düzenlemelerin veya endüstri standartlarının eksikliğinin yanı sıra start-up kültürünün yaygınlaşması nedeniyle daha da büyümektedir.

Diğer taraftan, mobil bulut teknolojisinin çerçevesi göz önüne alındığında; saldırganlar, geleneksel istemci-sunucu mimarilerine göre çok daha geniş bir kaynak/protokol yelpazesini hedefleyebilmekte ve bunları tehdit edebilmektedir. Örneğin, kötü niyetli kişiler mobil cihazdaki güvenlik açıklarından (mobil uygulamalar, mobil işletim sistemleri ve mobil şebeke) veya bulut bilişim kapsamındaki (bulut yönetimi, bulut sanallaştırma ve bulut erişim protokolleri) güvenlik açıklarından faydalanabilmektedir. Yapılan saldırılar, kişisel bilgilerin ifşa edilebileceği, bilgi işlem görevlerinin kötü niyetli olarak değiştirilebileceği ve mobil kullanıcılar için bulut hizmetlerinin devre dışı bırakılabileceğini göstermektedir ki bu durum, mobil bulut bilgi işlemi içeren güvenlik konularının incelenmesinin önemini vurgulamaktadır (Aery, 2016).

4.1 Mobil Bulut Bilişimde Güvenlik Tehditleri

Mobil cihazlar, anlık ve tam zamanlı hizmet almada kişiler için varsayılan bir araç haline gelmiştir. Çoğu mobil bulut bilişim platformu, uygulamaların ve hizmetlerin mobil şebeke üzerinden kullanıcılara sağlarken güvenlik faktörünü de göz önüne alarak tasarlanmıştır. Mobil bulut ile kullanıcılar güvenlik problemlerinin tespiti ve kötü amaçlı yazılımların önlenmesi konularında bulut bilgi işlemin avantajlarından yararlanılabilmektedir. Ancak bu durum bulut tabanlı uygulamaların ve hizmetlerin kötü amaçlı yazılım tehlikesinden tamamen kurtulduğu anlamına gelmemekte, sadece bulut hizmetlerinin manipüle edilmesi ve kötü amaçlı yazılım uygulamalarının dağıtılması daha zorlaşmaktadır. Bulutta bulunan uygulamalar ve hizmetler, istemci terminallerinde karmaşık virüsten koruma ile kötü amaçlı yazılım programlarının yüklenmesini ve bakımını gereksiz kılmaktadır. Ancak yine de mobil cihaza yönelik bazı önlemler ekstra koruma olarak alınmaktadır.

Mobil bulut bilişimde ortaya çıkan güvenlik ve mahremiyet sorunları, geleneksel bulut bilişime göre daha değişkendir. Mobil bulut bilişim, geleneksel bulut bilişimin güvenlik tehditlerini devralırken; aynı zamanda, kablosuz iletişim kanalları aracılığıyla kullanılan mobil cihazlara özgü problemleri de barındırmaktadır. Mobil bulut teknolojisi kullanılarak oluşturulan uygulamalar karmaşıklığı ve her bir işlemin yürütme yolları ile konumlarının dikkate alınmasını gerektirdiğinden, mobil bulut uygulamaların güvenliğini sağlamak zor olmaktadır. Ayrıca mobil cihazların, kaynak sınırlamaları ve karmaşık algoritmaları yürütmek için işleme yeteneğinin olmaması nedeniyle de bilgisayarlara kıyasla yoğun hesaplamalı kötü amaçlı yazılımdan koruma uygulamaları bu cihazlara yüklenememekte veya çalıştırılamamaktadır. Bu nedenle, bulut bilişim ortamı için önerilen güvenlik algoritmaları doğrudan bir mobil cihaz üzerinde çalıştırılamamaktadır.

Mobil bulut bilgi işlemin güvenliği çok çeşitli yönleri kapsamakta ve buluttaki tüm bileşenleri etkilemektedir. Bu güvenlik sorunları; kullanıcıların kişisel verilerinin gizliliği ve mahremiyeti, hesaplamanın bütünlüğü, bulut hizmetlerinin kullanılabilirliği, hesaplama ve bilgi yönetiminin denetlenmesi ile kaynakların tahsisini de içermektedir.

Bütünlük sorunu, mobil cihazların daha az güvenilir olması ve mobil uygulamaların buluta yüklenmesi nedeniyle ortaya çıkmaktadır. Güvenilmeyen cihazlardan ve devre dışı bırakılmış uygulamalardan elde edilen hesaplama sonuçlarının doğrulanması gerekmektedir. Gizlilik sorunu ise kodun ve verilerin bulut ile paylaşılmasından kaynaklanmaktadır. Bilgiler bulutta yedeklendiğinden, mobil cihazlardaki kişisel veriler gibi kritik bilgilere buluttan erişilebilmektedir. Akıllı telefonların yaygınlaşmasıyla birlikte, mobil bulut gizlilik sorunu daha karmaşık ve ciddi bir hal alacaktır. Kullanılabilirlik sorunu ise sınırlı kaynaklar nedeniyle mobil bilgi işlemin doğasından gelmektedir. Saldırganlar, bulutta konuk sistemler için kullanılması gereken kaynakları tüketebilmektedir (Gu ve Guirguis, 2014).

Öte yandan, güvenlik ve performans arasındaki denge de korunmalıdır. Mobil bulut bilgi işlemde, yüklenen mobil uygulamalar ile verilerin şifrelenmesi, kullanıcıların

kimliğinin doğrulanması, kimlik bilgilerinin güncellenmesi gibi işlemler gerçekleştirilirken mobil cihazlar ve bulut arasındaki güvenilir ilişkiyi sürdürmek için ekstra koruma prosedürleri gerekmektedir. Ancak güvenlik işlevlerinin gerçekleştirilmesi, kimlik bilgilerinin tutulması gibi görevler daha fazla kaynağa ihtiyaç duymakta ve işlem süresi ile güç tüketimi açısından ek bir yük getirmektedir (Gu ve Guirguis, 2014).

Mobil bulut bilgi işlem mimarileri, geleneksel bilgi işlem sistemlerine göre daha farklı ve daha geniş bir saldırı yelpazesine karşı savunmasızdır. Bu kapsamda, mobil uygulama, kullanıcı, cihaz ve bulut güvenliğini etkileyebilecek aşağıda yer alan güvenlik sorunları ile karşı karşıya gelmektedir;

- Hizmet dışı bırakma saldırısı (Denial of Service, DoS), ağın çok fazla trafik verisiyle doldurarak cihazların ağ hizmetine erişiminin reddedilmesini içermektedir. Bu saldırı türü, kaynaklarını aşırı yükleme ve erişilemez hale getirme girişiminde birden fazla kaynak kullanılarak bir cihaza veya ağa büyük hacimli istekler gönderilerek gerçekleştirilmektedir. Saldırganın amacı, cihazı veya ağı kullanılamaz hale getirerek hizmetlerin kesintiye uğramasına ve erişilebilirlik kaybına neden olmaktır. Saldırı, cihazı trafikle doldurmak, ağdaki güvenlik açıklarından yararlanmak veya bağlı cihazların kontrolünü ele geçirmek için yazarlı yazılım kullanmak da dâhil olmak üzere çeşitli teknikler kullanılarak gerçekleştirilebilmektedir (Chinanu ve diğerleri, 2018).
- Kimlik sahtekârlığı saldırıları, ağdaki başka bir cihaz veya kullanıcı gibi davranma eylemini ifade etmektedir. Saldırı ile ağ kaynaklarının sahte düğümler tarafından tüketilmesi sonucunda meşru düğümler için büyük bir hizmet reddine neden olabilmektedir (Chinanu ve diğerleri, 2018).
- SQL (Yapısal Sorgulama Dili, Structured Query Language) enjeksiyonu saldırıları, veri tabanlarının güvenliğini hedefleyen bir tür uygulama katmanı saldırısıdır. Bu saldırı, bir veri tabanı sorgusuna zararlı SQL kodunun enjekte edilmesini içermektedir. Zararlı kod daha sonra çalıştırılarak saldırgana parola, kimlik bilgileri veya diğer hassas verilere erişim imkânı sağlayabilmektedir.

Saldırgan bu bilgileri sisteme erişmek veya verileri değiştirmek için kullanabilmektedir (HaddadPajouh ve diğerleri, 2021).

- Veri sızıntısı, hassas verilerin, internette ya da kaybedilen sabit disk veya cihazlar sebebiyle yanlışlıkla ifşa olmasıdır. Bu durumda, saldırganlar bir çaba göstermeden hassas verilere yetkisiz erişim elde edebilmektedir (Binglaw, 2021).
- Siteler arası komut dosyası çalıştırma saldırısı (Cross-Site Scripting, XSS), web uygulamalarını etkileyen bir tür güvenlik açığıdır. Bu tür bir saldırıda, bir saldırgan diğer kullanıcılar tarafından görüntülenen bir web sayfasına zararlı kod enjekte etmekte ve bu kod daha sonra kullanıcıların tarayıcılarında zararlı kodu çalıştırabilmektedir. Böylece, saldırganın oturum açma kimlik bilgileri veya diğer kişisel veriler gibi hassas verileri çalmasına veya zararlı yazılım yaymak veya web uygulamasının çalışmasını bozmak gibi diğer kötü amaçlı faaliyetler gerçekleştirmesine olanak sağlayabilmektedir (Binglaw, 2021).

Bahse konu güvenik sorunları aşağıdaki nedenlerden kaynaklanmaktadır;

Sınırlı kaynaklar: Büyük teknolojik gelişmelere rağmen, mobil cihazlar, normal bilgisayarlarla karşılaştırıldığında hesaplama, ağ, depolama ve güç yetenekleriyle hâlâ sınırlıdır. Bu durum mobil cihazları gerekli güvenlik uygulamalarını çalıştırmasını engellemekte ve onları saldırılara karşı savunmasız bırakmaktadır. Örneğin, şebeke trafiği dinleme araçları ve izinsiz giriş tespit sistemleri cihazın performans ömrünü kısaltacak kadar çok kaynak tüketebilmektedir. Bu nedenle, güvenlik ve performans arasında doğal bir denge bulunmaktadır.

Depolama ve hesaplama için birden çok konum: Mobil cihazlardan alınan veriler genellikle buluta yüklenmekte ve depolanmaktadır. Ayrıca, kapsamlı hesaplama işlemleri de buluta yürütülmekte ve boşaltılmaktadır. Böylece veriler birden çok konumda (mobil cihaz, bulut uygulaması gibi), saldırılara karşı savunmasız hale gelmektedir. Ayrıca, verilerin aktarımında kullanılan bağlantılar saldırganlar tarafından hedef alınabilmektedir. Temelde saldırgan, gizli bilgilere erişmek veya hesaplamanın bütünlüğünü tehlikeye atmak için zincirdeki en zayıf halkayı

hedefleyebilmektedir. Üçüncü tarafların katılımı bu sorunları daha da karmaşık hale getirmektedir (Gu ve Guirguis, 2014).

Hizmet olarak mobilite: Mobil bulut bilgi işlem, kullanıcılara hizmet olarak mobilite sunan bulut bilişim sağlayıcılarına ek olarak, hesaplama işlemlerinin farklı bulutlar arasında taşınması yeteneğine de sahiptir. Kötü niyetli kullanıcılar, bulutun özelliklerini (örneğin, bulut topolojisi, darboğaz bağlantıları ve makinelerdeki yük) öğrenerek, belirli kaynakları (örneğin darboğaz bağlantıları) hedef alan gelişmiş saldırılar başlatabilmektedir. Bulut mimarilerindeki mobilite, yeni tehditleri de ortaya çıkarmaktadır.

Mobil cihazlar, anlık hizmet almak için varsayılan araç haline gelmiştir. Bu nedenle, çoğu mobil bulut bilişim platformu, mobil şebeke üzerinden kullanıcılarına uygulama ve hizmetler sağlamak için güvenlik önlemleri alınarak tasarlanmıştır. Mobil bulut bilişim, kullanıcılarını koruyabilecek izleme, güvenlik tespiti ve kötü amaçlı yazılım önleme konularında bulut bilişimin avantajlarından yararlanılmaktadır. Ancak bu durum, bulut tabanlı uygulama ve hizmetlerin kötü amaçlı yazılım tehlikesinden tamamen arındığı anlamına gelmemektedir. Sadece saldırganların, bulut servis sağlayıcılarını ve hizmetlerini manipüle etmek için kötü amaçlı yazılımları dağıtmaları daha da zorlaşmaktadır (Gu ve Guirguis, 2014).

Uygulamalar ve hizmetlerin bulutta yer alması, istemci terminallerine karmaşık anti-virüs ve kötü amaçlı yazılım yazılımlarının yüklenmesini gereksiz kılsa da bazı cihaz içi korumalar ekstra bir güvenlik önlemi olarak alınmaktadır. Mobil bulut için mevcut güvenlik endişesi öncelikle akıllı telefon ve tablet platformlarına yönelik tehditlerdir.

a) Mobil Cihaz Güvenliği

Mobil cihazlar değerli kişisel bilgileri (fotoğraflar, kişi listeleri ve iletişim geçmişi gibi) ve ayrıca kritik uygulama verilerini (örneğin sağlık kayıtları ve kredi kartı bilgileri) taşımaktadır. Bir mobil cihaz yanlış ellere geçtiğinde (kısa bir süre için bile olsa), saldırganlar kullanıcının mahrem bilgilerini elde edebilmektedir.

Bu doğrultuda, mobil uygulamalar tarafından işlenen kişisel verilerden bazıları aşağıda yer almaktır (KVKK, 2023c);

- Kimlik bilgileri (ad ve soyadı, T.C. kimlik numarası, doğum tarihi vb.),
- Üyelik bilgileri (kullanıcı adı, parola vb.),
- İletişim bilgileri (ev adresi, telefon numarası, e-posta adresi vb.),
- Finansal bilgiler (IBAN, kredi kartı numarası vb.),
- Kullanıcı etkileşimleri (arama geçmişi, uygulama içi satın alımlar vb.),
- Konum bilgisi,
- Telefon rehberi veya uygulamalardaki arkadaş listeleri,
- Biyometrik veriler (yüz tanıma verisi, parmak izi verisi, ses izi biyometrisi vb.),
- Uygulamanın sağlık ile ilgili olması durumunda sağlık verileri (kalp atış hızı, uyku düzeni vb.),
- Cihazın kamerası ve galerisine erişim izni verilmesiyle toplanan görsel veriler,
- Mesajlaşma platformlarından toplanan metin verileri.

Mobil cihazlardaki kullanıcı gizliliğiyle ilgili belki de en önemli olaylardan biri, 2011 yılında yaşanan Carrier IQ adlı yazılımın, kullanıcının akıllı telefondaki etkinliklerini (ziyaret edilen web sayfaları, gönderilen metinler, hatta basılan tuşlar dahil) izinsiz bir şekilde izleme yeteneğine sahip olduğunu fark edilmesidir. Başta Amerika Birleşik Devletleri'nde olmak üzere yaklaşık 150 milyon cep telefonunun Carrier IQ yazılımından etkilendiği tahmin edilmektedir. Söz konusu olayda, şebeke güvenilirliğini artırmak amacıyla donanım ve şebeke performansını izlemek için Carrier IQ'nun kurulumu belirli mobil operatörler tarafından kullanılmış, ancak bu operatörlerden bazıları (T-Mobile, Sprint ve AT&T dâhil), yazılımın kullanıcının kişisel verilerini elde etmek için kullanılmadığını savunmuştur (Medium, 2019).

Mobil cihazlara yönelik bazı tehditlere aşağıda yer verilmektedir.

- **Fiziksel Tehditler**

Mobil cihazlara yönelik fiziksel tehditler, cihazın ödünç verilmesi, kaybedilmesi veya çalınması ile ortaya çıkmakta, böylece bir başkası kullanıcının rızası olmadan verilere veya uygulamalara erişebilmektedir. Mobil cihazlar parola tabanlı kilitleme özelliğine sahip olsa da bu özellik genellikle cihaz sahipleri tarafından kullanılmamaktadır. Ayrıca bu özellik etkinleştirildiğinde bile, parolayı aşmanın sayısız yolu bulunmaktadır. Buna ek olarak, mobil cihazlara yüklenen uygulamalar genellikle bulut hizmetleri ile verilere doğrudan ve otomatik erişim sağlamaktadır (Chang ve diğerleri, 2013).

- **Kötü Amaçlı Yazılım Tehditleri**

Güvenlik açısından bakıldığında, mobil cihazlar çok çeşitli teknolojileri kullanarak birbirleriyle ve dış dünyayla yakından etkileşim kurmaktadır. Akıllı cihazların hayatımızdaki yerinin artmasıyla kötü amaçlı yazılım üreticilerinin ilgisi de giderek büyümüştür. Bu cihazların sayısı artmaya devam ettikçe, mobil cihazlar web tabanlı tehditler olarak yalnızca virüsler ve botnetlerle değil, aynı zamanda kötü amaçlı yazılımlar ile sosyal ağlardan gelen kimlik avı, kimlik hırsızlığı ve spam gibi ciddi güvenlik sorunlarıyla da karşı karşıya kalmıştır. Öte yandan, mobil kullanıcılar çevrim içi ödeme, sosyal ağ vb. mobil uygulamaları kullanırken kritik kişisel ve kurumsal bilgiler depolanmakta ve aktarılmaktadır. Bu kapsamda, kötü niyetli kişiler, kullanıcıların verilerini tehlikeye atabilecek saldırılar gerçekleştirebilmektedir.

Son yıllarda, mobil işletim sisteminden yararlanarak kullanıcıların gizliliğini tehdit eden kötü amaçlı yazılımlar çoğalmıştır. Kötü amaçlı yazılım, kullanıcı bilgilerini toplayarak ve uzak bir sunucuya göndererek arka planda çalışmaktadır. Genel olarak, bir saldırgan kötü amaçlı yazılım aracılığıyla bir mobil cihazda kök izinleri elde ederse, diğer uygulamaların yanı sıra işletim sistemlerinin hesaplama bütünlüğünü (örneğin, yanlış algılama bilgileri veya sonuçları sağlamak gibi) etkileyebilmektedir. Ayrıca bir mobil cihazı kontrol edebilen kötü amaçlı yazılım, diğer uygulamaları

tehlikeye atmak ve gerçekleştirilen hesaplamanın bütünlüğünü etkilemek için de düzenlenebilmektedir.

Bununla birlikte, kullanılabilirlik söz konusu olduğunda, mobil cihazlardaki kablosuz iletişim doğası gereği parazit ve karıştırma saldırılarına karşı da savunmasızdır. Saldırganlar, cihazın amaçlanan sinyalleri almasını engellemek için donanım bozucular edinebilmektedir. Birçok mobil cihaz, iletişim için bir kablosuz arabirim kullanması dolayısıyla saldırganların kablosuz bağlantıyı doyuracak büyük miktarda trafik göndererek arabirimdeki diğer bilgilerin iletilmesini önlediği geleneksel hizmet dışı bırakma (DoS, Denial-of-Service) saldırılarının yanı sıra Medya Erişim Kontrolü (MAC, Media Access Control) katmanında da çok çeşitli saldırılara maruz kalabilmektedir. Kullanılabilirliği hedefleyen başka bir saldırı biçimi ise yalnızca mobil cihazın gücünü boşaltmak için önemsiz yönergeleri yürüten kötü amaçlı yazılımlardır (Gu ve Guirguis, 2014).

Mobil bulut bilişim, akıllı cihazların popülaritesi tarafından yönlendirilen gelişmekte olan bir pazar olmakla beraber, bulut tabanlı uygulamalar, geleneksel uygulamalardan birçok yönden farklılık göstermektedir. Kimlik katmanı, kullanıcı başına her zamankinden daha fazla uygulama olması ve hizmetlerin her yerden erişilebilmesi nedeniyle çok daha zor olmaktadır (Chang ve diğerleri, 2013).

Ayrıca mobil bulut bilişimin bir avantaj olarak sunduğu mobilite beraberinde birtakım mahremiyet sorunları da getirmektedir. Bu bağlamda en temel problem, çok sayıda uygulamanın kullanılabilir olmasıyla birlikte bu uygulamaların güvenilirliğidir. Öte yandan, mobil cihazlardan üçüncü kişilere özel bilgi toplanması veya uygulamaların arka planında tehlikeli yazılımlar barındırması da başlıca risklerdendir.

Bununla birlikte ücretsiz mobil uygulamalar genellikle reklamlara bağlıdır ve reklamlar kişisel bilgi gerektirmektedir. Reklamların kaldırılması içinse birçok uygulama ücret talep etmektedir. Çözüm olarak ise kullanıcılara daha fazla kontrol ve seçenek sunulmaktadır. Böylece kullanıcıların, mobil uygulamaların hangi bilgileri

topladığını ve gönderdiğini, yani mobil uygulamaların şeffaflık konularını bilmelerine izin verilmektedir (Karthik ve Manhar, 2020).

Ayrıca mobil cihazlar ve bulut hizmeti sağlayıcıları arasındaki iletişimi destekleyen kablosuz kanallar gizli dinleme, kimliğe bürünme saldırısı, tekrarlama saldırısı (replay attack), ortadaki adam (man-in-the-middle) saldırısı ve DoS gibi birçok türdeki saldırıya karşı savunmasızdır. Öte yandan, erişim dolandırıcılığı ve abonelik dolandırıcılığı gibi mobil şebekelerde başka tehditler de bulunmaktadır.

Mobil bulut bilişim, doğası gereği yüksek düzeyde sanallaştırılmıştır. Bu nedenle, farklı bulutlardaki kimlikleri kontrol etmek ve yönetmek için yeni yaklaşımların geliştirilmesi gereklidir (Chang ve diğerleri, 2013).

b) Bulut Bilişim Güvenliği

Bulut bilişim kapsamında depolanan veriler, bu gibi problemleri içermese de kendine özgü bazı mahremiyet sorunları mevcuttur;

- Kullanıcılar fiziksel olarak kendi veri depolarına sahip değildir ve bu nedenle verilerin korunmasından bulut bilişim sağlayıcıları sorumludur.

- Veriler harici olarak tutulduğunda, veri gizliliği ile ilgili konular bulut sağlayıcısının elindedir ve bulut hizmeti sunucusu çok fazla kişisel veri toplamaktadır.

- Bir kullanıcı bulut sağlayıcısını değiştirdiğinde, veri geçişi bir sorun haline gelmektedir. Yeni bulut sitesine bütün verilerin aktarılması veya eski bulut sitesindeki verilerin tamamen temizlenmesi sorunları ortaya çıkmaktadır.

- Bir bulut sağlayıcısı iflas ederse, depolanan verilerin nereye gideceği veya verilerin sahibinin kimin olacağı konusunda da çeşitli problemler mevcuttur (Karthik ve Manhar, 2020).

- Bulut sunucu; fiziksel olarak hasar görebilmekte ya da kodlama anahtarının kaybı veya kötü niyetli kişilerden dolayı veri kaybı riski doğabilmektedir.

- Kötü niyetli bir müşteri, bulut sunucusuna diğer kullanıcıların verilerini tehlikeye atabilecek kimlik avı saldırısı (phishing) yaptığında, bulut sağlayıcı, şirketin gizlilik politikası nedeniyle bunu fark edemeyebilmektedir.

- Bulut hizmetlerinin uygulama arayüzünün güvenliğindeki bir boşluk, API veya baypas saldırısı gibi tehlikelere yol açabilmektedir.

- Bulut sağlayıcı çok sayıda kullanıcıya hizmet verdiği için şifreleme algoritmasındaki küçük bir zafiyet, kişilerin verilerine yetkisiz erişime sebep olabilmektedir (Malik ve Chaturvedi, 2013).

Cloudlet

Bir mobil cihaz, buluta veri veya kod yüklediğinde depolama/işleme için, gizlilik sorunlarına ve hesaplama bütünlüğü saldırılarına karşı savunmasız hale gelmektedir. Örneğin, birçok mimaride mobil cihazın bulutta bir görüntü klonu oluşturulmakta, yürütme ise daha sonra cihazda veya sanallaştırılmış bulut ortamında gerçekleşmektedir. Hesaplamanın bütünlüğü de bulutta benimsenen teknolojilerden doğrudan etkilenmektedir. Sanallaştırma, bulut bilgi işlem mimarilerinin geliştirilmesinde önemli bir oyuncu olmaktadır.

Bununla birlikte kullanıcılar, görüntülerini buluta sanal makine olarak yüklemekte ve kaynaklardan tasarruf etmek için birden çok sanal makine ile aynı sunucuyu paylaşabilmektedir. Bu durum, kullanıcı verilerinin gizliliği kapsamında bir güvenlik

uyumsuzluğuna neden olurken, bulutun fiziksel altyapılarında yürütülmekte olan verinin güvenliğini ve emniyetini sağlaması gerekmektedir. Bu bağlamda, rootkit saldırıları, sanal makine monitörünü hedefleyebilmekte ve ana bilgisayar işletim sisteminin yürütülmesini kontrol edebilmektedir. Ayrıca, belirli kötü amaçlı yazılım türlerinin sanal bir ortamda yürütüldüklerini algılayabildikleri ve davranışlarını buna göre değiştirebilecekleri de gösterilmiştir. Ayrıca, mobil bulut bilişim teknolojisinin hesaplamayı bulutlar arasında taşıma yeteneği, gerçekleştirilecek saldırılar için arka kapılar da açmaktadır (Gu ve Guirguis, 2014).

Ad-Hoc Mobil Bulut

Ad-Hoc mobil bulutta kod bölümlerini yürütmesini sağlayan kod dağıtım mekanizmalarına yönelik tehditler bulunmakta; birçok uygulama, kod bölümlerini yürütmek için yakındaki cihazların yardımına ihtiyaç duymaktadır. Bu durum, aşağıda yer alan çeşitli kısıtlamalar nedeniyle tüm uygulamanın tek bir cihazda yürütülmesinin mümkün olmadığı senaryolarda ortaya çıkmaktadır;

- Pil gücü kısıtlamaları, (tek bir cihazın tüm uygulamayı yürütmek için yeterli pil ömrü olmayabilmektedir.)

- Sınırlı altyapı erişimi, (tek bir cihazın altyapıya erişimi olmayabilmekte (örneğin kırsal bölgeler) veya hücresel veri miktarını aşmak gibi yüksek bir maliyet söz konusu olabilmektedir.)

- Farklı çalışma veri setlerinin kullanılmasıdır (yakındaki mobil cihazlar üzerlerinde depolanan yerel verilerle çalışabilmekte (örneğin, belirli bir zaman aralığında çekilen fotoğraflar) veya sensör bilgilerini toplayarak, etraflarındaki ortamdan veri alabilmektedir).

Kod bölümlerinin yürütülmesinde dağıtık yöntemlerin kullanılması nedeniyle, kötü amaçlı düğümlerin (malicious nodes) varlığı da dikkate alınmalıdır. Kötü amaçlı

düğümler, tersine mühendislik işlemiyle kodun işlevselliği ve kapasitesini ortaya çıkarabilmektedir. Eğer kötü amaçlı düğümler üzerinde çalıştıkları kodu ve verileri paylaşırsa kullanıcının gizliliği ihlal edilebilmektedir.

Yürütülen kod bölümlerin bütünlüğüne bakıldığında ise kullanıcılar yakındaki cihazlardan kendileri için kod bölümleri yürütmelerini istediğinde, diğer cihazların yanıt vermemesi veya yanlış sonuçlarla yanıt vermesi riskiyle karşı karşıya kalmaktadırlar. İstekte bulunan cihaz, fazladan bir katman eklemedikçe (bu aşamada birden fazla cihazdan aynı kod bölümlerini yürütmesi istenmekte ve sonuçlar karşılaştırılmaktadır) sonuçların doğruluğunu emin olunamamaktadır. Ancak bu durum, çok fazla ek yük getirerek, kod bölümlerinin yönetilme sürecinde çeşitli saldırılarla karşı karşıya bırakabilmektedir. Mobil düğümler arasındaki bağlantılara yapılan radyo yayını bozma (Jamming) saldırıları veya DoS saldırıları, kod dağıtım modüllerini etkileyebilmektedir. Özellikle mobil cihazlar kendilerine atanan kod bölümlerini alamamakta ve böylece istekte bulunan kullanıcıların sonuçları alması engellenerek, yürütülmemiş bölümlerin yeniden dağıtılması için yapılan ek çalışmalarda daha uzun gecikmelere sebep olunmaktadır (Gu ve Guirguis, 2014).

4.2 Mobil Bulut Bilişimde Gizlilik ve Veri Güvenliğinin Sağlanması

İnsanların mobil bulut kullanımıyla ilgili en önemli endişelerinden biri, mobil cihazdaki kişisel verilerinin bulutta depolanabilmesi veya bu verilere bulut tarafından erişilebilmesidir. Bir mobil cihaz, kişinin özel hayatı hakkında birçok şeyi ortaya çıkarabilen kişi listeleri, metin mesajları, kişisel fotoğraflar ve videolar, takvimler, konum bilgileri içermektedir. Son zamanlarda, dünya çapındaki veri ihlali vakaları nedeniyle artan bir güvenlik talebi bulunmaktadır. Mobil bulut bilişimin elverişli doğasına rağmen verilerinin gizliliği ve korunması da giderek artan bir şekilde temel veri sorunlarından biri olarak kabul edilmekte olup, kullanıcılar için bilgilerinin gizliliği ve güvenliği ile ilgili çeşitli zorluklar ortaya koymaktadır.

Mobil bulut bilişimde, mobil cihaz haricindeki sağlayıcılarda yer alan veriler ve uygulamalar da dâhil olmak üzere mobil kaynak korunmaktadır. Kullanıcı, kişisel

verilerini veya özel aile bilgilerini mobil cihazda saklayabilmektedir. Çoğu mobil cihazda, bulut altyapılarıyla paylaşılan tıbbi kayıtlar, banka bilgileri, konum ve diğer kişisel bilgiler gibi kullanıcıların gizli bilgileri saklanmaktadır. Özel bilgilerin bulut ortamında saklanması ve bunlara internet hizmetleri ve kablosuz şebekeler aracılığıyla erişilmesi, bu bilgileri çok sayıda siber saldırgana karşı savunmasız hale getirmektedir.

Gelişmiş WiFi, 5N şebekesi ve bulut teknolojisi sayesinde kişi istediği yerden kişisel verilerine her an ulaşabilmektedir. Bulut verilerine erişmek içinse kişiler genellikle akıllı telefon kullanmaktadır. Saldırganlar verileri gizlice dinlemek, çalmak veya değiştirmek için farklı bulut ve mobil altyapı seviyelerine girebileceğinden, mobil kullanıcılar yeni bir saldırı türü olan gelişmiş sürekli tehdidin (APT, Advanced Persistent Threat) kurbanı olabilmektedir.

Genel olarak araştırmacılar bu zorlukları, kişinin mahremiyeti, kişisel verilerin mahremiyeti, kişisel davranışın mahremiyeti ve kişisel iletişimin mahremiyeti şeklinde dört ana kategoride gruplanmıştır. Kullanıcılar, politika yapıcılar ve şirketler de dâhil olmak üzere birçok paydaşın kendileri için risk teşkil eden mahremiyet konularına yönelik veri ihlali, şantaj, sosyal mühendislik ve özel bilgilerin toplanması kişisel verilerin mahremiyeti kategorisine girmektedir (Alnajrani ve Norman, 2020).

Mobil bulut bilişim bileşenlerinin gizlilik ve güvenliğine yönelik tehditler karşısında alınabilecek önlemler şu şekildedir.

a) Mobil Cihaza Yönelik Önlemler

Mobil bulut bilişimin sacayaklarından biri olan mobil cihazlara yönelik özellikle depolama ve işletim sisteminin güvenliği, bulutta mobil bilgi işlem üzerinde doğrudan etkilere sahip olmakla birlikte, alınan önlemler kullanıcı güvenini temelini oluşturmaktadır.

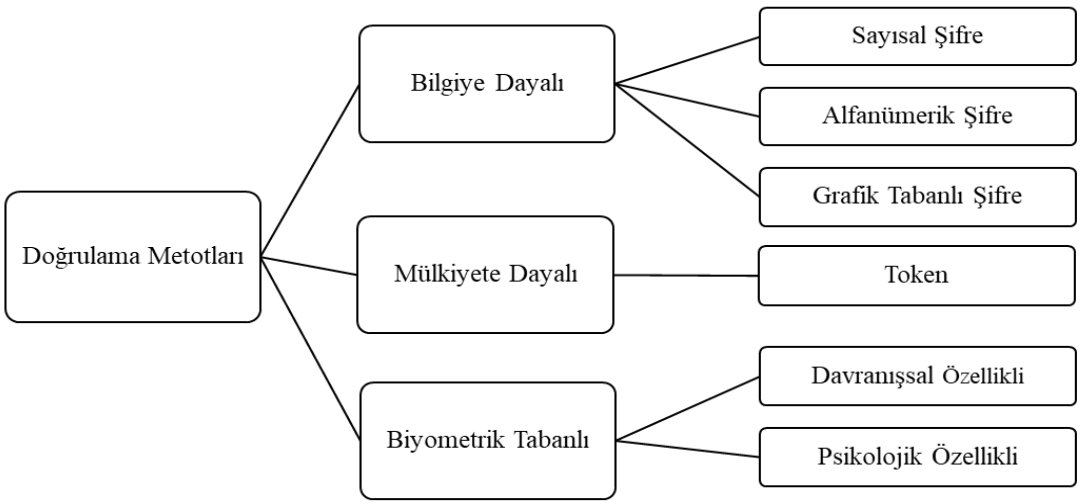
Mobil bulut bilişimde, güvenlik açısından kritik kod ve veriler bulutta da çalıştırılmaktadır. Mobil cihazlar kaybolabileceği veya çalınabileceğinden dolayı

saldırganlar, buluta girmeye gerek kalmadan mobil cihazdan mahrem verilere erişebilmektedir. Koruma önlemleri, verilerin veya belleğin şifrelenmesine dayanmaktadır (Gui ve Guirguis, 2014).

Mobil cihazın fiziksel tehditlere karşı korunması kapsamında geliştiriciler, hassas verilere yazılımları tarafından erişilebildiğinde, uygulama düzeyinde fazladan bir güvenlik katmanı ekleyebilmektedir. Bununla birlikte, ses tanıma ve parmak izi gibi daha gelişmiş tanımlama teknikleri, mobil cihazları korumak için ikinci bir kimlik doğrulama yöntemi olarak kullanılabilmektedir. Bu bağlamda, çok faktörlü kimlik doğrulama yöntemleri önerilmiştir.

Çok faktörlü kimlik doğrulamada, kullanıcının gizli bilgilerini korumak için veriler, kimliği doğrulanmış kişiler tarafından erişilebilir olmalıdır. Bu minvalde, çeşitli kimlik doğrulama yöntemleri önerilmiştir. Kullanıcı kimlik doğrulaması yöntemleri bilgiye dayalı, mülkiyete dayalı ve biyometrik tabanlı kimlik doğrulama olmak üzere üç farklı kategoride sınıflandırılmaktadır. Her kategorinin farklı özellikleri ve uygulama yöntemleri olmakla beraber, bu sınıflandırma Şekil 4.1'de verilmiştir (Alizadeh ve diğerleri, 2014).

Şekil 4.1 Doğrulama Faktörleri



Kaynak: Alizadeh ve diğerleri, 2014

Çok faktörlü kimlik doğrulamada, güvenliği artırmak ve verileri kullanmak için istekte bulunan kişinin, doğrulanmış kullanıcı olduğunu anlayabilmek amacıyla birden fazla kimlik doğrulama faktörü kullanılmaktadır. Örneğin, kimlik ve şifre birinci faktör olarak kullanılırken, biyometrik özellikleri ikinci bir doğrulama faktörü olarak ele alınabilmektedir. Bu durumda, saldırgan kullanıcının kimliği ve şifresini bulursa, biyometrik özellikleri geçerli olmadığı için sisteme erişememektedir (Alizadeh ve diğerleri, 2014).

Ayrıca birden fazla kimlik doğrulama yöntemi işlenmesi sebebiyle çok faktörlü kimlik doğrulama yöntemlerini uygulamak için yeterli hesaplama kaynağına ihtiyaç duyulmaktadır. Mobil cihazın doğası gereği barındırdığı kaynak sınırlaması sorunu bulut bilişim kullanılarak çözülebilmektedir. Mobil bulut bilişimde, mobil cihazlar bulut bilişim altyapısına bağlanmakta ve kimlik doğrulama yöntemlerini işlemektedir. İşlem adımları, mobil cihaz işlem gücü kullanılmadan bulutta gerçekleştirilmektedir. Bununla birlikte, kimlik doğrulama yöntemi, hesaplamalı işleme bulut tarafında yapılacak şekilde tasarlanmalıdır. Aynı zamanda çok faktörlü kimlik doğrulama yöntemlerinin enerji tüketimi de bilgi işlem süreçlerini buluta aktarılmasından dolayı azaltılabilmektedir (Alizadeh ve diğerleri, 2014).

Sonuç olarak, çok faktörlü kimlik doğrulama yöntemleri, güvenliğin önemli olduğu mobil bulut bilişim ortamı için oldukça uygun olup, söz konusu yöntemlere ilişkin detaylara aşağıda yer verilmektedir.

Bilgiye Dayalı Kimlik Doğrulama: İlk kimlik doğrulama yöntemlerinden biri olan bilgiye dayalı kimlik doğrulama, geleneksel kullanıcı adı ve parola yöntemine dayanmaktadır. Kullanıcı kimlik doğrulaması için kullanıcı adı ve şifre kullanmak, farklı kimlik doğrulama yöntemleri arasında en yaygın kullanılan yöntem olmakla birlikte, kullanıcının güvenliğini tehdit eden bazı güvenlik açıkları bulundurmaktadır. İlk sorun, kullanıcılar için şifreleri ezberlemenin zorluğudur. Bu sorun, kullanıcıların çok basit şifreler kullanmasına neden olmakta ve şifre saldırganlar tarafından kolayca kırılabilmektedir. Diğer bir sorun ise oltalama saldırılarıdır. Bu saldırı türünde, bir

saldırgan, gerçek web sitesi yerine sahte bir web sitesi oluşturmak gibi farklı yöntemler kullanarak kullanıcının parolasını bulabilmekte ve parolayı ele geçirebilmektedir. (Alizadeh ve diğerleri, 2014).

Mülkiyete Dayalı Kimlik Doğrulama: Bu doğrulama türünde, bir kullanıcının sisteme kimlik doğrulamasını kanıtlamak amacıyla token adındaki bir yazılım veya donanım aygıtı kullanılmaktadır. Bu aygıt tek kullanımlık parola ile oturum açmada veya USB token, akıllı kartlar ve açık anahtar altyapısında kullanılabilmektedir. Sahiplik tabanlı kimlik doğrulamada en önemli konu, bu kimlik doğrulama yönteminin uygulanmasının zorluğu ve maliyetidir. Bu tür bir kimlik doğrulamayı uygulamak için yeterli bilgi işlem kaynağı gerekmekte ve bir kimlik doğrulama algoritmasını yürütmek çok fazla enerji tükettiğinden, bu yöntemi mobil cihazlarda kullanmak bazı zorluklar getirmektedir (Alizadeh ve diğerleri, 2014).

Biyometrik Tabanlı Kimlik Doğrulama: Biyometrik tabanlı kimlik doğrulama yönteminde, kullanıcının sahip olduğu özelliklerden biri ele alınmaktadır. Kullanıcının kimliğini doğrulamak için kullanılan bazı biyometrik özellikler arasında parmak izi, iris, ses ve yüz tanıma bulunmaktadır. Bu kimlik doğrulama, kabul edilebilir düzeyde bir güvenlik sağlamakta ancak biyometrik özellikler kullanılması bazı gizlilik sorunları da ortaya çıkarmaktadır. Örneğin, biyometrik verilerin nasıl depolanacağı ve korunacağı önemli bir mahremiyet sorunudur. Çünkü saldırgan kullanıcının biyometrik bilgilerini alırsa, kişinin biyometrik özellikleri değiştirilemeyeceği için saldırgan bu biyometrik özellikleri her zaman kullanabilmektedir. Bu doğrulamayla ilgili başka bir sorun da uygulama maliyetidir. Tüm mobil cihazlarda biyometrik özellikleri tanıyacak bu tür özellikler bulunmamaktadır. Bu tür bir kimlik doğrulamayı uygulamak için yeterli bilgi işlem kaynağı gerekmekte ve bir kimlik doğrulama algoritmasını yürütmek çok fazla enerji tükettiğinden, bu yöntemi mobil cihazlarda kullanmak bazı zorluklar getirmektedir (Alizadeh ve diğerleri, 2014).

Literatürde, kötü amaçlı yazılımlara yönelik alınacak önlemlerde ise ilk olarak, yetkili yazılımın önceden kurulup, buluttan dağıtılmasını önermiştir. Bu öneride kötü amaçlı yazılım algılandığında, akıllı telefon yazılımı buluttaki güvenilir sistem yedeklerini

geri yükleyecektir. Ayrıca bu tür tehditlere ilişkin kullanıcıları gerekli eğitimler ile bilinçlendirmek de önemli bir savunma faktörü olarak yer almaktadır. Kullanıcılar tehditler konusunda eğitmeli ve mobil şebekeleri veya uygulamalarını kullanırken nelere dikkat etmeleri gerektiği açıklanmalıdır. İkinci olarak ise şebeke altyapısı geliştirilmeye devam edilerek, yetkisiz sitelere mobil erişim kısıtlanmalı ve filtrelenmelidir. Böylece kullanıcının mobil şebekeleri ve cihazları kötü amaçlı veya casus yazılımlardan korunarak, diğer güvenlik yazılımlarının kullanılmasıyla güçlendirilecektir (Chang ve diğerleri, 2013).

Bununla birlikte, mobil uygulamalar, bilgi güvenliği ve görev ayrılığı ilkelerine dayalı olarak güvenlik kontrolü ile tasarlanmalı; her uygulama, yalnızca bir işi tamamlamak için gereken ayrıcalıklarla çalışmalıdır. Birçok uygulama, kurulum sırasında gerekenden daha fazla ayrıcalık talep etse de kullanıcılar uygulamaların kullanmalarını istemedikleri ayrıcalıkları devre dışı bırakmalıdır. İstenmeyen ayrıcalıkları devre dışı bırakmak veya çalışma esnasında gerekli izinlerin atanması güvenlik önlemleri kategorisinde yer almaktadır (Gui ve Guirguis, 2014).

Mobil uygulamalar kullanılırken kişisel verilerin korunmasına yönelik şu hususlara dikkat edilmesi gerekmektedir (KVKK, 2023c);

- Uygulamanın güvenilir bir kaynaktan geldiğinden emin olunmalı ve uygulama, güvenilir olduğu değerlendirilen platformlar (örneğin, uygulama mağazaları) üzerinden cihaza indirilmelidir.
- Bir uygulama yüklenmeden önce uygulamanın geliştiricisi hakkında bilgi edinilmeli ve uygulama adının doğruluğundan emin olunmalıdır. Ayrıca uygulamaya yönelik kullanıcı yorumları ve uygulamanın kullanıcılardan aldığı puan da göz önünde bulundurulmalıdır.
- Uygulama yüklenmeden önce hangi verilere erişim izni istendiği kontrol edilmeli ve uygulamanın gizlilik politikası gözden geçirilmelidir. Uygulamanın sunduğu hizmet ile herhangi bir ilişkisi bulunmayan kişisel veri taleplerine karşı dikkatli olunmalıdır.

- Uygulamalara giriş yapmak için sosyal medya hesaplarının kullanılmasından kaçınılmalıdır. Zira bir uygulamada kullanıcının sosyal ağ hesabına ilişkin bilgiler ile oturum açılması, kimi durumlarda uygulamanın ilgili sosyal ağ hesabından bilgi toplamasına olanak tanıyabilmekte ve hesapları tehditlere karşı daha savunmasız hâle getirebilmektedir.
- Uygulamalara giriş yapmak için kullanılacak parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay şekilde tahmin edilebilecek şifreler yerine büyük-küçük harf, rakam ve sembolleri içerecek şekilde güçlü kombinasyonlar tercih edilmelidir.
- Geliştiriciler, mobil uygulamanın sunulması ve ilgili kişiler tarafından kullanılması süreçlerinde farklı paydaşların veri sorumlusu veya veri işleyen olma statülerini kişisel veri işleme faaliyetine başlamadan önce belirlemelidir. Bu kapsamda, her bir paydaşın veri koruma mevzuatı bağlamındaki sorumluluğu ve paydaşlar arasındaki hukuki ilişki netleştirilerek Kanun ve ikincil mevzuata uyumu sağlanmalıdır.
- Mobil uygulamalara yönelik düzenli olarak yama yönetimi ve yazılım güncellemesi süreçleri gerçekleştirilmelidir. Uygulamalardaki açıkların ve zafiyetlerin kapatılması adına yazılımların güncel tutulması, uygulama güvenliğinin sağlanmasına yardımcı olacaktır.
- Mobil uygulamalarda kişisel verilerin depolanması ve aktarımı sırasında veri güvenliğinin sağlanması kapsamında, ağ iletişiminde uygun şekilde yapılandırılmış yeterli bir şifreleme katmanı ve ilgili şifreleme anahtarlarının güvenli yönetimi aracılığıyla koruma için şifreleme kullanılmalıdır.
- Mobil uygulamalar aracılığıyla işlenen kişisel veriler açısından açıkça tanımlanmış iş ihtiyaçlarına veya yasal yükümlülüklere göre gerekçelendirilmiş saklama ve imha süreleri belirlenmeli ve bu veriler gerekli olan süreden daha uzun süre saklanmamalıdır. Bu çerçevede, bir mobil uygulama geliştiricisinin bulutta depoladığı kişisel veriler açısından saklama süresi, mobil uygulamanın kullanıldığı sektöre özel mevzuatta öngörülen azami bir saklama süresi varsa bu süre göz önünde bulundurularak

belirlenmeli; eğer bu şekilde bir azami saklama süresi bulunmuyorsa bu verilerin işlendikleri amaçla bağlantılı bir saklama süresi belirtilmelidir.

b) Bulut Bilişime Yönelik Güvenlik Önlemleri

Bulut bilişim teknolojisi, bulutun farklı bileşenlerinin hedef alındığı birçok saldırı çeşidine maruz kalabilmektedir. Bu kapsamda, mobil bulut bilişimin güvenliği ile yakından ilgili olan bulut teknolojisi ve bulutta mobil bilgi işlem için güvenlik önlemleri ele alınmaktadır.

Geleneksel bulut, istemci-sunucu modeli üzerine kurulu olması sebebiyle, güvenlik önlemleri genellikle bulut tarafına odaklanmaktadır. Özellikle, bulut sunucularında bilgi işlemin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için savunma mekanizmaları ile bulut sunucusundaki sistem bileşenleri, konuk sistemleri, sanal makine yöneticisini (hipervizör) ve ana bilgisayar sistemini içermektedir. Buna göre güvenlik önlemleri; konuk sistemdeki hesaplamanın güvenliği, hipervizörün konuk sistemi nasıl yönettiği ve bulutun güvenliğini etkileyebilecek kullanıcı kontrollü işlemler şeklinde üç kategoriye ayrılmaktadır.

Konuk Sistemler

Giderek daha fazla hizmet buluta aktarıldıkça, kullanıcının kişisel bilgileri de buluta aktarılmaktadır. Kullanıcılar uygulamalarının kişisel bilgileriyle birlikte konuk sistemler üzerinden yürütmesi sebebiyle bulut içindeki hesaplamanın gizliliği ve bütünlüğü de ele alınması gereken endişelerdendir.

Genel yaklaşım, yalnızca yetkili varlıkların ve süreçlerin veriler ile uygulamalara ulaşabilmesi için güvenlik ilkeleri uygulanarak, erişim denetimi yapılmasıdır. Ancak veriler ile uygulamalar açık bir şekilde saklanırsa, bulutun yöneticileri bunlara erişebilmekte ve hatta güvenlik politikalarını değiştirebilmektedir. Bu nedenle, verilerin ve uygulamaların bulutta şifrelenmesi için kriptografik çözümler

önerilmektedir. Kriptografik çözümlerde veriler yalnızca depolamada değil, aynı zamanda hesaplamada da şifrelenmektedir.

Araştırmacılar, istenen hesaplama güvenliğinin istemci tarafında elde edilmesi için bazı köklü kriptografik çözümler kullanmayı da önermiştir. Bu çözümlerde kişisel veriler, yalnızca gizlenmekle kalmayıp daha sonra da buluttaki verileri doğrulaması için de kullanılabilen kriptografik taahhütler olarak şifrelenmekte ve hesaplama bulutta değil, istemcide gerçekleştirilmektedir. Bulut, kullanıcının verileri işlemesi gerektiğinde, taahhütleri kullanıcıya göndermekte ve kullanıcıdan bazı hesaplamalar yapmasını istemektedir. Ardından, kullanıcı sonuçları etkileşimli olmayan sıfır bilgi kanıtlarıyla birlikte geri göndermektedir. Bulut ise hesaplamanın bütünlüğünü doğrulamak için taahhütler ve sıfır bilgi kanıtlarıyla sonuçları doğrulamaktadır (Gui ve Guirguis, 2014).

Sanal Makine Monitörü

Bir bulut sunucusunda birden çok konuk sistemini yöneten ‘sanal makine mönitörü güvenliğinin’ iki farklı yönü bulunmaktadır. Bunlardan ilki, birden çok konuk sistemi arasındaki güvenliğin sağlanmasıdır. Böylece bir konuk sisteminin güvenliği ihlal edilirken, diğer konuk sistemleri tehlikeye atılmamaktadır. Diğer bir değerlendirme ise konuk sistemlerinin güvenliğinin sağlanarak, konuk sistemin beklenildiği gibi kendi hesaplamasını yapabilmesidir.

İlk güvenlik hedefinin sağlanması için sanal makine monitörünün farklı konuk sistemlerinin hesaplama kaynakları arasına sınırlar koyduğu izolasyon mekanizması önerilmektedir. Bu sınır fiziksel olarak, her konuk sisteminin farklı konumlarda ve farklı makinelerde barındırılmasıyla konulabilmektedir. Uygulamada ise izolasyon sanallaştırılarak; bulut bilişim sağlayıcılarının, talep edilen hesaplama kaynaklarını konuk sistemlere esnek bir şekilde tahsis edebilmesi sağlanmaktadır. Ancak sanallaştırılmış izolasyonda, bir konuk sistemi başka bir konuk sisteme müdahale edebilmektedir. İzolasyon olsa da aynı bilgisayardaki birden çok konuk sistemi, CPU çekirdekleri, önbellekler, bellek ve giriş/çıkış kanalları gibi hesaplama kaynaklarını

paylaşmaya devam etmektedir. Bu kaynaklar arasında önbelleğin, CPU çekirdeğinin içinde olması ve genellikle doğrudan QoS provizyonlu sanal makine mönitörü tarafından kontrol edilememesi sebebiyle izole edilmesi en karmaşık faktör olarak yer almaktadır (Gui ve Guirguis, 2014).

Bu doğrultuda sunulan önbelleğe duyarlı bir izolasyon çözümünde, aynı son düzey önbelleği paylaşan çekirdekler, ortak bir çekirdek grubuna yerleştirilmiş ve ardından her çekirdek grubu en fazla bir konuk sisteme atanmıştır. Böylece bir konuk sisteminin, diğer konuk sistemleriyle önbellek için rekabet etmemesi sağlanmıştır. Ancak bu çözüm, hesaplama kaynağının ayrıntı düzeyinin çekirdek grup düzeyinde olması şeklinde bir dezavantaj barındırmaktadır. Ayrıca çekirdek grubun kaynağı bir konuk sistemde yeterince kullanılamıyorsa, bu kaynak diğer konuk sistemlere de atanamamaktadır (Gui ve Guirguis, 2014).

İkinci güvenlik hedefinde ise çalışan konuk sistemlerinin bütünlük kontrollerinin yapılması gerekmektedir. Konuk sistemlerdeki uygulamalar internete erişebilmekte ve dolayısıyla bilgisayar sistemlerinde olduğu gibi çeşitli saldırılara maruz kalabilmektedir. Bu yüzden çalışma esnasında konuk sistemlerin güvenliğinin ihlal edilmediğinden emin olmak önemlidir.

Bulut, sanallaştırma teknolojileri kullanılarak oluşturulmakta ve bütünlük denetimi sanal makine monitörünün bir parçası olarak uygulanabilmektedir. Bu doğrultuda çeşitli bütünlük kontrolü çözümleri önerilmektedir. İlk olarak, sanal makine iç gözlemcisi adlı, sanal makine monitörünün izinsiz giriş eylemlerini algılaması için konuk sistemlerdeki işlemcilerin, belleklerin ve disklerin durumunu izleyen bir izinsiz giriş algılama modülü kullanılmaktadır. İkinci çözüm önerisi ise konuk sistem kodunun yürütülmesinin denetlenmesidir. Bu çözümde, kod çalıştırılmadan önce korumalı bir hafızada saklanarak, bu hafızadan alınmakta veya önceden kodun kontrol akışı doğrulanmaktadır. Belirtilen önerilerde çalışan konuk sisteminin davranışlarının öngörülere uyup uymadığının karşılaştırabilmesi için sanal makine monitöründe, bu davranışların depolanmasına ihtiyaç duyulmaktadır (Gui ve Guirguis, 2014.)

Kullanıcı Kontrollü Güvenlik Önlemleri

Bulut bilgi işlemde mobil kullanıcılar, sanal makine görüntüsünün yayımlanması ve son kullanıcı yapılandırması şeklinde iki tür işlemle yer almaktadır. Kullanıcılar sanal makine görüntülerinin oluşturulması, yüklemesi ve alınması gibi yayımlama işlemlerinde kişisel bilgilerini ifşa edebilmektedir. Bu bağlamda 'Mirage' adı verilen ve dört bileşenden oluşan sanal makine görüntü yönetim sistemi önerilmektedir. İlk bileşen, görüntü sahibinin isteğine bağlı olarak sanal makine görüntülerinin paylaşımını düzenleyen bir erişim kontrol çerçevesidir. İkinci bileşen, görüntüleri paylaşırken hassas bilgileri kaldırmak veya gizlemek için uygulanan görüntü filtrelerinden oluşmaktadır. Üçüncü bileşen, bir kullanıcı görüntüyü revize ettiğinde ve yeni bir tane oluşturduğunda görüntünün türetme geçmişini izleyen bir kaynak izleme mekanizmasıdır. Son bileşen ise görüntülerdeki güvenlik açıklarını algılayan ve düzelten bir dizi havuz bakım hizmetidir. Bulutta, kullanıcıların makineleri gruplamasına ve gruplar arasındaki iletişimi kontrol etmek için kurallar koymasına izin verilmektedir. Bu sayede kullanıcılar, farklı güvenlik seviyelerine sahip gruplar kurabilmekte ve bulutta özelleştirilmiş hizmetler sunabilmektedir. Fakat bu tür bir son kullanıcı yapılandırması, bulut altyapısının ve hizmetlerinin karmaşıklığı göz önüne alındığında, kullanıcı bilgilerini riske atabilmektedir. Dolayısıyla, kullanıcı bilgilerini korumak için son kullanıcı yapılandırması güvenliğinin de değerlendirilmesi gerekmektedir. Bu kapsamda, çok katmanlı bulut altyapısında son kullanıcı yapılandırmasının denetlenmesi için bir yaklaşım önerilmiştir. Yaklaşımda, güvenlik ilkesi kuralları, tepe noktasının bilgi havuzunu, kenarların ise bilgi akışını temsil ettiği bir bilgi akış grafiği olarak modellenmiştir. Bununla birlikte bilgi akış grafiği kullanılarak güvenlik politikası kurallarına göre erişilebilirlik analizi yapılmaktadır. Ayrıca grafikte, bir bilgi akış yolu bulunduğunda ise ilke kuralları tarafından belirtilmediği sürece ihlal olarak algılanmaktadır (Gui ve Guirguis, 2014).

Geleneksel bulut bilişimdeki güvenlik önlemleri, bulut sunucularının tasarımı ve yönetimi istemci türlerinden etkilenmemesi sebebiyle mobil bulut bilişime yönelik güvenlik gereksinimlerinin önemli bir bölümünü karşılamak üzere uygulanabilmektedir. Bununla birlikte literatürde, mobil bulut bilişimin güvenli kod

bölümleme ve boşaltma, mobil kullanıcı kimlik doğrulaması ile güvenli mobil veri yönetimi özelliklerine yönelik güvenlik önlemleri de yer almaktadır. Bu üç özelliğin güvenliğinin sağlanması ile yalnızca bulutta mobil bilgi işlemin bütünlüğü ve gizliliği sağlanmış olunmamakta, aynı zamanda mobil cihazlarda bulunan özelliklerden de yararlanılmaktadır (Gui ve Guirguis, 2014).

Güvenli Kod Bölme ve Boşaltma

Kod bölümleme ve boşaltma, mobil bulut bilgi işlem mimarisinin tümünde ortak işlevler olarak yer almaktadır. Bu yüzden mobil bulut bilgi işlemde uygulamaların güvenliğinin sağlanmasında kod bölme ve boşaltmanın güvence altına alınması vazgeçilemez bir unsur olarak yer almaktadır.

Güvenli kod bölme ve boşaltmanın sağlanması için güvenli kurulum, modül kimlik doğrulaması, güvenli geçiş ve izin yetkilendirmesi şeklinde dört bileşenden oluşan bir çerçeve önerilmiştir. Çözüm önerisi internet tabanlı elastik uygulamalar için tasarlanmış olsa da güvenlik bileşenlerinin temel fikirlerinin diğer modüler uygulamalara uygulanabileceği değerlendirilmiştir (Gui ve Guirguis, 2014).

- Güvenli kurulum bileşeni mobil cihazlara orijinal uygulamaların yüklenmesini ve uygulamaların imzalı karma işlevlere (hash) sahip olmasını sağlamaktadır. Kurulum sırasında, uygulamaların bütünlüğünün sağlandığı kontrol edilmelidir.

- Modül kimlik doğrulama ile uygulamanın bir modülü, aynı uygulamaya ait başka bir modülün kimlik doğrulamasını sağlamaktadır. Aynı uygulamanın modülleri farklı konumlara taşınabileceğinden veya farklı konumlarda yürütülebileceğinden, aynı uygulamanın modüllerinin yürütme konumlarından bağımsız olarak çalıştırılması için bağımlı modüllerin yürütme sırasına göre doğrulanması gerekmektedir. Modüller çalıştırıldıktan sonra, elastik uygulamaların yöneticisi

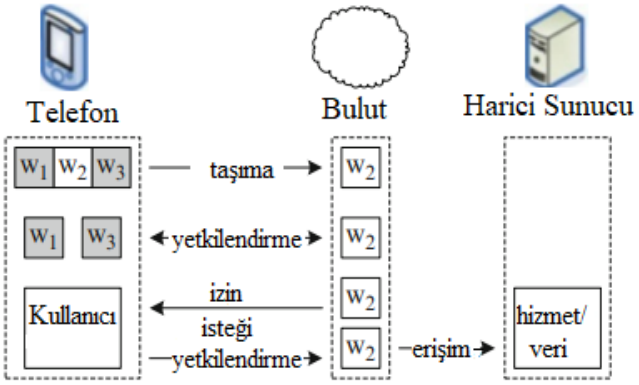
her modülle ilişkili bir çift oturum anahtarı[1] (session key) ve oturum sırrı (session secret) oluşturmaktadır. Oturum anahtarı ve sırrı çifti daha sonra kimlik doğrulama ile modüller arasında güvenli iletişim için kullanılmaktadır.

- Güvenli geçiş bileşeni, geçiş güvenliğinin sağlanması ve bir modülün taşınması gerektiğinde, modül durumunu kaydederek taşıma durumuna getirmektedir. Geçiş sırasında, modülle ilişkili anahtar ve sır çifti, kimlik doğrulaması için modülle birlikte hedefe teslim edilmektedir. Doğrulama yapıldıktan sonra ise taşınan modül, kaydedilen durumdan çalışmaya devam etmektedir.

- İzin yetkilendirme bileşeni ile uygulamanın modüllerine farklı izinler atanmaktadır. Aynı uygulama içindeki modüllerin, işlevlerinin ve konumlarının farklı olmasından dolayı, görevlerine göre farklı izinlerle yetkilendirilmeleri gerekmektedir. Önerilen bir yaklaşımda, buluttaki modüller hassas verilere erişmek istediğinde, bu isteğin karşılanması için mobil cihaza kimlik bilgisi talebi iletilerek, ardından bu kimlik bilgilerinin doğrulama ve yetkilendirme almak için kullanması gerekmektedir. Başka bir değerlendirmede ise buluttaki modüllerin hassas verilere erişmek için bir kimlik doğrulama talebi başlatmakta ve mobil cihazdan kimlik doğrulama süreci tamamlandıktan sonra kimliği doğrulanmış oturumu buluttaki modüllere iletmektedir.

[1] Oturum anahtarı, tüm mesajları tek bir iletişim oturumunda şifrelemek için kullanılan tek kullanımlık simetrik bir anahtar olarak tanımlanmaktadır.

Şekil 4.2 Esnek Uygulamanın Güvenli Şekilde Yürütülmesi



Kaynak: Gui ve Guirguis, 2014

Dört bileşenli bir elastik uygulama yürütme yaklaşımı Şekil 4.2'de gösterilmektedir. Söz konusu şekilde uygulama, w1, w2 ve w3 olmak üzere üç weblet'e sahip olup, w2 geçiş bileşeni tarafından yürütülmek üzere buluta geçirilmektedir. Yürütme sırasında, w2'nin kimlik doğrulaması w1 ve w3 kimlik doğrulama bileşeni kullanılarak yapılmaktadır. w2 harici sunucuya erişmek istediği zaman yetkilendirme bileşeni aracılığı ile yetki istemektedir. Bununla birlikte kullanıcı da cihazın kullanıcı arabirimi aracılığıyla erişim izni verebilmekte ve w2 sunucuya erişmektedir.

Önerilen bu çerçeve ile bir uygulamanın boşaltılmış modüllerinin yönetimine, taşınmasına ve yürütülmesine vurgu yapılmaktadır. Ana güvenlik hedefi olarak ise modüller farklı konumlarda çalıştırıldığında elastik uygulamanın bütünlüğünün sağlanması verilmektedir. Ancak bu yaklaşım kod bölümlerinin kendi güvenliğini sağlaması konusunda oldukça zayıf kalmaktadır (Gui ve Guirguis, 2014).

Özetle, mobil bulut bilişimde, mobil cihazlar tarafından toplanan bilgiler bulut hizmetlerinin bir parçası olarak işlenmekte, depolanmakta ve kullanıcılara sunulmaktadır. Mobil cihaz görüntüleri, cihazların işlevlerini artırmak için bulutta da saklanabilmektedir. Bu bilgilerin gizliliği ve mahremiyeti oldukça dikkat çeken bir husus olmakla birlikte, mobil bulut bilişimde güvenli veri işlemeyi içeren çeşitli yaklaşım bu endişeyi gidermek için önerilmiştir.

Kişisel verilerin bulutta depolanması, hukuka aykırı işlemenin ve erişimin önlenmesi ile hukuka uygun muhafaza yükümlülüğü olan veri sorumlusunun kendi bilgi teknolojileri sistemi ağından ayrılmasına ve kişisel verilerin bulut depolama hizmeti sağlayıcıları tarafından işlenmesine neden olmaktadır. Bu durum birtakım riskleri de beraberinde getirmekte ve bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin yeterli ve uygun olup olmadığının değerlendirilmesi gerekmektedir.

Bu kapsamda, bulutta yer alan kişisel verilerin güvenliğine yönelik ne tür bilgilerin depolandığının detaylıca bilinmesi, verilerin yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması önerilmektedir.

Ayrıca, söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması, kişisel veriler için mümkünse özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Öte yandan, bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmeye yarayabilecek şifreleme anahtarlarının tüm kopyalarının da yok edilmesi gerekmektedir (KVKK, 2018a).

4.2.1 Bulut Standartları

Bulut kullanıcılarının, hizmet sağlayıcılarının uyguladığı teknik ve idari önlemleri doğru bir şekilde değerlendirmeleri genellikle zor ve zaman alıcı bir süreçtir. Bu nedenle bulut hizmet sağlayıcıları tarafından elde edilen sertifikalar, kullanıcıları için büyük önem taşımaktadır. Bulut bilişime yönelik birçok uluslararası standart bulunmakta ve bu standartlar sayesinde bulut kullanıcıları, bulut hizmet sağlayıcıların hizmetleri hakkında bilgi sahibi olabilmektedir. Bulut hizmet sağlayıcıları, genellikle standartlara uyum sürecinde gerekli teknik ve idari tedbirleri alarak bu gereksinimlere uygun hizmet sunmaktadır (Maya, 2023).

A. BSI C5 Standartı

C5 Standardı (Cloud Computing Complianca Criteria Catalogue) güvenli bir bulut bilişim sistemi için bulut hizmet sağlayıcıları, denetçileri ve kullanıcıları için hazırlanmıştır. Bu bağlamda, söz konusu standart bir bulut bilişim sisteminin sahip olması gereken asgari özellikleri belirlemektedir. C5 standardı 2016 yılında Federal Bilgi Güvenliği Ofisi (Bundesamt für Sicherheit in der Informationstechnik - BSI) tarafından yayımlanan, Almanya'daki bulut bilişim standardıdır. C5 standardı hâlihazırda ISO 27001, CSA Bulut Kontrol Matrisi, Güvenilir Bulut Standardını da kapsamaktadır.

C5 Standardı kullanıcıların, bulut hizmet sağlayıcı seçmesi ve risk yönetimi yapabilmesi kapsamında bir kılavuz niteliği taşırken, 2020 yılında tamamen revize edilerek yeni bir sürümü yayımlanmıştır (Amazon, 2023d).

B. Cloud Security Alliance

ABD merkezli bir kuruluş olan Cloud Security Alliance (CSA), özellikle bulut bilişim güvenliği alanında faaliyet göstermektedir. Bulut bilişim kullanımının artmasıyla birlikte, güvenliğin sağlanması için gereken standartları ve en iyi uygulamaları belirlemesi amaçlanmaktadır.

CSA, bulut hizmetlerini değerlendirmek için kullanılan kriterleri belirlemek amacıyla CSA Güvenlik Kılavuzu'nu da kapsayan CSA Bulut Kontrol Matrisi gibi önemli kaynakları yayımlamıştır. Bu kaynaklar, bulut bilişim sistemlerinin güvenliği konusunda endüstri standardını oluşturmak ve organizasyonlara rehberlik etmek amacıyla geliştirilmiştir (Maya, 2023).

CSA, bulut bilişimle ilgili riskleri anlama, yönetme ve azaltma konusunda endüstriye önemli bir katkı sağlamakta ve rehberler ile standartlar geliştirmeye devam etmektedir. Bu kapsamda, bulut hizmet sağlayıcılarına sertifikalar da verilmektedir. Bu sertifikalara örnek olarak CSA STAR (Security, Trust, and Assurance Registry) ve

CSA CCM (Cloud Controls Matrix) gösterilmektedir. CSA STAR sertifikasyonu için hizmet sağlayıcıları, bulut bilişim hizmetlerine ilişkin belirlenen gereksinimleri karşılayarak, güvenlik kontrollerine uyması gerekmektedir (CSA, 2023a). CSA CCM ise hizmet sağlayıcılarının güvenlik ve uyumluluk seviyelerini ölçmek için anket formunda hazırlanmıştır (CSA, 2023b).

C. EuroCloud Star Sertifikası

EuroCloud Star Sertifikası, Avrupa'daki bulut hizmet sağlayıcılarının güvenlik, uyumluluk ve sürdürülebilirlik düzeylerini değerlendirmek amacıyla geliştirilmiş bir sertifika programıdır. Cloud Security Alliance (CSA) STAR programına dayanarak hazırlana sertifika, Avrupa'nın mevzuat, düzenleme ve standartları göz önünde bulundurarak özelleştirilmiştir (EuroCloud, 2023).

EuroCloud Star, ilgili hizmet sağlayıcıların güvenlik seviyelerini göstererek, bağımsız bir denetçinin gerçekleştirdiği değerlendirmelere dayanmaktadır. Sertifikasyon süreci, bulut hizmet sağlayıcıların güvenlik kontrollerine uyum sağlamalarını, müşterilerin verilerini güvenli bir şekilde saklamalarını ve işlemelerini temin etmektedir. Sertifikanın değerlendirilmesi kapsamında, kalite seviyeleri derecelendirilmekte ve en yüksek düzey olarak beş yıldıza dayandırılmaktadır (CBDDO, 2020).

D. ISO 27001 ve ISO 9001 Standardı

Uluslararası Standardizasyon Kurumu (ISO, International Organization for Standardization), uluslararası standart geliştiren ve yayımlayan Türkiye'nin de aralarında bulunduğu 167 ülkeden üyesi bulunan kâr amacı gütmeyen bir organizasyondur.

ISO 27001, bilgi güvenliği yönetim sistemlerine yönelik uluslararası bir standarttır. Bu standart, bir kuruluşun bilgi varlıklarının korunmasına ilişkin süreçlerin yönetilmesi ve kontrol edilmesi için bir çerçeve oluşturmaktadır. Ayrıca ISO 27001, kuruluşun risk analizi yapmasını, güvenlik politikaları oluşturmasını, bilgi güvenliği

farkındalığına yönelik eğitimi vermesini ve düzenli denetimler yapmasını da gerektirmektedir. Bu kapsamda, bulut hizmet sağlayıcısı da ilgili riskleri ve tehditleri belirleyerek, güvenlik kontrollerini ve denetimlerini uygulamalıdır.

ISO 9001, uluslararası bir kalite yönetim sistemi standartıdır. Bu standart, kuruluşun müşterilerinin ihtiyaçlarını karşılanması ve sürekli olarak iyileştirilmesi için kalite yönetim sistemi kurulmasını ve uygulamasını sağlamaktadır. Burada, temel amaç, kuruluşun müşteri memnuniyetini artırmak, maliyetleri azaltmak, süreçleri optimize etmek ve rekabet avantajı elde etmek için kalite yönetim sistemini standartlaştırmaktır. ISO 9001 standart uyumluluğu, kuruluşların iş süreçlerini etkili bir şekilde yönetmelerine ve sürekli gelişmeye odaklanmalarına yardımcı olmaktadır (Maya, 2023).

E. Güvenilir Bulut (Trusted Cloud) Sertifikası

Almanya'nın Federal Ekonomi ve Teknoloji Bakanlığı tarafından başlatılan, Güvenilir Bulut (Trusted Cloud) Sertifikası, Almanya'daki bulut bilişim hizmet sağlayıcılarının, belirli güvenlik kriterlerine uygunluğunu kanıtlamalarını sağlamak amacıyla oluşturulmuş bir programdır. Bu kapsamda, bulut hizmeti verenlerin güvenlik standartlarına uygunluğu değerlendirilerek, kullanıcılara daha güvenli ve uyumlu bulut hizmetleri sunmaları sağlanmaktadır (Maya, 2023).

Güvenilir Bulut Sertifikası, bulut hizmet sağlayıcının hizmetlerini güvenli ve etkili bir şekilde kullanılması amacıyla belirli güvenlik gereksinimlerinin yerine getirilmesi gerektiğini vurgulamaktadır. Bu gereksinimler, veri gizliliği ve güvenliği, veri bütünlüğü, veri erişimi ile müşteri hizmetleri gibi bileşenleri kapsamaktadır. Bulut hizmet sağlayıcıları, uluslararası bir standart olan Güvenilir Bulut'a uygun davranarak, kullanıcıların verilerini güvenli bir şekilde ayrıştırıp depolamalarını sağlamalıdır. Bu yaklaşım, farklı kullanıcıların verilerinin sağlıklı bir şekilde depolanmasını ve güvenlik standartlarına uygun bir şekilde yönetilmesini temin etmektedir (Sen, 2015).

F. TSE Bulut Standartları

Türk Standartları Enstitüsü (TSE) tarafından oluşturulan bir bulut bilişim standartı olan TSE Bulut Standartı ile bulut bilişim hizmeti sağlayıcılarının belirli kriterleri karşılayarak, hizmetlerini kullanıcılarına güvenli ve tutarlı bir şekilde sunmaları amaçlanmaktadır. TSE bünyesindeki Siber Güvenlik Özel Komitesi Bulut Bilişim Çalışma Grubu tarafından Bulut Bilişim Güvenlik ve Kullanım Standardı Taslağı 2014, bulut bilişim sistemleriyle ilgili olarak sektörde standartları belirlemek üzere oluşturulmuştur. Bu taslak ile bulut hizmet sağlayıcılarının hizmet kalitesi ve güvenliği konusunda uyumlu bir çerçeve oluşturarak sektörde güvenilirliğinin artırılması hedeflenmektedir (Maya, 2023).

Bu kapsamda, buluttaki kişisel verilerin korunmasına yönelik TS EN ISO/IEC 27018 Bulut Hizmetlerinde Kişisel Verilerin Korunması Yönetim Sistemi ve bulut hizmeti sağlayıcıları ile kullanıcıları için güvenli ortam oluşturarak riskleri azaltmak amacıyla geliştirilen TS EN ISO/IEC 27017 Bulut Hizmetlerinde Bilgi Güvenliği Yönetim Sistemi standartları bulunmaktadır.

SONUÇ VE ÖNERİLER

SONUÇ

Küreselleşen dünyada gerçekleşen teknolojik ilerlemeler, insanların günlük yaşantısını büyük ölçekte etkilemiştir. Dijital dönüşüm hem toplumsal yapılarda hem de bireyin toplum içindeki rollerinde büyük bir değişime yol açmıştır. Bilişim hizmetlerinin internet erişimine açık hale getirilmesiyle ihtiyaç duyulan her yerde ve her zaman bağlanabilirlik, bilgiye erişimin önemini artırmıştır. Bu kapsamda ortaya çıkan yenilikçi teknolojilerden birisi de bulut bilişimdir. NIST tarafından, minimum yönetim çabası veya hizmet sağlayıcısı etkileşimi ile hızlı bir şekilde sağlanabilen ve serbest bırakılabilen, yapılandırılabilir bilgi işlem kaynaklarının paylaşıldığı bir havuza, her yerden, uygun, isteğe bağlı ağ erişiminin sağlandığı bir model şeklinde tanımlanan bulut teknolojisi; standart bir yapıdan ziyade, kullanıcının isteği ve ihtiyacı doğrultusunda kullanılabilen esnek ve çeşitli hizmet servisleri sunmuştur.

Yeni teknolojilere ve bilgiye her yerden ulaşabilme ihtiyacı güçlü mobil teknolojileri de öne çıkarmıştır. Mobil teknolojilerde son yıllarda yaşanan gelişim, dijital dönüşümün en büyük hızlandırıcılarından biri olarak yer almaktadır. Bu kapsamda, zamana ve mekâna bağlı olmayan akıllı telefonlar, tabletler gibi mobil iletişim araçlarının hayatımızdaki yeri de giderek artmaktadır. Bireyler mobil uygulamalar üzerinden eğitim, sağlık, bankacılık gibi faaliyetlerini yürütmekte ve çeşitli hizmetler almaktadır. Teknolojik yenilikler, mobil cihazları işlem hızı ile depolama açısından giderek daha yetenekli hale getirmekte ve yeni nesil mobil teknolojiler sahayı şekillendirerek, daha düşük gecikme süresi ile daha yüksek hız sunmaktadır. Ancak mobil cihazların işleme kapasitesi giderek artsa da yeterli olmamakta; pil ömrü, depolama ile bant genişliği gibi kaynaklar bakımından sınırlı olması ve çeşitli güvenlik sorunlarını içermesi nedeniyle birçok zorlukla karşı karşıya kalmaktadır. Bu sınırlı kaynaklar da hizmet kalitesinin iyileştirilmesini önemli ölçüde engellemektedir.

Bulut bilişimin hayatımıza girmesiyle beraber, mobil uygulamaların bulut bilişimi kullanması günlük hayatı kolaylaştıracak bir faktör olarak öne çıkmıştır. Bulut bilişim,

mobil cihazlara kolayca yararlanabileceği bol miktarda bilgi işlem gücü sunmuş ve kaynak kısıtlamalı mobil cihazlara sunulan kablosuz altyapı ve bulut teknolojisi, yeni bir bilgi işlem kavramı için zemin hazırlamıştır. Bu doğrultuda hem veri işlemenin hem de veri depolamanın mobil ortam dışında gerçekleştirildiği sistemler olan mobil bulut teknolojisi ortaya çıkmıştır. Bu yenilikçi teknoloji sayesinde hesaplamalar ile veri depolama doğrudan mobil cihazda yapılması yerine bulutta yürütülmüş ve uygulamalar daha geniş bir kapsama sahip olmuştur. Kablosuz şebeke erişim teknolojilerinin gelişmesiyle de giderek popülerleşen mobil bulut bilgi işlem sayesinde cihazlar, buluta bağlanarak kablosuz şebeke üzerinden her zaman ve her yerde erişim sunmuştur. Böylece kullanıcılar, bulutta depolanan kaynaklar, uygulamalar ile verilere kolaylıkla erişebilmiş ve bilgi işlem yoluyla çeşitli hizmetleri dağıtabilmiştir. Bu durum mobil cihazların bilgi işlem gücünü, depolama kapasitesini ve bağlamsal farkındalığı artırmasını sağlamıştır. Bu bağlamda mobil bulut bilişim; mobil bankacılık, mobil eğitim, mobil sağlık, mobil bulut depolama, mobil oyun gibi sektörlerde kullanılmaya başlanmıştır.

Mobil bulut bilişim, kullanıcılarına zengin bilgi işlem kaynakları sunmak için bulut bilişim, mobil bilgi işlem ve çeşitli ağ teknolojilerini birleştiren bir platformdur. Bu yenilikçi teknolojinin nihai hedefi, uygulamaların mobil cihaz üzerinde zengin bir kullanıcı deneyimiyle yürütülmesini sağlamaktır. Mobil bulut bilişimin çalışma prensibi ise şu şekildedir; mobil cihazlar bağlantılar ile işlevsel arayüzleri kuran ve kontrol eden çeşitli ağlarla bağlanmaktadır. Mobil kullanıcıların istekleri ve bilgileri, şebeke hizmetleri sağlayan sunucuların bağlı olduğu merkezi işlemcilere iletilmektedir. Ardından, kullanıcıların istekleri internet üzerinden buluta gönderilmekte ve burada bulut denetleyicileri, mobil kullanıcıların talep ettiği hizmetlerini sağlamak üzere bu istekleri işlemektedir. Görüldüğü gibi, mobil bulut bilişim ekosistemi, mobil cihaz kullanıcıları, şebeke işletmecileri, internet servis sağlayıcıları, uygulama hizmetleri ve bulut hizmeti sağlayıcıları gibi farklı katılımcılardan oluşmaktadır. Bu paydaşlar, çeşitli şebekeler aracılığıyla birbirine bağlanmaktadır.

Mobil bulut bilişim ile kullanıcılar, bellek kapasitesi ile işlemci hızı gibi bilgi işlem ve depolama kaynaklarına ihtiyaç duymadan bulutlardaki mevcut hizmetlere erişebilmekte, tüm karmaşık bilgi işlem süreçleri mobil cihazların dışında gerçekleştirmektedir. Bu kapsamda, mobil bulut bilişimin şebekeler arası sorunsuz hizmet sunabilmesi için bazı gereksinimleri bulunmaktadır. Mobil uygulamaların yoğun kaynak kullanan bileşenlerini belirleme, bölümleme ve bulut tabanlı kaynaklara geçirme işlemi olan hesaplama-boşaltma, literatürde en çok çalışılan gereksinimlerden biridir. Bununla birlikte, kullanıcıların her yerde ve her zaman mobil bulut bilişimdeki mevcut kaynaklara erişebilmesi için veri bütünlüğü de büyük bir önem taşımaktadır. Mobil bulut bilişimin kullanılmasında, verinin bütünlüğü ile ilgili sorunların üstesinden gelmek için standart bir depolama ve yönetim altyapısı gerekmektedir.

Her an her yerden buluta erişilerek, verilerin alınması için uygun ve hızlı bir yöntem sağlamayı vadeden mobil bulut bilişim; kullanıcılarına bulut teknolojisinin sunduğu altyapı, platform ile yazılımları düşük maliyetle ve talep üzerine esnek bir şekilde kullanma olanağı tanıyarak, çeşitli avantajlar sunmaktadır. Ancak mobil bulut bilişim kullanıcılarına birçok kazanım sunarken aynı zamanda birtakım riskleri de barındırmaktadır. Bu dezavantajların temelinde mobil cihazların performans sınırlaması gelmektedir. Mobil cihazlar, depolama, ekran boyutu, işlemci kapasitesi, kablosuz iletişim, işletim sistemleri gibi her açıdan gelişmiş olsa da karmaşık uygulamaları kurmak için bilgi işlem yeteneği ve enerji kaynağında ciddi sınırlamaları içermektedir. Başka bir zorluk olarak ise bağlantı problemleri verilmektedir. Ayrıca, mobil cihaza dayalı bir uygulama geliştirmek için uygulama yazılımının, istemci tarafı basitleştirilmeli ve kullanıcı arayüz sorunları giderilmelidir. Bununla birlikte, mobil bulut teknolojisinde, mobil cihazlar, bulutlar ve kablosuz şebekeler kapsamında çeşitli donanım, mimari, altyapı ve teknolojileri sunulmakta; yapılarındaki çeşitlilik nedeniyle mobilite yönetimi ve birlikte çalışabilirlik oldukça zorlaşmaktadır.

Yürütülen çalışmalar çerçevesinde, mobil bulut bilişimin karşılaştığı en önemli sorunlardan biri olarak veri güvenliği görülmektedir. Mobil cihazlara yönelik fiziksel güvenlik kaybı, şifreleme, sanal makinelerin güvenlik ve denetim sorunları ile çeşitli kaynakların hizmet platformu uyumsuzluğu da dâhil olmak üzere birtakım güvenlik

endişeleri bulunmaktadır. Ayrıca, verilerin buluta aktarılması da veri güvenliği ve mahremiyetiyle ilgili çeşitli riskler barındırmaktadır. Diğer yenilikçi teknolojilerde olduğu gibi mobil bulut teknolojilerinde de verileri ve altyapıyı korumak büyük önem arz etmektedir. Kötü niyetli kişiler, geleneksel istemci-sunucu mimarileriyle karşılaştırıldığında mobil bulut bilgi işlem ortamında çok daha geniş bir kaynak/protokol yelpazesini hedefleyebilmektedir. Mobil bulut bilgi işlem; mobil cihaz, kablosuz şebeke sistemi ile bulut bilişim bileşenlerinden oluşmakta ve her bir unsurunun güvenlik zafiyetlerinden etkilenmektedir.

Mobil kullanıcı bilgilerinin, bulutlarda saklanması ve işlenmesi; veri kaybı, veri ihlali, veri yerelliği ile veri gizliliği gibi önemli güvenlik riskleri barındırmaktadır. Diğer taraftan, bulut üzerinden hizmet sunumunun yaygınlaşmasıyla birlikte, depolanan kişisel veri miktarı da giderek artmaktadır. Bu bağlamda, mobil kullanıcıların verilerinin işlenmesi ve mobil cihazlardan heterojen dağıtılmış bulut sunucularına iletilmesi sürecinde gizliliğin sağlanması, bulut hizmetlerine yönelik önemli bir zorluk olarak ortaya çıkmaktadır. Ayrıca, uygulamaların yürütülmesi ve kişisel verilerin depolanması konuk sistemler üzerinden yapıldığı için bulut içindeki hesaplamanın gizliliği ve bütünlüğü de ele alınması gereken endişelerden biri olarak görülmektedir. Bununla birlikte mobil cihazlara yönelik kötü amaçlı yazılımlar ya da cihazın kaybedilmesi ve çalınması gibi fiziksel tehditler de bulunmaktadır. Kablosuz şebekelerin ise tekrarlama saldırısı, ortadaki adam saldırısı ve hizmet reddi gibi birçok türdeki saldırıya karşı savunmasız olduğu da ifade edilmektedir.

Bulut teknolojisi, kablosuz şebekeler veya mobil cihazlara ilişkin alınan güvenlik önlemleri mobil bulut teknolojisini de etkilemektedir. Yapılan çalışmalarda, mobil cihazlara yönelik temel güvenlik önlemi olarak şifreleme ve biyometrik kimlik doğrulama yer almaktadır. Ayrıca güvenlik yazılımlarının kullanılması ve mobil işletim sistemi kapsamında çekirdek sağlamlaştırma, adres alanı düzeni rastgeleleştirme gibi çalışmaların yapılması da önerilmektedir.

Kablosuz şebeke güvenliğinin sağlanmasında da şifreleme ana önlem olarak belirtilmekte ve kullanıcı terminali ile şebekeye erişim noktası arasındaki iletişim

gizliliğinin büyük önem taşıdığı görülmektedir. Bulut bilişimin bileşenlerinden biri olan sanallaştırmanın güvenliğine dair tedbirlerin başında ise izolasyon gelmektedir. Ek olarak, güvenilir kimlik bilgileri yönetimi, veri bütünlüğü ile güvenli kod bölme ve boşaltmanın sağlanması da bulut teknolojisine ilişkin alınacak önlemler arasında yer almaktadır. Literatürde mobil bulut bilişime yönelik çeşitli yaklaşımlar yer alırken; bu yaklaşımların çoğunluğunun uygulamaya geçirilmediği görülmektedir.

Kişisel veri güvenliğinin teknik açıdan incelenmesi kadar gelişen teknolojilerin hâkim olduğu bu dönemde dijital hakların yönetilmesi de oldukça ehemmiyet taşımaktadır. Bu kapsamda, depolanan kişisel verilerin kötüye kullanımının engellenmesi, kişisel hakların ihlal edilmesinin önüne geçilmesi ve verinin güvenliğin sağlanması hukuki açıdan dikkat edilmesi gereken hususlardandır.

Kişisel verilerin korunma sürecine yönelik ilk adım 1948'de kabul edilen İnsan Hakları Evrensel Beyannamesi ve 1950'de imzalanan Avrupa İnsan Hakları Sözleşmesi ile atılmıştır. Yıllar içerisinde çeşitli anlaşmalar ile kişisel verilerin korunmasına yönelik bireylerin sahip olduğu haklar ve hizmet sağlayıcılarının yükümlülükleri genişlemiştir. 2018 yılında yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü'nde detaylı veri koruma kuralları getirilmiş; ayrıca veri güvenliği noktasında uygun teknik ve idari tedbirlerin alınması başta olmak üzere veri sorumlusu ve veri işleyenler için birçok yükümlülük belirlenmiştir. Ülkemizde kişisel verilerin toplanması, saklanması ve işlenmesine dair yapılan düzenlemeler kapsamında Türkiye Cumhuriyeti Anayasası, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5237 sayılı Türk Ceza Kanunu ve 5809 sayılı Elektronik Haberleşme Kanunu ele alınmıştır. Normlar hiyerarşisinin tepesinde yer alan Anayasa, kişisel verilerin korunması alanındaki tüm düzenlemelerimizin hukuki altyapısını oluşturmaktadır. Anayasamıza eklenen *"... Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* hükmü ile bu alanda çıkarılacak usul ve esasların kanun seviyesinde düzenleneceği belirtilmiştir. Bununla birlikte, TCK ile kişisel verilerin işlenmesi hakkında suçlar ve bu suçlara ilişkin cezalar belirlenmiştir. 2016 yılında, 6698 sayılı Kanun ile kişisel verilerin korunmasına yönelik genele şamil bir düzenleme hayata geçirilmiştir. Bu doğrultuda kişisel verilerin işlenmesinde başta mahremiyet olmak üzere temel hak ve

özgürlüklerin korunması saikiyle, veri işleyen gerçek ve tüzel kişilerin uyması gereken yükümlülüklerin belirlenmesi ve gerçek kişilere ait verilerin korunması amaçlanmıştır. Elektronik haberleşme sektörüne özel kanun olan ve sektörü denetleme ve düzenleme amacı taşıyan EHK'nın "Kişisel verilerin işlenmesi ve gizliliğin korunması" başlıklı 51'inci maddesi ile de kişisel verilerin korunmasında işletmecilere yönelik çeşitli hükümler düzenlenmiştir.

İncelenen kişisel verilerin korunmasına yönelik ulusal ve uluslararası düzenlemelerde, mobil bulut bilişim veya bulut bilişim özelinde hükıümlere rastlanılmamış olmakla birlikte; kişisel verilerin korunmasına ve veri güvenliği sağlanmasına ilişkin ilgili düzenlemelerde belirlenen hak ve yükümlükler bulut teknolojisini de kapsamaktadır. Bulut hizmet sağlayıcıları veri işleme faaliyetlerinde belirtilen yükümlülüklere tabi olup, uymamaları halinde düzenlemelerde öngörülen yaptırım ve cezalarla karşı karşıya kalmaktadır.

6698 sayılı Kanun incelendiğinde kişisel verilerin korunmasına ilişkin önemli tedbirlerin alındığı görülmektedir. Bu bağlamda, kişisel verilerin korunmasında kişisel verilerin işlenmesi büyük bir yer tutmaktadır. Kapsamı oldukça geniş olan kişisel verilerin işlenmesinde, mobil bulut veya bulut kullanıcısı ile hizmet sağlayıcısının rollerinin her bir durum özelinde ayrı ayrı değerlendirilmesi gerekmektedir. Öte yandan bulut bilişimde kişisel verilerin transferi de kişisel verilerin korunması kapsamında kritik önem taşımaktadır.

Mobil bulut bilişim teknolojisine yönelik mevzuat düzenlemelerine ilişkin yapılan uluslararası inceleme ve sualnameye verilen cevaplar doğrultusunda mobil bulut bilişim kapsamında özel bir mevzuat düzenlemesine rastlanılmamıştır. Ancak bulut bilişimde meydana gelen gelişmeler sonucu özellikle verilerin güvenliği başta olmak üzere kişisel verilerin korunmasına yönelik mevzuat düzenlemelerinde birtakım değişiklikler yapılmakta ve bu çerçevede çeşitli kurallar, anlaşmalar ortaya konulmaktadır. Doğası gereği mobil bulut teknolojisi de bulut bilişime ilişkin yapılan düzenlemelerden etkilenmektedir. Bu kapsamda özellikle GDPR'da veri güvenliğine

yönelik getirilen yükümlülüklerle daha yüksek bir veri güvenliği ve veri koruma standardı hedeflendiği söylenebilmektedir.

ÖNERİLER

Tez kapsamında incelenen makaleler, uluslararası ve ülkemizdeki çalışmalar değerlendirilerek elde edilen sonuçlar doğrultusunda mobil bulut bilişimde kişisel veri güvenliğinin sağlanmasına ilişkin geliştirilen önerilere aşağıda yer verilmektedir.

- **Bulut bilişime yönelik strateji ve eylem planları oluşturulurken mobil bulut teknolojisine de yer verilmesi:**

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi öncülüğünde yürütülen Türkiye Kamu Bulut Bilişim Stratejisi projesinde kamu kuruluşlarında hızlı ve güvenilir bulut bilişimin kullanımının yaygınlaşması, verimliliğin sağlanması ve yeni nesil teknolojilere değer üretmek hedefiyle bulut bilişime yönelik strateji ve eylem adımları tanımlanmaktadır. Bu proje çerçevesinde, "Kamu Bulut Bilişim Stratejisi ve Eylem Adımları, Ülke İncelemeleri, Mevcut Durum Analizi, Belgelendirme Kriterleri (Bulut Hizmet Sağlayıcılara Yönelik), Göç Rehberi" gibi çeşitli raporlar hazırlanmaktadır.

Bu raporlarda ve hazırlanması öngörülen diğer planlarda, bulut bilişimle beraber, mobil bulut teknolojisinin de ele alınmasının yerinde olacağı değerlendirilmektedir. Hızla gelişen mobil teknolojilerin etkisi ile mobil cihazların kullanımı ve mobil bulut tabanlı uygulamaların sayısı giderek artmaktadır. Her ne kadar bulut bilişimin bir alt dalı olarak görülse de mobil bulut teknolojisi ayrı bir başlık altında ele alınarak, söz konusu teknolojiye yönelik özel strateji ve eylem adımlarına yer verilmelidir. Bu kapsamda, yayımlanacak strateji ve eylem adımlarında mobil bulut bilişimin genel bir tanımlanmasının yapılması da belirleyici bir unsur olacaktır. Ayrıca bulut bilişim ve mobil bulut bilişimin değerlendirilme çerçevesinin sadece kamu sektörüne yönelik değil, genele şamil şekilde oluşturulmasının daha faydalı olacağı değerlendirilmektedir.

- **Biyometrik kimlik doğrulamanın mobil buluta taşınması:**

Mobil cihazlar üzerinde güvenliğin sağlanmasında kimlik doğrulama yöntemlerinden genellikle şifreleme kullanılmaktadır. Şifreleme yönteminde, kullanıcı tarafından belirlenen şifreye göre güvenlik seviyesi belirlenmektedir. Eğer kullanıcı basit şifre belirlerse, saldırganlar tarafından ele geçirilen cihazın şifresi çözülebilmekte ve yer alan kişisel bilgiler aleyhine kullanılabilmektedir. Bu doğrultuda, kullanıcı tarafından noktalama işaretleri, rakam veya harflerin bir birleşiminden oluşan görece daha zor ve karmaşık şifreler belirlenmektedir. Ancak bu şifreler de karmaşıklıklarından dolayı unutulabilmekte ve kullanım bakımından elverişli olmayabilmektedir. Tüm bu sebeplerden ötürü, kullanıcının hatırlamasına ihtiyaç duyulmayan ve kişiye özgü bir şifreleleme yöntemi olan biyometrik teknikler kullanılmaya başlanmıştır. Biyometrik kimlik doğrulamada, bireylerin parmak izi, ses, iris, yüz, avuç izi gibi bilgileri kullanılmaktadır. Söz konusu biyometrik veriler ise cihaz üzerinde saklanmaktadır. Ayrıca biyometrik kimlik doğrulamanın kullanılması için mobil cihazların bazı işlevlere sahip olması gerekmektedir.

Günümüzde mobil cihazlar bir tüketim malı haline gelmiş, alımı ve satımı gittikçe yaygınlaşmıştır. Mobil cihazların satılmadan önce fabrika ayarlarına sıfırlanması, tüm kişisel verileri ve ayarları otomatik olarak silmemektedir. Bazı üreticiler, biyometrik verilerin yanlışlıkla kalıcı olarak silinmesini önlemek için ayrıca güvenlik önlemleri uygulamaktadır. Bu doğrultuda, mobil cihaz üzerinde depolanan biyometrik verilerin silinmesi için “hard reset” denilen, cihazın ilk alındığı duruma getirildiği sıfırlama tekniğinin kullanılması gerekmektedir. Ancak bu durum, çoğu mobil cihaz kullanıcısı tarafından bilinmememekte ve cihazın fabrika ayarlarına döndürülmesinin yeterli olduğu düşünülmektedir. Bu kapsamda, biyometrik veriler cihazların alımı veya satımıyla birlikte kötü niyetli kişilerin eline geçebilmektedir.

Biyometrik kimlik doğrulamanın buluta taşınmasıyla beraber bu tür sorunların önüne geçilebileceği değerlendirilmektedir. Bulut tabanlı biyometrik kimlik doğrulamada, cihazdaki güvenlik açıklarından etkilenilmemektedir. Ayrıca cihaz üzerinde kimlik doğrulamada, cihazı en son yazılım ve güvenlik yamalarıyla güncel tutma sorumluluğu

cihaz sahibindedir. Bulut sisteminde ise güvenlik açıklarına yönelik önlemler teknik ekiplerce hızlıca alınmaktadır. Bununla birlikte, kimlik doğrulama süreci donanımdan bağımsız olmakta ve cihaz yalnızca aracı olarak yer almaktadır. Böylece mobil cihazların biyometrik kimlik doğrulama kapsamında ihtiyacı olan teknik gereksinimlere sahip olmasa bile bu kimlik doğrulama türünü kullanabilmesine olanak sağlamaktadır.

Öte yandan, 6698 sayılı Kanun kapsamında özel nitelikli veriler arasında sayılarak gerek işlenme gerekse bulut hizmet sağlayıcılar gibi üçüncü taraflara aktarım bakımından belirli koşullara tabi tutulan biyometrik verilerin mobil cihazlar için kimlik doğrulama amacıyla kullanılması ve mobil buluta taşınması durumunda ilgili veri sorumlularının ve veri işleyenlerin 6698 sayılı Kanun'un 9'uncu maddesi başta olmak üzere ilgili maddelerini, Kişisel Verileri Koruma Kurulu'nun "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" başlıklı Kararını[1] ve Kurul tarafından hazırlanan "Kişisel Veri Güvenliği Rehberi"ni[2] dikkate almaları yerinde olacaktır.

- **Mobil bulut bilişim kullanıcılarına farkındalıklarının artmasına yönelik eğitimlerin verilmesi:**

Tüketici dışında kalan diğer mobil bulut bilişim kullanıcıları sözleşmelerin hukuki boyutu bakımından profesyonel yardım alma konusunda daha avantajlı bir konumda yer almaktadır. Ancak tüketiciler hem teknik hem de sözleşme hükümleri açısından diğer kullanıcılara kıyasla daha dezavantajlı kalmaktadır. Bu doğrultuda tüketicilerin mobil bulut hizmet sağlayıcılarını dikkatle seçmesi ve onayladıkları sözleşmelerin içeriğinden haberdar olmalarına yönelik farkındalıklarının artırılabilmesi için eğitimler hazırlanarak, çeşitli platformlar üzerinden yayımlanması önem arz etmektedir. Bu kapsamda, Bilgi Teknolojileri ve İletişim Kurumu bünyesinde yer alan

[1] Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı için bknz. https://www.kvkk.gov.tr/Icerik/4110/2018-10

[2] Kişisel Veri Güvenliği Rehberi için bknz. https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

BTK Akademi üzerinde, kişilerin mobil bulut teknolojisi ve bulut bilişim hizmet sağlayıcılarını seçerken dikkat etmeleri gereken hususlara, onayladıkları sözleşmelerin içeriğine, sahip oldukları imkânlara, özellikle mobil bulut uygulamalarının talep ettiği izinlere yönelik dijital okuryazarlıklarının ve bilinç düzeylerinin artırılmasına yönelik sunulan eğitimlerin ve videoların artırılmasının faydalı olacağı değerlendirilmektedir.

- **Mobil bulut bilişime yönelik gerekli siber güvenlik önlemlerinin alınması:**

Mobil bulut bilişim sistemlerine ve ana kolu olan bulut teknolojisine yapılan saldırılarda, verilerin üçüncü kişilerin eline geçmesini önlemek amacıyla alınabilecek güvenlik tedbirlerinin en başında şifreleme gelmektedir. Bu doğrultuda, Kişisel Verileri Koruma Kurulunun yayımlamış olduğu rehberde de verilerin bulutta şifreli olarak tutulması konusu ele alınmaktadır.

Veri güvenliği ile kişisel bilgilerin korunabilmesi için en temel çözüm olarak şifreleme belirtilmektedir. Güvenli şifreleme algoritmalarının kullanılmasıyla birlikte veri gizliliği sağlanırken, analiz ile işleme için kullanılabilirlik korunmakta ve yüksek düzeyde işlevsellik de sunulmaktadır. Bu bağlamda, mobil bulut hizmet sağlayıcılarının gerekli şifreleme önlemlerini standart olarak kullanmalarını sağlayacak denetimlerin yapılması gerektiği de değerlendirilmektedir.

Bilgi Teknolojileri ve İletişim Kurumu bünyesinde bulunan Ulusal Siber Olaylara Müdahale Merkezi (USOM)'nin siber saldırılara karşı önemli bir yeri bulunmaktadır. Günden güne artan kullanımıyla birlikte sık sık siber saldırılar ile karşı karşıya kalan mobil bulut bilişime ilişkin USOM önderliğinde, çeşitli iş birlikleri kurularak, koordineli çalışmalar yürütülmesinin faydalı olacağı öngörülmektedir.

Bu doğrultuda, özellikle kamu kurumları başta olmak üzere bulut ve mobil bulut teknolojisine yönelik siber saldırılar konusunda personele eğitim verilmesi, kullanılan sistemlerin siber saldırılara karşı dirençli hale getirilmesi, teknolojik gelişmelerin takip edilerek gerekli güncellemelerin yapılmasının bulut ve mobil bulut teknolojisini siber saldırılara karşı daha güvenli hale getireceği değerlendirilmektedir.

- **Bulut bilişim teknolojisi kapsamında ortaya çıkan yenilikler sebebiyle mevzuatta yapılacak değişikliklerde mobil bulut bilişimin de ele alınması ve bu doğrultuda yapılacak değişikliklerde BTK'nın aktif rol alması:**

Bulut bilişim ve mobil bulut teknolojisindeki gelişmeler nedeniyle yapılacak mevzuat çalışmalarında BTK'nın özellikle siber güvenlik alanındaki görev ve yetkisi sebebiyle bulut ve mobil bulut bilişimde ihtiyaç duyulabilecek teknik ve hukuki gereksinimleri tespit edebileceği öngörülmekle birlikte, bu kapsamda yapılabilecek çalışmaların bulut ve mobil bulut teknolojisine uygun olmasının da temininde yarar bulunmaktadır.

Ayrıca teknolojinin hayatımızdaki yerinin giderek artmasıyla birlikte paylaşılan veri miktarı da çoğalmakta ve kişisel verilerin korunması kritik önemi haiz olmaktadır. Bu kapsamda, BTK'nın aktif katılımında Kişisel Verileri Koruma Kurumu gibi ilgili paydaşlarla iş birliği yapılarak ve bulut ile mobil bulut teknolojisinin getirdiği gelişmeler göz önünde bulundurularak, kişisel verilerin korunması ve güvenliği hususunda ortak çalışma yapılmasının faydalı olacağı değerlendirilmektedir.

Bununla birlikte bulut bilişim hizmet sağlayıcılarının, gerçek veya tüzel kişilerle yaptıkları gizlilik sözleşmelerinin Kişisel Verileri Koruma Kurumu tarafından incelenmesi ve sunulan bulut hizmetleri açısından uygulama birliğinin sağlanmasının faydalı olacağı değerlendirilmektedir.

- **Mobil bulut bilişim teknolojisinde standardizasyonun oluşturulması:**

Mobil cihaz kullanımının günlük hayatta giderek artması ve gelişiminin sürekli devam etmesi, mobil bulut bilişimin teknik ve teknolojik altyapısına uygun sertfika temelli standardizasyonun yapılmasının gerekliliğini ortaya koymaktadır. Bulut ve mobil bulut teknolojisindeki ilerlemeler analiz edilerek, ülkemizde hizmet verecek bulut servis sağlayıcılarına, sundukları bulut temelli mobil uygulamalar da göz önünde bulundurularak ulusal ve uluslararası temel sertifikaları bulundurma ile ilgili standartlara uyma şartının söz konusu teknolojiye yönelik hizmet kalitesini artıracağı düşünülmektedir.

Bu doğrultuda, bilgi teknolojileri alanındaki uluslararası standartların takip edilerek, mobil bulut bilişimi de kapsayacak şekilde bulut bilişime yönelik çeşitli sertifika ve standardizasyon çalışmalarında BTK'nın TSE ile iş birliği yapmasının da yararlı olacağı değerlendirilmektedir.

- **Kamu Bulutunda çoklu kiracılık modelinin uygulanması:**

Ülkemizde kamu kurum ve kuruluşları, veri merkezleri ile sistem odalarını geleneksel olarak kendi bünyelerinde kurarak, donanım ve yazılım ihtiyaçlarını kurum kendi imkânlarıyla karşılamaktadır. Ancak her kurumun kendi altyapısını kurması ve işletmesi, yüksek yatırım ile işletme maliyetlerine yol açmaktadır. Ayrıca farklı kurumlar tarafından kurulan ve işletilen altyapılarda birlikte çalışılabilirlik hususunda da birtakım tutarsızlıklar oluşabilmektedir. Diğer taraftan, farklı güvenlik protokolleri ile standartlar kullanılan altyapılar, siber saldırılara karşı daha savunmasız hale gelmekte ve hassas kamu verilerinin güvenliğini riske atmaktadır. Bu gibi durumlar kurumlar arasındaki veri paylaşımı ile iş birliğini zorlaştırarak hem genel sistem verimliliğini hem de kamu kaynaklarının daha etkin kullanımını azaltmaktadır.

Bu doğrultuda söz konusu dezavantajları ortadan kaldırmak için kamu kurumlarında veri merkezi altyapısının çoklu kiracılık modeli ile kullanılmasının faydalı olacağı değerlendirilmektedir. Böylece merkezi bir altyapı üzerinden kamu kurumlarına bulut hizmetinin sunulması ile her kurumun kendi yatırımını yapmasına kıyasla daha düşük maliyete katlanacağı öngörülmekle beraber, kamu kaynaklarının daha verimli bir şekilde kullanılmasına da yardımcı olacaktır. Özellikle orta ve küçük ölçekli kamu kurumlarının kendi veri merkezlerini işletmek yerine ortak bir bulut veri merkezinden hizmet almalarının kısıtlı kaynakların etkin kullanımına yönelik başka bir avantaj olacağı da düşünülmektedir. Bununla birlikte, kamu sektöründe bu şekilde bir ortamın kurulması için devletin direkt kurabileceği anonim şirketinin veya mevcut büyük çaplı internet servis sağlayıcılarının öncülük ederek söz konusu hizmeti sağlanmasının ve ayrıca bu kapsamda bir teşvik uygulamasının da faydalı olacağını değerlendirilmektir.

KAYNAKLAR

ABOLFAZLI Saeid vd., 2015, Mobile Cloud Computing: The State-Of-The-Art, Challenges, And Future Research, https://www.researchgate.net/publication/266774480_MOBILE_CLOUD_COMPUTING_THE_STATE-OF-THE-ART_CHALLENGES_AND_FUTURE_RESEARCH, (10.08.2023)

AERY Manish, 2016, Mobile Cloud Computing: Security Issues and Challenges, International Journal of Advanced Computer Research, https://www.researchgate.net/publication/323028305_Mobile_Cloud_Computing_Security_Issues_and_Challenges, (10.08.2023)

AHMED Ejaz vd., 2015, Application Optimization in Mobile Cloud Computing: Motivation, Taxonomies, and Open Challenges, Journal of Network and Computer Applications, Cilt 52, s.52-68

ANABİLGİ ANADOLU, 2020, Bağlam Farkındalıklı Bilgi İşlem, https://anabilgi.anadolu.edu.tr/?contentId=171027, (10.08.2023)

ALIBABA, 2023, Mobile Platform as a Service, https://www.alibabacloud.com/help/en/mobile-platform-as-a-service?spm=a2c63.p38356.0.0.11bf3fc4aG84e, (25.11.2023)

AL-JANABI Samaher vd., 2017, Mobile Cloud Computing: Challenges and Future Research Directions, 10th International Conference on Developments in eSystems Engineering

ALIZADEH Mojtaba vd., 2013, A Brief Review of Mobile Cloud Computing Opportunities. Research Notes in Information Science, Cilt 12, s.155-160

ALIZADEH Mojtaba vd., 2014, Feasibility of Implementing Multi-Factor Authentication Schemes İn Mobile Cloud Computing, 5th International Conference on Intelligent Systems, Modelling and Simulation

ALLAM Hesham vd., 2017, A Critical Overview of Latest Challenges and Solutions of Mobile Cloud Computing, Second International Conference on Fog and Mobile Edge Computing

ALNAJRANI Hussain Mutlaq, NORMAN Azah Anir, 2020, The Effects of Applying Privacy By Design to Preserve Privacy and Personal Data Protection in Mobile Cloud Computing: An Exploratory Study, Symmetry, Cilt 12, Sayı 2039

AMAZON, 2023a, AWS Amplify, https://aws.amazon.com/tr/amplify/, (10.11.2023)

AMAZON, 2020, CareMonitor Scales Telehealth and Remote Patient Monitoring Platform with AWS, https://aws.amazon.com/tr/solutions/case-studies/caremonitor/, (10.11.2023)

AMAZON, 2023b, AWS Device Farm, https://aws.amazon.com/tr/device-farm/, (10.11.2023)

AMAZON, 2023c, AWS Wavelength, https://aws.amazon.com/tr/wavelength/, (10.11.2023)

AMAZON, 2023d, Bulut Bilişim Uyumluluğu Denetimler Kataloğu (C5), https://aws.amazon.com/tr/compliance/bsi-c5/, (12.01.2023).

AYDIN Sedat Erdem, 2014, AİHM İçtihatları Kapsamında Kişisel Verilerin Kaydedilmesi Suçu, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul

BAHL Paramvir vd., 2012 Advancing The State of Mobile Cloud Computing, Proceedings of The Third ACM Workshop on Mobile Cloud Computing and Services

BINGLAW Ftayem, 2021, Nesnelerin İnternetinde Güvenlik Konuları: Gereksinimler, Saldırılar ve Karşı Önlemler, Yüksek Lisans Tezi, Ankara

BHATIA Punit, 2023, Contents of the Data Protection Policy according to GDPR, https://advisera.com/articles/contents-of-the-data-protection-policy-according-to-gdpr/, (29.12.2023)

BOZ Ahmet, 2014, Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Güvenlik Stratejileri ve Yönetimi Ana Bilim Dalı, Yüksek Lisans Tezi, Ankara

BULUTİSTAN, 2021, Hybrid Cloud (Hibrit Bulut) Nedir? İşletmeler Neden Hibrit Bulut Bilişim Teknolojilerini Kullanmalıdır?, https://bulutistan.com/blog/hybrid-cloud-hibrit-bulut-nedir/, (20.04.2023)

CAREEM, 2023, https://www.careem.com/en-AE/engineering-at-careem, (29.12.2023).

CBDDO, 2020, Bilgi ve İletişim Güvenliği Rehberi, https://cbddo.gov.tr/bigrehber/, (01.01.2024)

CHANG Ruay-Shiung vd., 2013, Mobile Cloud Computing Research - Issues, Challenges, and Needs, 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, s.442-452

CHAVAN Pragati, RAJANI Rakesh, 2013, Mobile Cloud Computing for Cloud Based Application and Services-Security Considerations, International Journal of Engineering Research & Technology, Cilt 2, Sayı 10, s.877-879

CHINANU Uwazie Emmanuel vd., 2018, Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures, Scientific Review, Cilt 4, Sayı 10, s.80-89

COUNCIL OF EUROPE, 1981, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108, (20.12.2023)

CSA, 2023a, Cloud Security Alliance, Security, Trust, Assurance and Rısk (STAR) https://cloudsecurityalliance.org/star/, (01.01.2024)

CSA, 2023b, Cloud Security Alliance, Cloud Controls Matrıx (CCM) https://cloudsecurityalliance.org/research/cloud-controls-matrix/, (01.01.2024)

ÇELİK Yeşim, 2017, Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı. Türkiye Adalet Akademisi Dergisi, Cilt 8, Sayı 32, s.391

ÇELİKEL Serdar, 2022, Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, Ankara, 2022

DAI Qinyun vd., 2012, An Improved Security Service Scheme in Mobile Cloud Environment, IEEE 2nd International Conference on Cloud Computing and Intelligence Systems

DATAVERSITY, 2021, A Brief History of Cloud Computing, https://www.dataversity.net/brief-history-cloud-computing/#, (15.03.2023)

DEV Dipayan, BAISHNAB Krishna, 2014, A Review and research towards Mobile Cloud Computing, 2nd IEEE International Conference on Mobile Cloud Computing, Services and Engineering

DEVELİOĞLU Hüseyin Murat, 2017, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul

DINH Hoang T. vd., 2011, A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches, Wireless Communications and Mobile Computing, Cilt 13, Sayı 18, s.1587-1611

DÜLGER Murat Volkan, 2019, Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Kullanılması, Yaşar Hukuk Dergisi Cilt 1, Sayı 2

EDPS, 2012, European Data Protection Supervisor, 2012, Data protection reform package, https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf, (10.01.2023).

EU CLOUD, 2020, EU Cloud Code of Conduct, EU Data Protection Code of Conduct for Cloud Service Providers, 2.10 version, https://eucoc.cloud/fileadmin/cloud-coc/files/former-versions/European_Cloud_Code_of_Conduct_2.10.pdf, (03.01.2024)

EUROCLOUD, 2023, Staraudit, https://eurocloud.org/streams/staraudit/, (01.01.2024)

FELLAH Hadjer vd., 2020, Mobile Cloud Computing: Architecture, Advantages and Security Issues, Proceedings of the 3rd International Conference on Networking, Information Systems, s.1-9

FERNANDO Niroshinie vd., 2013, Mobile Cloud Computing: A Survey, Future Generation Computer Systems, Cilt 29, Sayı 1, s.84-106

GAYATHRI M. R., SRINIVAS K., 2014, A Survey on Mobile Cloud Computing Architecture, Applications and Challenges, International Journal of Scientific Research Engineering & Technology, Cilt 3, Sayı 6, s.1013-1021

GDPR, 2018, General Data Protection Regulation, https://gdpr-info.eu/, (28.12.2023)

GIAKOUMOPOULOS Christos vd., 2018, Handbook on European Data Protection Law, Publications Office of the European Union, Luxembourg

GİTMEZ Emin, 2023, Bulut Bilişimde Gizlilik Sözleşmesi, Selçuk Üniversitesi Hukuk Fakültesi Dergisi., Cilt 31, Sayı 2, s.629-663

GLASSHOUSE, 2021, Bulut Bilişimin Beş Temel Özelliği ve Türkiye'nin İhtiyacı Olan Altıncı Özellik, https://www.glasshouse.com.tr/list/bulut-bilisimin-bes-temel-ozelligi-ve-turkiyenin-ihtiyaci-olan-altinci-ozellik#:~:text=NIST%20tan%C4%B1m%C4%B1ndan%20hareketle%20bulut%20bili%C5%9Fiminin,%C3%BCzere%20be%C5%9F%20temel%20%C3%B6zelli%C4%9Fi%20i%C3%A7ermelidir, (15.03.2023)

GOOGLE CLOUD, 2019, JapanTaxi Co., Ltd. Implementation Example: Utilizing Bigquery to Build a Data Analysis Platform That Supports JapanTaxi, One Of The Largest Taxi Dispatch Apps in Japan https://cloud.google.com/blog/ja/topics/customers/japantaxi-bigquery?hl=ja, (12.01.2024)

GOOGLE CLOUD, 2023a, Starling Bank: Enhancing Data-Driven Decision-Making with BigQuery, https://cloud.google.com/customers/starling-bank, (15.12.2023)

GOOGLE CLOUD, 2023b, Reshaping Flipkart's Technological Landscape with a Mammoth Cloud Migration, https://cloud.google.com/blog/products/data-analytics/flipkarts-dx-journey-to-futureproof-its-platform, (12.01.2024)

GOOGLE CLOUD, 2024, Google Cloud Mobile App: A Troubleshooting and Management Companion For Your Cloud Applications, https://cloud.google.com/blog/products/management-tools/google-cloud-mobile-app-overview, (20.01.2024)

GU Qijun, GUIRGUIS Mina, 2013, Secure Mobile Cloud Computing and Security Issues, High Performance Cloud Auditing and Applications, s.65-90

GUPTA Pragya, GUPTA Sudha, 2012, Mobile Cloud Computing: The Future of Cloud, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Cilt 1, Sayı 3, s.134-145

HADDADPAJOUH Hamde vd, 2021, A survey on internet of things security: Requirements, challenges, and solutions, Internet of Things, Cilt 14, 100129

HIREMATH Tej C., MALLAPUR Jayashree D., 2015, Mobile Cloud Computing: A Survey of Research Issues & Challenges, International Journal of Innovation in Engineering, Research and Technology ICITDCEME'15 Conference

HUANG Dijiang vd., 2013, Mobile Cloud Computing Service Models: A User-Centric Approach, IEEE Network, Cilt 27, Sayı, s.6-11

HUAWEI, 2023a, HUAWEI Mobil Cloud, https://consumer.huawei.com/tr/mobileservices/mobilecloud/, (20.11.2023)

HUAWEI, 2023b, HUAWEI Mobil Bulut'ta Veri Koruma ve Güvenlik, https://cloud.huawei.com/security, (20.11.2023)

HUKUK VE BİLİŞİM DERGİSİ, 2022, KVKK ve GDPR Arasında Genel İlkelerin Kıyası, https://www.hukukvebilisimdergisi.com/kvkk-ve-gdpr-arasinda-genel-ilkelerin-kiyasi/, (27.12.2023)

IBM, 2023a, Mobile App Development Platform, https://www.ibm.com/cloud/mobile, (15.11.2023)

IBM, 2023b, IBM Cloud App ID, https://www.ibm.com/products/app-id, (15.11.223)

IBM, 2023c, IBM Push Notifications, https://www.ibm.com/products/push-notifications, (15.11.2023)

IBM, 2023d, IBM Cloud App Configuration. https://www.ibm.com/products/app-configuration, (15.11.2023)

IBM, 2023e, IBM API Connect, https://www.ibm.com/products/api-connect#Use+cases, (15.11.2023)

IBM, 2023f, IBM Cloudant, https://www.ibm.com/products/cloudant, (15.11.2023)

IBM, 2023g, IBM MaaS360 Mobile Device Management (SaaS), https://www.ibm.com/docs/en/maas360, (15.11.2023)

IONOS, 2023, Welcome to the IONOS Help Center, https://www.ionos.com/help/, (30.12.2023)

JALAN Shraddha A., BHAGAT Vaishali B., 2014, Mobile Cloud Computing An Efficient Technique for Mobile Users, International Journal of Computer Science and Mobile Computing, Cilt 3, Sayı 3, s.145-154

JEEVAN J vd., 2014, Mobile Cloud Computing Service Models: A User-Centric Approach, International Journal of Scientific Engineering and Techology Research, Cilt 3, Sayı 8, s.1507-1515

KARTHIK Setti, MANHAR Advin, 2020, Mobile Cloud Computing Research-Issues, Challenges and Needs, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, s.241-262

KALENDER Ata Umur, 2020, Parçalı Bulutlar, Cloud Act ve Etkileri, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 2, s. 74-107

KAYA İslam Safa, TOLUN Yüksel, 2020, Uygulayıcılar için Türkiye'de ve Avrupa'da Kişisel Verilerin İşlenmesi KVKK-GDPR Karşılaştırması, Adalet Yayınevi

KILINÇ Doğan, 2012, Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 61, Sayı 3, s.1089-1169

KORKMAZ İbrahim, 2016, Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, Türkiye Barolar Birliği Dergisi

KÜZECİ Elif, 2010, Kişisel Verilerin Korunması, Ankara

KVKK, 2018a, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf, (10.01.2023)

KVKK, 2018b, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, (23.12.2023)

KVKK, 2023a, Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler, (29.12.2023)

KVKK, 2023b, Kişisel Verilerin Yurt Dışına Aktarılması, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7387ee16-00cc-4502-8a0d-28f6f28f4d39.pdf, (05.05.2024)

KVKK, 2023c, Mobil Uygulamalarda Mahremiyetin Korunmasına Yönelik Tavsiyeler, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8ba209bb-fa93-4479-84f0-dd55aac97a0f.pdf, (04.01.2024)

KVKK BLOG, 2023, Kişisel Verilerin Korunması Tarihine Yolculuk, https://kvkkblog.com/kisisel-verilerin-korunmasi-tarihine-yolculuk/#:~:text=108%20say%C4%B1l%C4%B1%20S%C3%B6zle%C5%9Fmenin%20yenilenmesi%20ve,Bakanlar%20Komitesi%20taraf%C4%B1ndan%20kabul%20edilmi%C5%9Ftir., (25.12.2023)

LIV, 2024, Data Privacy Policy, https://www.liv.me/en/privacy, (11.01.2024)

MALIK Sapna, CHATURVEDI MM, 2013, Privacy and Security in Mobile Cloud Computing: Review, International Journal of Computer Applications, Cilt 80, Sayı 11, s.20-26

MAPLE, 2024, We Take Excellent Care of Your Data, https://www.getmaple.ca/security/, (04.01.2024)

MAYA Duygu, 2023, 6698 sayılı Kişisel Verilerin Korunması Kanunu Çerçevesinde Bulut Bilişim Sistemleri, Bahçeşehir Üniversitesi Lisansüstü Eğitim Ensitüsü, Özel Hukuk Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul

MEDIUM, 2019, Case study: Carrier IQ, https://medium.com/golden-data/case-study-carrier-iq-cad935f30ab7, (06.05.2023)

MEDIUM, 2023, Title: Zomato's Cloud Odyssey: A Delicious Tale of Success with AWS, https://medium.com/@mahimarastogi7603/title-zomatos-cloud-odyssey-a-delicious-tale-of-success-with-aws-56dfa0e733e2, (09.01.2024)

MICROSOFT, 2021, Emirates NBD's Liv. Elevates Digital Banking Experiences with Microsoft Azure Cloud Services, https://news.microsoft.com/en-xm/2021/07/15/emirates-nbds-liv-elevates-digital-banking-experiences-with-microsoft-azure-cloud-services/, (12.01.2024)

MICROSOFT, 2023, Mobile Apps, https://azure.microsoft.com/en-us/products/app-service/mobile, (02.01.2024)

NOOR Talal H. vd., 2018, Mobile Cloud Computing: Challenges and Future Research Directions, Journal of Network and Computer Applications, Cilt 115, s.70-85

OECD, 2002, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris

OECD, 2023, Personal Data Protection at the OECD, https://www.oecd.org/general/data-protection.htm, (28.12.2023)

OPEN TELEKOM CLOUD, 2023, Cloud Technology Use Cases, https://www.open-telekom-cloud.com/en/solutions/use-cases, (28.12.2023)

RAKUTEN, 2024, Start Selling in Japan, https://marketplace.rakuten.net/, (15.01.2024)

PAŞAOĞLU Cengiz, CEVHEROĞLU Emel, 2020, Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması, Cilt 13, Sayı 2, s.183-195.

PRASAD Rajendra M. vd., 2012, Mobile Cloud Computing: Implications and Challenges, Journal of Information Engineering and Applications, Cilt 2, Sayı 7, s.7-15

SANAEI Zohreh vd., 2014, Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges, IEEE Communications Surveys & Tutorials, Cilt 16, Sayı 1, s.369-392

SHAMSHIRBAND Shahab vd., 2020, Computational Intelligence Intrusion Detection Techniques in Mobile Cloud Computing Environments: Review, Taxonomy and Open Research Issues, Journal of Information Security and Applications, Cilt 55, s.102582

SCHWARTZ P. M., 2013, Information Privacy in the Cloud, University of Pennsylvania Law Review, s.1624-1662

SEN Jaydip, 2015, Security and Privacy Issues in Cloud Computing, Cloud Technology, s.1585-1630

SHOPIFY, 2023a, Shopify's Infrastructure Collaboration with Google, https://shopify.engineering/shopify-infrastructure-collaboration-with-google, (30.12.2023).

SHOPIFY, 2023b, Security of Transfers of Personal Data, https://help.shopify.com/en/manual/privacy-and-security/privacy/international-data-transfers, (30.12.2023)

SIAS Suzanne L., 2008, Confidentiality and Nondisclosure Agreements, Buisness Law, Cilt 4, s.3-4

STARLING BANK, 2023, Mobile Banking Security, https://www.starlingbank.com/mobile-banking-security/, (29.12.2023)

ŞAHİN Osman, 2011, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Korunması, Bilgi Teknolojileri ve İletişim Kurumu Bilişim Uzmanlık Tezi, Ankara

TUNÇ, Aybike, 2020, Bulut Bilişim Sözleşmeleri, Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, Özel Hukuk Anabilim Dalı, Doktora Tezi, Ankara.

ÜLKER İsmail, 2016, Kişisel Verilerin İşlenmesi ve Korunması Konusunda Elektronik Haberleşme Sektörüne Yönelik Düzenlemeler, Bilgi Teknolojileri ve İletişim Kurumu Bilişim Uzmanlık Tezi, Ankara.

ZHOU Bower, BUYYA Rajkumar, 2018, Augmentation Techniques for Mobile Cloud Computing, ACM Computing Surveys, Cilt 51, Sayı 1, s.1-38

ZOMATO, 2011, Zomato is Now on Android, https://blog.zomato.com/zomato-is-now-on-android, (04.01.2024)

18/10/1982 tarihli ve 2709 sayılı Türkiye Cumhuriyeti Anayasası, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5, (20.01.2023)

5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu, https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5809.pdf, (04.01.2023).

24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu, https://www.resmigazete.gov.tr/eskiler/2016/04/20160407.htm, (23.12.2023).

EKLER

Ek-1) Bağımsız Düzenleyiciler Grubu (Independent Regulators Group-IRG) Üyesi Ülkelere Mobil Bulut Bilişimin Kişisel Veri Güvenliği Açısından İncelenmesine İlişkin Sualname

1. Do you have Mobile Cloud Computing applications used in the public sector in your country?

If yes,

1.1 In which areas (health, education, agriculture etc.) are these applications being used?

1.2 Do you cooperate with technological companies in your country on this issue?

1.3 Do the applications used have legal validity?

2. Are there any regulation regarding Mobile Cloud Computing in force in your country?

If yes,

2.1 What technical standards, regulations or legislation do you take as references?

If no,

2.2 Do you have any work on this?

3. Do you have any work to protect personal data in Mobile Cloud Computing?

If yes,

3.1 What is the technical subject/standard you take as references? In this context, what are your cyber security studies?

4. Please kindly provide any relevant additional information, document or web page.

Ek-2) Bağımsız Düzenleyiciler Grubu (Independent Regulators Group-IRG) Üyesi Ülkelere Mobil Bulut Bilişimin Kişisel Veri Güvenliği Açısından İncelenmesine İlişkin Sualnamenin Gayri Resmi Çevirisi

SORU / ÜLKE (Düzenleyici Kurum)	1. Ülkenizde kamu sektöründe kullanmakta olduğunuz mobil bulut bilişim uygulaması bulunmakta mıdır?
Avusturya (RTR)	Herhangi bir mobil bulut bilişim uygulaması kullanılmamakla birlikte, bu tür faaliyetler RTR'ye raporlanmamaktadır. Söz konusu anket RTR yetkisinde olmayıp, sorularla ilgili olan tarafta bilinmemektedir.
Birleşik Krallık (OFCOM)	Bu tür bilgiler tutulmamaktadır.
Çek Cumhuriyeti (CTU)	Bu konu CTU'nun yetki alanının dışında kalmaktadır.
Fransa (ARCEP)	Yapılan mobil bulut bilişim uygulamaları tanımı kapsamında, kendi başında bulut teknolojisine erişim sağlayacak mobil uygulamalar kullanmamaktayız. Ancak SaaS hizmetlerini de kapsandığında, kamu hizmetinde kullanılan birçok uygulama bulunmaktadır. ARCEP bu alanda özel yetkinliklere sahip olmamakla birlikte, genellikle kamu idarelerine yönelik dijital hizmet projeleri için Bakanlıklar Arası Dijital Konular Yönergesinin (DINUM) çalışmalarına dayanılmaktadır. Bu alanda, genel uygulanabilir yasal standartlar dışında kalan özel düzenlemeler bilinmemektedir.
İrlanda (ComReg)	-
Kıbrıs (OCECPR)	Kamu sektöründe bulut hizmetlerinin benimsenmesini teşvik edecek her türlü tedbir, Araştırma, İnovasyon ve Dijital Politika Bakan Yardımcılığının yetkisinde yer almaktadır.
Lihtenştayn (AK)	-
Norveç (NKOM)	Soruların kapsamı Nkom'un yetkileri dışında olmakla birlikte, Norveç Dijitalleşme Ajansı (https://www.digdir.no/) ve Norveç Veri Koruma Kurumu (https://www.datatilsynet.no/en/) bakılması uygun olacağı değerlendirilmektedir.
Portekiz (ANACOM)	Bu konu ANACOM'un yetkileri dışında olmakla birlikte, herhangi bir katkımız bulunmamaktadır.
Slovakya (RU)	-
Slovenya (AKOS)	AKOS'un yetki alanına girmediği için konuyla ilgili herhangi bir bilgi bulunmamaktadır.

Eğer evetse,

SORU / ÜLKE (Düzenleyici Kurum)	1.1 Bu uygulamalar hangi alanlarda (sağlık, eğitim, tarım vb.) kullanılmaktadır?	1.2 Bu konuda ülkenizdeki teknoloji şirketleriyle iş birliği yapıyor musunuz?	1.3 Kullanılan uygulamaların yasal dayanağı bulunmakta mıdır?
Avusturya (RTR)	Bulunmamaktadır.	Bulunmamaktadır.	Bulunmamaktadır.
Birleşik Krallık (OFCOM)	-	-	-
Çek Cumhuriyeti (CTU)	-	-	-
Fransa (ARCEP)	-	-	-
İrlanda (ComReg)	-	-	ComReg'in yetki alanı dışında olup, bilgi bulunmamaktadır.
Kıbrıs (OCECPR)	-	-	-
Lihtenştayn (AK)	Elektronik kimlik, turizm, bilgi alanlarında (belediyede ve konut sakinleri kullanmaktadır).	-	Evet, elektronik kimlik.
Norveç (NKOM)	-	-	-
Portekiz (ANACOM)	-	-	-
Slovakya (RU)	Birçok alanda kullanılmaktadır.	Hayır.	Hayır.
Slovenya (AKOS)	-	-	-

SORU / ÜLKE (Düzenleyici Kurum)	2. Ülkenizde mobil bulut bilişim ile ilgili yürürlükte olan herhangi bir düzenleme bulunmakta mıdır?	Eğer evetse, 2.1 Referans olarak hangi teknik standartları, yönetmelikleri veya mevzuatı alıyorsunuz?	Eğer hayırsa, 2.2 Bu konuda herhangi bir çalışmanız var mı?
Avusturya (RTR)	Bulunmamaktadır.	Bulunmamaktadır.	-
Birleşik Krallık (OFCOM)	-	-	Özellikle mobil bulut bilişime yönelik herhangi bir düzenlememiz bulunmamaktadır.
Çek Cumhuriyeti (CTU)	-	-	-
Fransa (ARCEP)	-	-	-
İrlanda (ComReg)	-	-	Bilgi bulunmamaktadır.
Kıbrıs (OCECPR)	-	-	-
Lihtenştayn (AK)	Siber Güvenlik Kanunu: Bu yasa, ağ ve bilgi sistemlerinin yüksek düzeyde güvenliğinin sağlanması amacıyla alınacak önlemleri belirlemektedir. *https://www.gesetze.li/konso/2023269000* Elektronik kimlik: E-Devlet Yasasıdır. Bu kanun, kamu makamları arasında ve kamu kurumları ile bireyler arasında elektronik ticari işlemleri düzenlemektedir. *https://www.gesetze.li/konso/2011575000*	a) Birlik genelinde ağ ve bilgi sistemlerinin yüksek düzeyde ortak güvenliğine yönelik tedbirlere ilişkin (AB) 2016/1148 sayılı Direktif; b) Avrupa Siber Güvenlik Sanayi, Teknoloji ve Araştırma Yetkinlik Merkezi ve Ulusal Koordinasyon Merkezleri Ağını kuran (AB) 2021/887 sayılı Tüzük, c)ISO/IEC 27002:2022; ISO/IEC 27017:2020; BSI C5 2020	-
Norveç (NKOM)	-	-	-
Portekiz (ANACOM)	-	-	-
Slovakya (RU)	Birçok alanda kullanılmaktadır.	Hayır.	Hayır.
Slovenya (AKOS)	-	-	-

SORU / ÜLKE (Düzenleyici Kurum)		**Eğer evetse,** **3.1 Referans aldığınız teknik konu/standart nedir? Bu kapsamda siber güvenlik çalışmalarınız nelerdir?**
Avusturya (RTR)	Bulunmamaktadır.	-
Birleşik Krallık (OFCOM)	Ofcom veri gizliliği ve korunması ile ilgili konularla ilgilenmemektedir. Birleşik Krallık'ta bu konu Bilgi Komiserliği Ofisi'nin (ICO) görev alanı olmakla birlikte, Birleşik Krallık Genel Veri Koruma Yönetmeliği (UK GDPR) ve 2018 Veri Koruma Yasası'nı (DPA) tanıtılması ve uygulanmasından sorumludur.	-
Çek Cumhuriyeti (CTU)	-	-
Fransa (ARCEP)	-	-
İrlanda (ComReg)		Bilgi bulunmamaktadır.
Kıbrıs (OCECPR)	-	-
Lihtenştayn (AK)	Veri koruması ve veri egemenliği her zaman sağlanmalıdır. Veriler ne kadar kritik veya hassas olursa, koruma gereksinimleri de o kadar yüksek olmaktadır. Veri koruma ve veri egemenliği gerekliliklerine sürekli uyum sağlamak için Bulut Bilişime ilişkin Kılavuzlar kullanılmaktadır.	Kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımına ilişkin 27 Nisan 2016 tarihli ve 2016/679 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (AB), kişisel verilerin suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai yaptırımların infazı amacıyla yetkili makamlar tarafından işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin 27 Nisan 2016 tarihli ve 2016/680 sayılı Avrupa Parlamentosu ve Konsey Direktifi ISO/IEC 27002:2022; ISO/IEC 27017:2020; BSI C5 2020.
Norveç (NKOM)	-	-
Portekiz (ANACOM)	-	-
Slovakya (RU)	-	Bilgi bulunmamaktadır.
Slovenya (AKOS)		

SORU / ÜLKE (Düzenleyici Kurum)	4. İlgili herhangi bir ek bilgi, belge veya web sayfası varsa paylaşabilir misiniz?
Avusturya (RTR)	-
Birleşik Krallık (OFCOM)	Ofcom, bulut hizmetleri pazar çalışmasını Ekim 2023'te tamamlanmış, ancak bu çalışma özellikle mobil bulut bilişimi ele alınmamıştır. Bu kapsamda BTK, Rekabet ve Piyasa Kurumu'nun (CMA) bulut oyunlarını kapsayan mobil ekosistemler pazar araştırması nihai raporuna (Haziran 2022) bakmasının uygun olduğu değerlendirilmektedir. Kısa bir süre önce Temyiz Mahkemesi, mobil tarayıcılar ve bulut oyunları pazarına ilişkin bir CMA pazar araştırmasına yönelik referansı yasal olarak kabul etmiştir. Soruşturma 24 Ocak 2023 tarihinde yeniden başlayacaktır.
Çek Cumhuriyeti (CTU)	-
Fransa (ARCEP)	-
İrlanda (ComReg)	-
Kıbrıs (OCECPR)	-
Lihtenştayn (AK)	-
Norveç (NKOM)	-
Portekiz (ANACOM)	-
Slovakya (RU)	-
Slovenya (AKOS)	-

Ek-3) Elektronik Haberleşme Sektöründe Mobil Bulut Bilişimin Kullanımına Yönelik Gerçekleştirilen Görüşmeler Sırasında İşletmecilere Yöneltilen Sorular

1) Kurum içi kullandığınız veya müşterilerinize yönelik sunduğunuz mobil bulut bilişim ya da bulut bilişim hizmeti/uygulaması bulunmakta mıdır?
Varsa;

- Örnekleriniz nelerdir?

2) Mobil bulut bilişim/bulut bilişim kapsamında kişisel verilerin korunmasına ilişkin tabi olduğunuz herhangi bir yasa/mevzuat/yönetmelik bulunmakta mıdır, varsa açıklayınız.

3) Mobil bulut bilişim/bulut bilişim çerçevesinde yapmış olduğunuz uluslararası iş birliğiniz bulunmakta mıdır?
Varsa;

- İş birlikleri kapsamında yapmış olduğunuz faaliyetler nelerdir?
- Bu iş birliklerinde uymak ile mükellef olduğunuz bir standart bulunmakta mıdır?

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Esra DURUOĞLU

ÖZGEÇMİŞ

1994 yılında Ankara'da doğdu. İlk, orta ve lise öğrenimini Ankara'da tamamladı. 2017 yılında Gazi Üniversitesi Endüstri Mühendisliği Bölümü'nden mezun oldu. 2020 yılının Eylül ayında Bilgi Teknolojileri ve İletişim Kurumu Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı'nda Bilişim Uzman Yardımcısı olarak çalışmaya başladı. 2023 yılı Ekim ayından itibaren Gazi Üniversitesi Bilişim Sistemleri Bölümü'nde Yüksek Lisans eğitimine devam etmektedir.