



**ULAŐTIRMA, DENİZCİLİK VE HABERLEŐME
BAKANLIĐI**

**ULUSAL VERİ MERKEZİ VE BİLİŐİM
ALT YAPISI: DÜNYA UYGULAMALARI
VE TÜRKİYE İÇİN ÖNERİLER**

Günseli AYTAÇ CANKURTARAN

Ulaőtırma ve Haberleőtme UzmanlıĐı Tezi

2014

Ankara



**ULAŐTIRMA, DENİZCİLİK VE HABERLEŐME
BAKANLIĐI**

**ULUSAL VERİ MERKEZİ VE BİLİŐİM
ALT YAPISI: DÜNYA UYGULAMALARI
VE TÜRKİYE İÇİN ÖNERİLER**

Günseli AYTAÇ CANKURTARAN

Ulaőtırma ve Haberleőtme UzmanlıĐı Tezi

2014

Ankara

KABUL VE ONAY

Günseli AYTAÇ CANKURTARAN tarafından hazırlanan Ulusal Veri Merkezi ve Bilişim Alt Yapısı: Dünya Uygulamaları ve Türkiye için Öneriler adlı bu tezin Ulaştırma ve Haberleşme Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Bülent ALTUNKAYNAK
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Ulaştırma ve Haberleşme Uzmanlığı Tezi olarak kabul edilmiştir.

Başkan: _____

Üye : _____

Üye : _____

Üye : _____

Üye : _____

Bu tez, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tez yazım kurallarına uygundur.

ÖZET

ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI	
Tezin Adı	Ulusal Veri Merkezi ve Bilişim Alt Yapısı: Dünya Uygulamaları ve Türkiye için Öneriler
Türü	Uzmanlık Tezi
Yazar	Günseli AYTAÇ CANKURTARAN
Teslim Tarihi	2014
Anahtar Kelimeler	Kamu Entegre Veri Merkezi, Ulusal Veri Merkezi, Yeşil Veri Merkezi, Bulut bilişim, Sanallaştırma
Tez Danışmanı	Doç. Dr. Bülent ALTUNKAYNAK
Sayfa Adedi	xvi+165
<p>Son yıllarda günlük yaşantımızın hemen her boyutunda karşımıza çıkan yoğun bilgi teknolojisinin kullanımıyla birlikte veri hacmi her geçen gün artmaktadır. Verinin korunması, saklanması ve hızlı bir şekilde iletilmesi önem arz etmektedir. Kurumlarda bilgi teknolojilerinin hızlı bir şekilde gelişmesi, veri merkezlerinin de bu hızla büyümesini gerektirmektedir. Güvenliği yeterince sağlanmış, merkezi olarak kurulacak sistemsel bir yapıyla birlikte kamusal alanda bilgi teknolojileri yatırımları daha efektif ve kontrol edilebilir olacaktır.</p> <p>Bu çalışmada, veri merkezlerinin özellikleri, hizmetleri ve bulut bilişim yapısı Türkiye ve Dünya örnekleriyle incelenmiştir. Ülkemizdeki mevcut ve hedeflenen kamu bilişim yapısı incelenerek, ortak veri merkezinin planlanmasındaki önemli hususlar açıklanmıştır. Sonuç olarak, Kamu Entegre Veri Merkezi'ne geçiş süreci, mevcut durum ve çözüm önerileri ile bu konuda yeni bir bakış açısı oluşturulmaya çalışılmıştır.</p>	

ABSTRACT

MINISTRY OF TRANSPORT, MARITIME AFFAIRS AND COMMUNICATIONS	
Thesis	National Data Center And Information Infrastructure: The World Practises and Recommendations for Turkey
Type	Expert Thesis
Author	Günseli AYTAÇ CANKURTARAN
SubmissionDate	2014
Keywords	Public Integrated Data Center, National Data Center, Green Data Center, Cloud Computing, Virtualization
Advisor	Associate Professor Doctor Bülent ALTUNKAYNAK
Total Page	xvi+165
<p>In recent years, each passing day data volume is increasing with the use of intense information technology in almost every size we encounter in our daily life. Protection, storage and quick transmission of data is becoming more of an issue. Rapid development of information technology in institutions requires the some rapid growth of data centers. If ensured with enough security, a centrally systematic structured information technology investments in public domain will be more effective and controllable.</p> <p>In this thesis, the structure of data center facilities, their services and cloud computing were examined with examples of Turkey and the world. Important issues in the planning of the data center partners are described by examining the structure of existing and targeted public information in our country. As a result, a new perspective to the transition process of Public Integrated Data Center has been tried to formed with current situation and solution suggestions.</p>	

TEŐEKKÜR

Çalıőmam boyunca deęerli yardım ve katkılarıyla beni yönlendiren danıőmanım Doç. Dr. Bülent ALTUNKAYNAK'a, bu süreçte hep yanımda olup beni destekleyen sevgili eőim Őemsettin CANKURTARAN'a, tez verilerimin toplanmasında büyük emekleri olan ve tez yazma sürecinde desteklerini eksik etmeyen mesai arkadaşlarıma ve beni yetiőtiren ve bugünlere gelmemi saęlayan annem Hatice AYTAÇ'a teőekkürü bir borç bilirim.

İÇİNDEKİLER

ÖZET.....	i
ABSTRACT.....	ii
TEŞEKKÜR.....	iii
İÇİNDEKİLER	iv
TABLOLAR LİSTESİ.....	x
ŞEKİLLER LİSTESİ	xi
KISALTMALAR LİSTESİ.....	xiii
GİRİŞ	1
1.1. Veri Merkezi Nedir?.....	4
1.2. Veri Merkezinin Tarihçesi.....	4
1.3. Veri Merkezi Neden Gereklidir?	6
1.4. Veri Merkezi Tasarım Standartları	7
1.4.1. ANSI-TIA-942	9
1.4.1.1. Tier I: Temel Veri Merkezi Altyapısı	9
1.4.1.2. Tier II : Bina Altyapısı Yedek Kapasite Bileşenleri.....	10
1.4.1.3. Tier III: Bina Altyapısının Eş Zamanlı Bakımı	12
1.4.1.4. Tier IV: Bina Altyapısı Hata Toleransı.....	13
1.4.2. CENELEC EN 50173-5	16
1.4.3. ANSI/TIA-606-A-1	16
1.4.4. ASHRAE TC9.9.....	16
1.4.5. ISO/IEC 24764.....	17
1.4.6. ANSI/BICSI-002.....	17
1.4.7. ISO 27001	18
1.4.8. ISO 9001	19

1.4.9.	ISO 20000-1	20
1.4.10.	SSAE16.....	20
1.4.11.	SOC 1, SOC 2 ve SOC 3.....	21
1.5.	Veri Merkezi Türleri	22
1.5.1.	Şirket Veri Merkezi.....	22
1.5.2.	İnternet Veri Merkezi.....	22
1.5.2.1.	Barındırma (Hosting) Hizmeti.....	23
1.5.2.2.	Yer paylaşımı (Co-location)	23
1.6.	Veri Merkezinde Olması Gereken Özellikler.....	23
1.6.1.	Güvenlik Politikaları	23
1.6.2.	Veri Yönetimi.....	25
1.6.3.	Erişim Kontrolü.....	25
1.6.4.	Sistem Geliştirme ve Bakımı	26
1.6.5.	İş Sürekliliği ve Felaket Kurtarma	26
2.1.	Türkiye’de Veri Merkezleri.....	28
2.1.1.	Türk Telekom Veri Merkezi	31
2.1.2.	Superonline Veri Merkezi	34
2.2.	Dünya Uygulamaları	42
2.2.1.	Güney Kore Veri Merkezi ve Bulut Bilişim Yapısı.....	44
2.2.1.1.	Güney Kore KEVM’nin Tanımı	44
2.2.1.1.1.	Amaç.....	44
2.2.1.1.2.	Tarihçe	48
2.2.1.1.3.	KEVM Tanım	49
2.2.1.1.4.	Önemli Özellikler	51
2.2.1.2.	Güney Kore Veri Merkezi’nde Verilen Önemli Hizmetler	52
2.2.1.2.1.	E-Devlet Sistemlerinin Entegre Yönetimi	52

2.2.1.2.2.	E-Devlet Sistemlerinin Entegre Güvenlik Yönetimi	54
2.2.1.2.3.	Entegre Bilgi Teknolojileri Kaynakları Yönetimi	56
2.2.1.2.4.	Özel Kamu İletişim Ağı	58
2.2.1.2.5.	Veri Merkezi Yönetimi için En Uygun Ortam	59
2.2.1.2.6.	İş Sürekliliği Garanti Hizmeti	61
2.2.1.2.7.	Kamu Platformu Paylaşım Hizmeti	62
2.2.1.3.	Sistemin Başarısı	65
2.2.1.3.1.	Önemli Başarılar	65
2.2.1.3.2.	Uluslararası Toplumlardaki Etkisi	71
2.2.1.3.3.	Küresel Birliktelik	73
2.2.2.	İngiltere Veri Merkezi ve Bulut Bilişim Yapısı	73
2.2.3.	ABD Veri Merkezi ve Bulut Bilişim Yapısı	75
2.2.4.	Japonya Veri Merkezi ve Bulut Bilişim Yapısı	79
2.2.5.	Google Veri Merkezi	81
2.2.6.	Facebook Veri Merkezi	89
2.3.	Yeşil Veri Merkezleri	91
2.3.1.	Veri Merkezlerinin Enerji Tasarrufu	92
2.3.2.	Veri Merkezi Kullanımı	93
2.3.3.	Veri Merkezi Tasarımı	93
2.3.4.	Enerji Tasarrufu Sağlayan Cihazların Kullanımı	94
2.3.5.	Japonya Yeşil Veri Merkezi Uygulamaları	96
2.3.6.	İngiltere Yeşil Veri Merkezi Uygulamaları	97
3.1.	Sanallaştırma Nedir?	99
3.2.	Sanallaştırma Çeşitleri	100
3.2.1.	Sistem Sanal Makineleri	100
3.2.2.	Proses Sanal Makinesi	100

3.3.	Sanallaştırmanın Avantajları	101
3.4.	Sanallaştırma Yazılım Çeşitleri	102
3.4.1.	Açık Kaynak Kodlu Sanal Makina Yazılımları	102
3.4.2.	Ticari Sanal Makina Yazılımları	102
3.5.	Sanallaştırma Çözümlerine Geçen Kurumlar	102
4.1.	Bulut Bilişim Nedir?	105
4.2.	Bulut Bilişim'in Tarihi	108
4.3.	Bulut Bilişim'in Avantaj ve Dezavantajları	110
4.4.	Bulut Bilişim Hizmet Modelleri	112
4.4.1.	Alt Yapı Hizmetleri (IaaS)	112
4.4.2.	Platform Hizmeti (PaaS)	113
4.4.3.	Yazılım Hizmeti (SaaS)	114
4.4.4.	Bazı Bulut Depolama Hizmetleri	114
4.5.	Bulut Bilişim Yerleştirme Modelleri	114
4.5.1.	Genel Bulut	115
4.5.2.	Topluluk Bulutu	115
4.5.3.	Hibrit (Karma) Bulut	115
4.5.4.	Özel Bulut	116
4.6.	Bulut Bilişim Mimarisi	116
4.7.	Bulut Bilişimin Güvenliği	117
5.1.	Kamu Entegre Veri Merkezi için Bilişim Yapısı	119
5.1.1.	Mevcut Kamu Bilişim Yapısı	119
5.1.2.	Hedeflenen Kamu Bilişim Yapısı	128
5.2.	Ortak Veri Merkezi Stratejisi	129
5.3.	Ortak Veri Merkezleri'nin Avantajları, Dezavantajları ve Riskleri	130
5.3.1.	Ortak Veri Merkezleri'nin Avantajları	130

5.3.2.	Ortak Veri Merkezileri'nin Dezavantajları	133
5.3.3.	Ortak Veri Merkezileri'nin Riskleri.....	133
5.3.4.	Ortak Veri Merkezi Planlaması.....	134
6.1.	Veri Merkezi Mimarisi	135
6.2.	Veri Merkezi Fiziksel Ağ Yapısı.....	136
6.3.	Veri Merkezi Güvenliği.....	136
6.3.1.	Fiziksel Güvenlik	136
6.3.2.	Yazılımsal Güvenlik.....	137
6.4.	Veri Merkezi Loglama	137
6.5.	Veri Merkezi Enerji Kullanımı.....	137
6.5.1.	Sera Gazı Etkisi.....	138
6.5.2.	Enerji Verimliliği	138
6.6.	Soğutma Sistemleri.....	138
7.1.	Analiz	140
7.1.1.	İhtiyaç Analizi.....	140
7.1.1.1.	Fiziksel Mekan İhtiyacı	140
7.1.1.2.	Donanımsal İhtiyaçlar.....	141
7.1.1.3.	Yazılımsal İhtiyaçlar.....	141
7.1.1.4.	Kalifiye İnsan Gücü İhtiyacı.....	142
7.1.2.	SWOT Analizi.....	142
7.1.2.1.	Tespit	143
7.1.2.2.	Analiz.....	144
7.1.3.	Alt Yapı Analizi	145
7.1.4.	Risk Analizi ve Yönetimi.....	145
7.1.5.	Maliyet Analizi.....	149
7.2.	Hazırlık.....	151

7.2.1. Fiziksel Alt Yapı Hazırlığı.....	151
7.2.2. Donanım ve Yazılım Tedariki.....	151
7.3. Uygulama	151
SONUÇ ve ÖNERİLER.....	153
KAYNAKLAR	157
ÖZGÜNLÜK BİLDİRİMİ.....	163
ÖZGEÇMİŞ	164

TABLolar LİSTESİ

Tablo 1.1 Tier Sınıflarının Özellikleri	15
Tablo 1.2 Tier Sınıflarına Göre Veri Merkezlerinin Genel Özellikleri	15
Tablo 2.1 Türkiye’de İnternet Veri Merkezleri.....	29
Tablo 2.2 Türkiye Veri Merkezleri Pazar Büyümesi	29
Tablo 2.3 Dünyada BT harcamalarının tahmini (Milyar Dolar)	43
Tablo 2.4 Güney Kore Veri Merkezi’nin Faydaları.....	47
Tablo 3.1 Sosyal Yardımlaşma ve Dayanışma Genel Müdürlüğü Sanallaştırma Öncesi ve Sonrası Genel Durum	103
Tablo 5.1 Aile ve Sosyal Politikalar Bakanlığı Sanallaştırma Öncesi ve Sonrası Genel Durum.....	124
Tablo 7.1 Kamu Entegre Veri Merkezi Swot Analizi.....	143
Tablo 7.2 Tehdit Etki-Olasılık Karar Çizelgesi	149
Tablo 7.3 Tahmini Maliyet Kalemleri	150

ŞEKİLLER LİSTESİ

Şekil 1.1 2014 yılı Gelişen Trendler	7
Şekil 1.2 Veri Merkezi Standartları Çizelgesi.....	8
Şekil 2.1 Türkiye'deki Veri Merkezi Hizmet Sağlayıcıları	30
Şekil 2.2 Türkiye Bulut Pazarı	31
Şekil 2.3 Superonline Veri depolama hizmet paketleri.....	39
Şekil 2.4 Superonline Veri Yedekleme Hizmet Paketleri	40
Şekil 2.5 Superonline Uzaktan Sunucu Yedekleme Hizmetleri.....	41
Şekil 2.6 Dünya'da Veri Merkezi Harcamaları.....	42
Şekil 2.7 Küresel Enerji Tüketimi ile Veri Merkezi Enerji Tüketimi.....	43
Şekil 2.8 Dünyada Bulut Pazarı	44
Şekil 2.9 Güney Kore KEVM Amaç ve Stratejiler Kavram Haritası	46
Şekil 2.10 Güney Kore Kamu Entegre Veri Merkezi	50
Şekil 2.11 Entegre Yönetim Hizmeti Kavram Haritası.....	53
Şekil 2.12 Entegre Güvenlik Yönetim Sistemi Kavram Haritası.....	56
Şekil 2.13 Entegre BT Kaynakları Yönetim Kavram Haritası.....	57
Şekil 2.14 Kamu Bilgi ve İletişim Ağı Kavram Haritası	59
Şekil 2.15 Veri Merkezi Alt Yapı Yönetimi Kavram Haritası.....	60
Şekil 2.16 İş Sürekliliği Garanti Hizmeti Kavram Haritası	62
Şekil 2.17 Kamu Platformu Paylaşım Hizmeti	64
Şekil 2.18 Güney Kore KEVM Kazanımları	65
Şekil 2.19 TCO/ROI Analizi.....	66
Şekil 2.20 Alanlara Göre ROI.....	66
Şekil 2.21 Cihazlardaki Aylık Ortalama Kesinti	67
Şekil 2.22 Kullanıcı Kurum Memnuniyet Düzeyi	67
Şekil 2.23 Otomatik Engelleme İçin Kural Setlerinin Artırılması.....	68
Şekil 2.24 Felaket Kurtarma Sistemi Kurulum Oranı	69
Şekil 2.25 Satın Alma ve İşlem Giderlerinde Tasarruf	70
Şekil 2.26 PUE İndeksinde Değişim	70
Şekil 2.27 ABD ve IBM Veri Merkezi Konsolidasyonu	78
Şekil 2.28 Google Berkeley County Veri Merkezi	81

Şekil 2.29 Google Council Bluffs Veri Merkezi.....	82
Şekil 2.30 Google Veri Merkezi	83
Şekil 2.31 Veri Merkezleri PUE değeri ortalaması.....	84
Şekil 2.32 Küresel Elektrik Tüketiminde Veri Merkezleri'nin Yeri.....	86
Şekil 2.33 Veri Merkezleri Elektrik Tüketiminde Google'ın Yeri	87
Şekil 2.34 Google'ın Yenilenebilir Enerji Kullanımı (%) (2012).....	88
Şekil 2.35 Facebook Aktif Kullanıcı Sayısı (2008-2014) (Milyon)	89
Şekil 2.36 BİT Tarafından Yayılan CO2 (Tahmini).....	92
Şekil 2.37 Veri Merkezi İşletmecileri, ASP/SaaS İşletmecileri ve Kullanıcılar Arasındaki İlişki	93
Şekil 2.38 Veri Merkezinde Enerji Tüketiminin Dağılımı.....	95
Şekil 3.1 Genel Sanallaştırma Mimarisi.....	101
Şekil 4.1 Bulut Bilişimin Gelişimi	110
Şekil 4.2 Bulut Bilişim'in Riskleri ve Faydaları.....	112
Şekil 5.1 Mevcut Kamu Bilişim Yapısı	119
Şekil 5.2 Tam Donanımlı Veri Merkezi Bulunan Kamu Kurumları.....	120
Şekil 5.3 Felaket Kurtarma Merkezi Bulunan Kamu Kurumları	121
Şekil 5.4 Kamuda Bulut Servislerinin Kullanımı	122
Şekil 5.5 BT Altyapılarında Sanallaştırma Kullanım Oranı	122
Şekil 5.6 Kurumlarda İnternet Türü Dağılımı.....	125
Şekil 5.7 Kurumlarda İnternet Hızı Dağılımı.....	126
Şekil 5.8 Kurumlarda Sanallaştırma Kullanımına İlişkin Mevcut Durum.....	127
Şekil 5.9 Kurumlarda Kullanılan Sanallaştırma Türleri	128
Şekil 5.10 Hedeflenen Kamu Bilişim Yapısı	129
Şekil 5.11 Kamu Entegre Veri Merkezi'nin Avantajları	131
Şekil 5.12 ITIL Hizmet Stratejileri	132
Şekil 6.1 Bilişim Teknolojilerini Hizmet Olarak Sunan Platform	135
Şekil 7.1 Risk Yönetimi	146
Şekil 7.2 Risk Değerlendirme Yöntem Bileşenleri	147

KISALTMALAR LİSTESİ

ABD	Amerika Birleşik Devletleri
ACL	Erişim Kontrol Listeleri (Access Control List)
AICPA	Amerika Yeminli Serbest Mali Müşavirler Enstitüsü (American Institute of Certified Public Accountants)
AKS	Adres Kayıt Sistemi
ANSI	Amerika Ulusal Standartlar Enstitüsü (American National Standards Institute)
API	Uygulama Programlama Arayüzü (Application Programming Interface)
ASHRAE	Amerikan Isıtma Soğutma ve İklimlendirme Mühendisleri Derneği (American Society of Heating, Refrigerating and Air Conditioning Engineers)
ASP	Uygulama Hizmeti Sağlayıcısı (Application Service Provider)
ATS	Otomatik Transfer Anahtarı (Automatic Transfer Switch)
BCP	İş Sürekliliği Planı (Business Continuity Planning)
BDDK	Bankacılık Düzenleme ve Denetleme Kurulu
BİT	Bilgi ve İletişim Teknolojileri
BM	Birleşmiş Milletler
BT	Bilgi Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu

BTSEP	Bilgi Teknolojileri Strateji Eylem Planı
BTYK	Bilim ve Teknoloji Yüksek Kurulu
BTU	İngiliz Isı Birimi (British Thermal Unit)
BPR	İş Sürecinin Yeniden Yapılanması (Business Process Reengineering)
CERT	Bilgisayar Acil Müdahale Ekibi (Computer Emergency Response Teams)
CCTV	Kapalı Devre Televizyon (Closed-Circuit Television)
CMMI	Bütünleşik Yetenek Olgunluk Modeli Entegrasyonu (Capability Maturity Model Integration)
CLR	Ortak Dil Çalışma Zamanı (The Common Language Runtime)
COBIT	Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri (Control Objectives for Information and Related Technology)
CPU	Merkezi İşlem Birimi (Central Processing Unit)
DB	Veri Tabanı (Database)
DDoS	Dağıtılmış Hizmet Aksatma Saldırıları (Distributed Denial Of Service Attack)
DRS	Felaket Kurtarma Sistemi (Disaster Recovery System)
e-ANSI	Elektronik Gelişmiş Milli Güvenlik Altyapısı (Electronic Advanced National Security Infrastructure)
GISMS	Kamu Bilgi Güvenliği Yönetim Sistemi (Government Information Security Management System)

GSA	ABD Genel Hizmetler Dairesi (General Service Administration)
HIPAA	Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (Health Insurance Portability and Accountability Act)
IaaS	Alt Yapı Hizmetleri (Infrastructure As A Service)
IBM	Uluslararası İş Makineleri (International Business Machines)
IDC	Uluslararası Veri Kurumu (International Data Corporation)
IPS	Saldırı Tespit Sistemleri (Intrusion Prevention Systems)
IPTV	İnternet Protokol Televizyon (Internet Protocol television)
IPv6	İnternet Protokol Sürüm 6 (Internet Protocol Version 6)
ISE	Anında Güvenli Silme (Instant Secure Erase)
ISP	Bilgi Stratejisi Planı (Information Strategy Plan)
ITIL	BT Altyapı Kütüphanesi (Information Technology Infrastructure Library)
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)
JVM	Java Sanal Makine (Java Virtual Machine)
KEVM	Kamu Entegre Veri Merkezi
LAN	Yerel Alan Ağı (Local Architecture Network)
MERNİS	Merkezi Nüfus İşleri Sistemi
MERSİS	Merkezi Sicil Kayıt Sistemi
MIC	Japonya İçişleri ve İletişim Bakanlığı (Ministry of Information and Communication)

NCIA	Ulusal Bilişim ve Bilgi Ajansı (National Computing Information Agency)
NIST	ABD Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)
nTops	Ulusal Yönetim Platformu Sistemi (National Total Operation Platform System)
PaaS	Platform Hizmeti (Platform As A Service)
PCD	Güç Soğutma Yoğunluğu (Power Cooling Density)
PCI	Çevre Birimleri Bağlantı Kartı (Peripheral Component Interconnect)
PDU	Protokol Veri Birimi (Protocol Data Unit)
PKI	Kamu Anahtar Altyapısı (Public Key Infrastructure)
PMI	Proje Yönetimi Enstitüsü (Project Management Institute)
PUE	Güç Kullanımı Etkinliği İndeksi (Power Usage Effectiveness)
RAM	Rastgele Erişim Belleği (Random Access Memory)
ROI	Yatırımın Getirisi (Return On Investment)
SaaS	Yazılım Hizmeti Sunucusu (Software As A Service)
SGK	Sosyal Güvenlik Kurumu
SLA	Hizmet Seviyesi Antlaşması (Service-Level Agreement)
SPICE	Yazılım Süreçlerinin İyileştirilmesi ve Yetenek Düzeyinin Belirlenmesi (Software Process Improvement and Capability Determination)
SSL	Güvenli Giriş Katmanı (Secure Socket Layer)

STS	Statik Transfer Anahtarı (Statik Transfer Switch)
SYDGM	Sosyal Yardımlaşma ve Dayanışma Genel Müdürlüğü
TAKBİS	Tapu ve Kadastro Bilgi Sistemi
TCDD	Türkiye Cumhuriyeti Devlet Demiryolları
TCO	Toplam Sahip Olma Maliyeti (Total Cost Of Ownership)
TIA	Telekomünikasyon Endüstrisi Birliği (Telecommunications Industry Association)
TSE	Türk Standartları Enstitüsü
TÜRKSAT	Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş.
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UBcN	Ultra Genişbant Yakınsama Ağı (Ultra Broadband Convergence Network)
UDHB	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
UPS	Kesintisiz Güç Kaynağı (Uninterruptible Power Supply)
UYAP	Ulusal Yargı Ağı Projesi
wLans	Sanal Yerel Alan Ağları (Wireless Local Area Network)
VDI	Sanal Masaüstü Altyapısı (Virtual Desktop Infrastructure)
VoIP	IP Üzerinden Ses Gönderimi (Voice Over Internet Protocol)
VPN	Sanal Özel Ağlar (Virtual Private Network)

GİRİŞ

Bilgi ve iletişim teknolojilerinin gelişip yaygınlaşması ve kullanımının artmasına paralel olarak elektronik ortamlarda üretilen, saklanan ve paylaşılan veriler her geçen gün hızla artmaktadır. Verinin kalıcı bir hale gelebilmesi için saklanması ve analiz edilmesi gerekmektedir.

İnternet' in hızla yaygınlaşması, özel ve kamu hizmet sektörlerini, internet üzerinden verdikleri hizmetleri artırmaya, çeşitlendirmeye, daha güvenli ve sürekli hizmet vermeye zorlamaktadır. Bu hizmetlerin daha etkin ve daha güvenli bir şekilde yapılabilmesi için bilgi teknolojileri alanında; birleştirme, dış kaynak kullanımı ve paylaşma yöntemlerinin sonucu olarak “veri merkezleri” kurumlar için vazgeçilmez bir ihtiyaç olarak ortaya çıkmıştır.

Günümüzde kurumlar çok hızlı bilgi teknolojisi büyümesi yaşarken, veri merkezlerinin de bu hızla büyümesi gerekmektedir.

E-Devlet kapsamında oluşacak verilerin saklanması, bilgi haline getirilmesi ve analizlerine olanak tanınması için ortak veri merkezlerin kurulması gerekmektedir. Bu yapılanma ile kurumlara özgü ayrık veri merkezlerindeki verilerin derlenmesi ve analiz edilmesi güçlüğüünün yanında, benzer sistemlerin farklı yerlerde kurulmasının da önüne geçilecektir. Bu nedenle; idari ihtiyaçlar, tasarruf imkânı ve siber güvenlik gereksinimleri doğrultusunda, halen her kurumda müstakil olarak işletilmekte olan veri merkezlerinin tek bir çatı altında birleştirilerek Türkiye Kamu Entegre Veri Merkezi'nin kurulması önem arz etmektedir.

15 Ocak 2013'te gerçekleştirilen Bilim ve Teknoloji Yüksek Kurulu'nun (BTYK), 25. toplantısında almış olduğu 2013/104 nolu kararda, Kamu kurumlarının veri merkezlerinin birleştirilmesine yönelik hukuki, teknik ve idari yapılanma modelinin oluşturulmasına ve Türkiye Kamu Entegre Veri Merkezi'nin kurulması çalışmalarının yapılmasına karar verilmiştir.

Söz konusu kararda, kamu kurumları arasında veri paylaşımının artırılması, siber tehditlere karşı daha güçlü bir yapılanmanın sağlanması için “Ulusal Veri Merkezi” çalışmalarında, sorumlu kuruluş olarak Ulaştırma, Denizcilik ve Haberleşme Bakanlığı belirlenirken, ilgili kuruluşlar olarak Başbakanlık, Kalkınma Bakanlığı, TÜRKSAT ve TÜBİTAK belirlenmiştir.

Bu çalışma, Kamu Entegre Veri Merkezi'nin kurulması konusunda dünya ülkelerinin, şirketlerin ve Türkiye'de bulunan veri merkezlerinin özellikleri, hizmetleri ve kapsamı incelenerek Türkiye için önerilerde bulunulması açısından önemlidir. Çalışma kapsamında, veri merkezi kavramı, önemi, standartları, özellikleri, hizmetleri, sanallaştırma, bulut bilişim, yapısı incelenerek, kamu veri merkezine geçiş süreci analiz, hazırlık ve uygulama adımları ile projelendirilmiştir. Veri merkezi, bulut bilişim yapısı ve yeşil veri merkezleri kavramı, Türkiye ve Dünya örnekleriyle açıklanmıştır.

Çalışmanın yöntemi olarak, ilk aşamada tez, makale ve rapor gibi bilimsel kaynakların yanında internet siteleri ve veri tabanlarından da yararlanılarak literatür taraması yapıldıktan sonra ülkemizde yapılan çalışmalar, mevcut durum, dünya ülkeleri veri merkezleri yapısı incelenmiştir. Sonraki aşamada, veri merkezi standartları ve dünya örnekleri baz alınarak Türkiye Kamu Entegre Veri Merkezi'nin kurulması için önerilerde bulunulmuştur.

Tezin birinci bölümünde; veri merkezlerinin tanımı ve tarihçesi, veri merkezinin gerekliliği, veri merkezleri türleri ve hizmetleri anlatılmıştır. Veri merkezlerinde olması gereken uluslararası standartlar hakkında bilgi verilmiş, veri merkezinde olması gereken özellikler açıklanmıştır.

İkinci bölümde; ülkemizdeki veri merkezleri yapısı ve mevcut durumu incelenerek, Türk Telekom ve Superonline veri merkezleri altyapısı, özellikleri ve hizmetlerinden bahsedilmiştir. Kamu veri merkezleri için dünya uygulamaları incelenmiş olup, Güney Kore Entegre Veri Merkezi, kurulum aşamasından itibaren detaylı bir şekilde açıklanmış, İngiltere, ABD ve Japonya'daki veri merkezleri ve

bulut bilişim yapısı anlatılmıştır. Daha sonra, Yeşil Veri Merkezi'nin tanımı yapılmıştır. Yeşil veri merkezlerinde enerji tasarrufu ve verimliliği konuları irdelenerek, bu konuda Japonya ve İngiltere'de yapılan yeşil veri merkezleri uygulamaları anlatılmıştır.

Üçüncü bölümde; sanallaştırmanın tanımı yapılarak, sanallaştırma çeşitleri, sanallaştırmanın avantajları, sanallaştırma yazılım çeşitleri ve sanallaştırma çözümlerine geçen kurumlar anlatılmıştır.

Dördüncü bölümde; bulut bilişimin tanımı yapılarak, avantajları ve dezavantajları ile hizmet ve yerleştirme modelleri, teknik/donanımsal özellikleri ve güvenliği incelenmiş olup, bulut bilişimde kullanılan yazılım teknolojilerinden bahsedilmiştir.

Beşinci bölümde; mevcut ve hedeflenen kamu bilişim yapısı incelenerek, ortak veri merkezi stratejisi, ortak veri merkezinin avantaj ve dezavantajları, riskleri ve veri merkezi planlanmasında önemli olan hususlar anlatılmıştır.

Altıncı bölümde; Kamu Entegre Veri Merkezi'ne geçiş sürecinde, mimari yapı, fiziksel ağ yapısı, güvenliğin sağlanması, loglama, enerji kullanımı ve soğutma sistemlerinin nasıl olunması gerektiği anlatılmıştır.

Daha sonra, Yedinci bölümde analiz, hazırlık ve uygulama süreci ile Kamu Entegre Veri Merkezi projelendirilerek anlatılmıştır.

Tezin sonuç ve öneriler kısmında; daha önceki bölümlerde anlatılan konulardan yola çıkılarak, Türkiye'de kurulacak olan Kamu Entegre Veri Merkezi için önerilerde bulunmaktadır.

1. VERİ MERKEZİ KAVRAMI

1.1. Veri Merkezi Nedir?

Veri, bir ham (işlenmemiş) gerçek ya da enformasyon parçasığına verilen addır (Sezgin & Akdemir, 2014).

Yalçıntaş (2013, s.71) veri merkezini aşağıda şekilde tanımlamıştır:

Veri merkezleri kamu, özel kurum ve işletmelerin kritik bilgilerinin yönetildiğı, depolama ve yedekleme ünitelerini barındıran, uygulama ve sistem sunucularını, ağ katmanlarını bulunduran fiziksel ortamlardır. Daha genel anlamda veri saklama ve yedekleme, web, elektronik posta, alan adı hizmetleri, donanım, yazılım, yönetim ve denetim hizmetleri, güvenlik, felaket kurtarma hizmeti, danışmanlık, tasarım, sistem entegrasyonu, kurulum hizmetleri veren büyük altyapılardır.

Bilgi sistemlerinin merkezi olan iyi tasarlanmış bir veri merkezi; yeni teknolojilerle gelişen, farklı veri türlerini barındıran, yüksek derecede erişebilirliğı sağlayan ve verilerin tutarlılığı için hosting (ev sahipliğı) hizmetlerini veren tesislerdir (Mohamed & H, 2011).

1.2. Veri Merkezinin Tarihçesi

Veri merkezinin geçmişi bilgisayar endüstrisinin ilk çağlarındaki büyük bilgisayar odalarına dayanmaktadır. Veri Merkezleri gibi ilk bilgisayar sistemlerinin işletimi ve bakımı oldukça zor olmuştur. Bilgisayar sistemlerinin çalışması için özel bir ortamın oluşması gerekmiştir.

İlk bilgisayarlar birçok ekipmanın çok sayıda kablo ile birbirine bağlanması ile oluşmuştur. Çok sayıda ekipmanın birbirine bağlanması, çeşitli prosedür ve yöntemleri mecbur kılmıştır. Örneğin veri merkezlerinde de kullanılan

ekipmanların monte edildiği standart raflar, yükseltilmiş zemin ve kablo tavaları ilk bilgisayar sistemlerinde de kullanılmıştır. Tek bir ana bilgisayarın çok büyük miktarda güce gereksinim duyması ve aşırı ısınmaması için soğutulması gerekmiştir. Oldukça pahalı olan bu bilgisayarlar askeri amaçlı kullanıldığı için güvenliğin çok önemli olması, kritik veri merkezlerinde olduğu gibi, bilgisayar odalarına giriş yapmak için de yetkilendirmeyi gerektirmiştir.

Mikroişlemci endüstrisinin gelişme gösterdiği dönemde, özellikle 1980'li yıllarda, bilgisayarlar her yerde kullanılmaya başlanmış, ama çoğu durumda çalışma gereksinimleri göz ardı edilmiştir. Bununla birlikte bilgi teknolojilerinin işleyiş olarak karmaşa içerisinde gelişmesi ile şirketler bilgi teknolojileri kaynaklarını kontrol edebilmenin gerekliliğini fark etmişlerdir.

İstemci-sunucu modeli ağ mimarisinin gelişimiyle 1990'larda mikroişlemciler (sunucular) eski bilgisayar odalarında yerlerini almaya başlamıştır. Ağ ekipmanlarının ulaşılabilir fiyatlarda olması, ağ yapılandırılmış kabloların yeni standartlarla belirlenmesi, sunucuları iş yerlerinde özel bir odanın içerisine konulması ile hiyerarşik bir düzenin oluşmasını sağlamıştır. Özel olarak tasarlanmış bilgisayar odalarına verilen 'veri merkezi' terimi günümüzde yaygın olarak kullanılmaktadır (Wikipedia, 2014a).

Dot-com balonu döneminde veri merkezleri büyük önem kazanmıştır. Kuruluşlar bilgisayar sistemlerini çalıştırabilmek ve internet ortamında varlıklarını oluşturabilmek için hızlı internet bağlantısına ve aralıksız çalışabilme özelliğine ihtiyaç duymuşlardır. Küçük işletmeler için bu özellikleri sağlayacak ekipmanların kurulması mümkün olmamıştır.

Birçok şirket, internet veri merkezi denen büyük tesisler inşa etmeye başlamış, internet veri merkezleri küçük şirketlere verilerin saklanması, işlenmesi ve sunulması gibi çeşitli çözümler sunmuşlardır (Wikipedia, 2014a).

Yeni teknolojiler ve uygulamalarla bu merkezler yüksek düzeyli güvenliğini sağlandığı, 7 gün 24 saat hizmetin alındığı, ölçeklenebilir ve yönetilebilir sistemler haline gelmişlerdir (Wikipedia, 2014a).

Bulut bilişimin kullanımının artmasıyla birlikte, iş dünyası ve devlet kurumları veri merkezlerine daha ileri derecelerde, örneğin; güvenlik, uygunluk, çevresel etkiler ve standartlara bağlılık gibi konularda dikkatlerini yoğunlaştırmışlardır. Kurumlar açısından bilgi teknolojileri ekipmanlarını bünyesinde tutmak istemesinin temelinde güvenlik konusundaki çekinceleri, kontrolü elinde bulundurma alışkanlığı, bilgiyi başkasının eline vermektan duyulan korku bulunmaktadır.

Güvenlik alanındaki gelişmeler işletmelerin bilişim altyapısı ve uygulamalarını kendi bünyesinde barındırma isteğini azaltmış, bilgi teknolojileri hizmetlerinin dışarıdan alınması hız kazanmıştır.

1.3. Veri Merkezi Neden Gereklidir?

Veri merkezleri; işletmelerin 7 gün 24 saat hizmet almalarına veya iş gereklerine uygun olarak çalışmasına olanak tanıyarak, kritik bilgi işleme kaynaklarının denetimli ortamlarda, merkezi yönetim altında birleştirilmesini sağlar (UBAK, 2005, s.16-17).

Kuruluşların günümüz rekabet koşulları içinde var olabilmeleri için; bilgi teknolojileri altyapılarını müşterilerini, ortaklarını, tedarikçilerini de entegre edecek biçimde zenginleştirmeleri, hizmet verme hızı ve kalitesini iyileştirmeleri, 7 gün 24 saat sistemlerini ayakta ve işler durumda tutmaları gerekmektedir. Bu zorunluluklar sonucunda artan kaynak kullanımının daha iyi yönetilebilmesi için merkezi yönetim olanaklarına gereksinim duyulmaktadır. Kaynak harcamalarının en iyi şekilde değerlendirilmesi için sistem, veri ve erişim olanaklarında birleştirmeye gidilmesi gerekmektedir. Bu yüzden bilgi teknolojileri hizmetlerini kapsayan iş ve hizmetlerde süreklilik, birleştirme ve kaynakların merkezi yönetimi büyük önem taşımaktadır. Bu gerekliliklerin gerçekleşmesini sağlayan veri merkezleri,

iřletmeler için vazgeçilmez bir ihtiyaç olarak ortaya çıkmaktadır (UBAK, 2005, s.16-17).

IDC'nin raporuna göre son dönemde dünyada gelişen 4 trend (Mobil Yaşam, Sosyal Ağlar, Bulut Bilişim ve Büyük Veri) birbirleriyle iç içe gelişme göstermektedir (Şekil 1.1). Bu trendlerin oluştuğu ve muhafaza edildiği yerin veri merkezleri olması, veri merkezlerinin önemi ve gerekliliğini göstermektedir.

Şekil 1.1 2014 yılı Gelişen Trendler



Kaynak: (IDC, 2013)

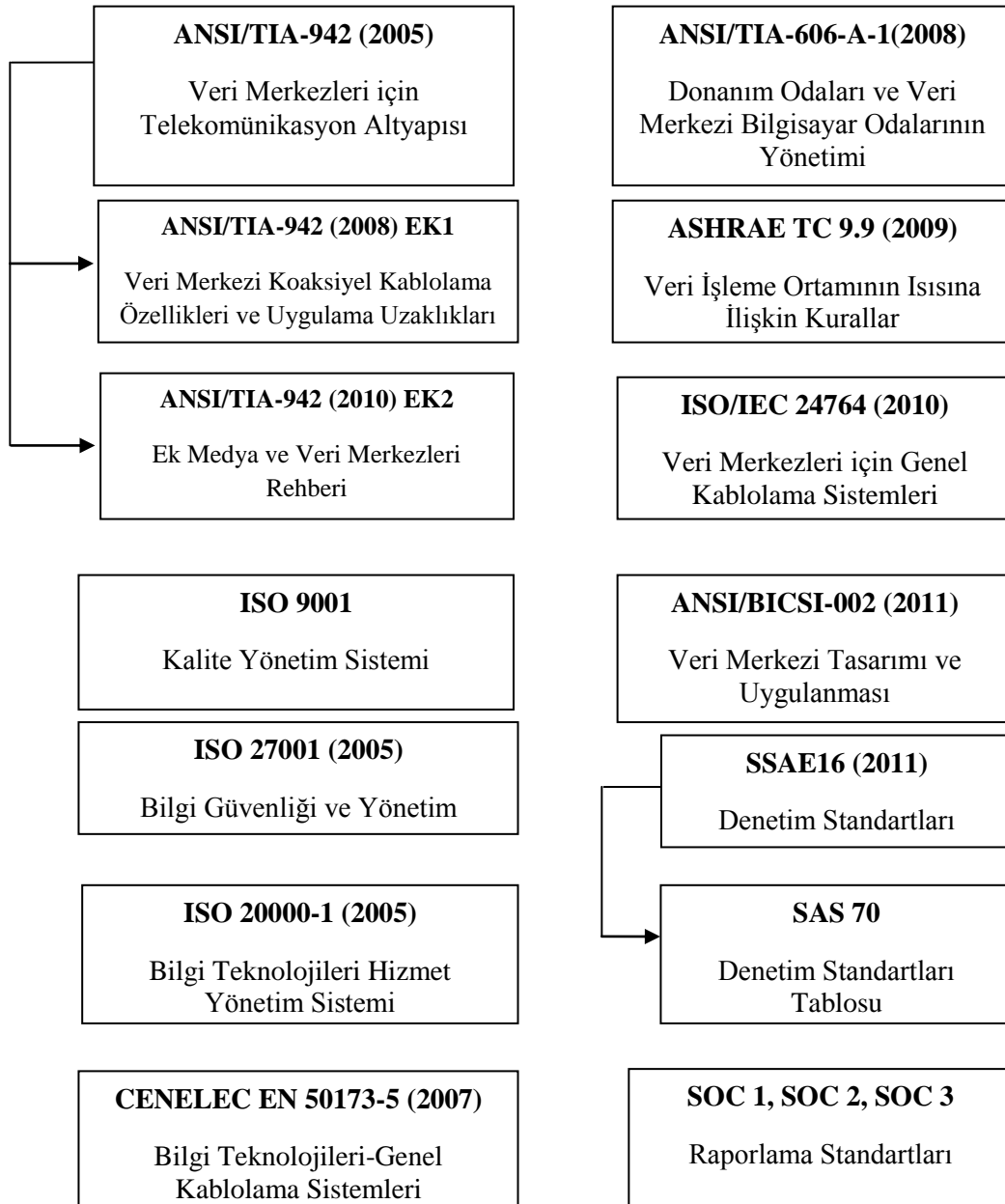
1.4. Veri Merkezi Tasarım Standartları

Veri merkezlerinin sürdürülebilirliği ve çevresel düzenlemelerine ilişkin hususların uygunluğunun sağlanmasına yönelik, mevzuata ilişkin düzenlemeler ve uluslararası kuruluşlar tarafından standartlar oluşturulmuştur.

Kurumlar ve şirketler, veri merkezi stratejileri oluştururken, veri merkezinde uluslararası standartları ne kadar uygulayabildiklerine dikkat etmeleri gerekmektedir.

Bu bölümde veri merkezleri ile ilgili anlatılan standartlara ilişkin Veri Merkezi Standartları Çizelgesi Şekil 1.2'deki gibidir.

Şekil 1.2 Veri Merkezi Standartları Çizelgesi



Kaynak: Kepekci ve diğer kaynaklardan derlenmiştir.

1.4.1. ANSI-TIA-942

ANSI (Amerika Ulusal Standartlar Enstitüsü) tarafından akredite edilmiş bir kuruluş olan Telekomünikasyon Endüstrisi Birliği'nin 2005 yılında yayınladığı "TIA-942 Veri Merkezleri için Telekomünikasyon Altyapısı" standardı, veri merkezi tasarımında kullanılan bir standarttır. Fiber optik, bakır kablolama ve ağ dizaynı konularında görüş bildirmektedir.

Bu standartlar 2008 yılında yayınlanan "Veri Merkezi Koaksiyel Kablolama Özellikleri ve Uygulama Uzaklıkları" ANSI/TIA 942 Ek 1 standardı ile 2010 yılında yayınlanan "Ek Medya ve Veri Merkezleri Rehberi" ANSI/TIA 942 Ek 2 standartları ile güncellenmiştir.

Tier standartları, belirli bir özellikteki veri merkezinin altyapısı, tasarımı, topolojisi, kullanılabilirliği, kapasitesi ve işlevselliğini diğer veri merkezleri ile karşılaştırarak Uptime Enstitüsü'nün objektif bir şekilde oluşturduğu temel standartlardır. Bu standartlar, yedek kapasite bileşenleri ve dağıtım yollarının artan düzeylerine dayanan veri merkezi altyapısını, dört farklı sınıflandırma (Tier I, Tier II, Tier III, Tier IV) ile açıklamaktadır (Uptime Institute, 2009-2012).

Her bir sınıflandırmanın temel özellikleri, sınıflandırmaya uygunluğunun denetimi için yapılması gereken performans doğrulama testleri ve operasyonel etkileri anlatılmıştır.

1.4.1.1. Tier I: Temel Veri Merkezi Altyapısı

Temel Özellikler:

- Tier I sınıfı veri merkezlerinde, yedek kapasite bileşenleri yoktur. Kritik ortamda ise tek dağıtım yolu vardır.
- Tier I altyapısı; BT sistemleri için özel bir alan, kesintisiz güç kaynağında ani voltaj yükselmeleri, sarkmalar, anlık kesintiler için güç kaynağı filtresi,

özel soğutma ekipmanları, BT fonksiyonlarını geniş çapta güç kesintilerinden korumak için jeneratör motorunu içermektedir.

- Motor jeneratörleri için 12 saat yakıt depolama yapılmaktadır (Uptime Institute, 2009-2012).

Performans Doğrulama Testleri:

- Binanın ihtiyaçlarını karşılamak için yeterli kapasiteye sahip olunmalıdır.
- Planlı çalışma, kritik ortamları, sistemleri ve son kullanıcıyı etkileyen bina altyapısının tümünün veya çoğu kısmının kapatılmasını gerektirmektedir (Uptime Institute, 2009-2012).

Operasyonel Etkiler

- Bina planlı ve plansız bir şekilde yapılan faaliyetlerde, aksamaya karşı hassastır.
- Plansız kesinti veya sistem kapasitesi, kapasite bileşeni veya dağıtım elemanından herhangi birinin hatası kritik ortamları etkilemektedir.
- Bina altyapısının gerekli önleyici bakım ve onarım işleri için yıllık bazda güvenli bir şekilde tamamen kapatılması gerekmektedir. Acil durumlarda ise daha sık kapatılması gerekebilir. Düzenli bakımdan kaynaklanan aksamalar, ani aksamaların yanı sıra bozulmalara bağlı olan önemli durumların artışına sebep olmaktadır (Uptime Institute, 2009-2012).

1.4.1.2.Tier II : Bina Altyapısı Yedek Kapasite Bileşenleri

Temel Özellikler:

- Tier II veri merkezlerinde yedek kapasite bileşenleri vardır. Yedek kapasite bileşenleri, ekstra motor jeneratörlerinde, kesintisiz güç kaynağı (UPS)

modüllerinde, enerji depolarında, soğutucularda, ısı atımı cihazlarında, pompalarda, soğutma ünitelerinde ve yakıt depolarında bulunmaktadır.

- Kritik ortamlarda ise yedekli olmayan, tek dağıtım yolu vardır.
- ‘N’ kapasite için yerinde yakıt depolama 12 saattir (Uptime Institute, 2009-2012).

Performans Doğrulama Testleri:

- Yedek kapasite bileşenleri, herhangi bir kritik ortamın kapatılmasına gerek olmadan hizmet dışı edilebilmektedir.
- Bakım veya diğer durumlarda, kritik ortamların kapatılması için dağıtım yolları hizmet dışı edilmektedir.
- Herhangi bir nedenle yedek bileşenler hizmet dışı edilirse, binanın ihtiyaçlarını karşılamak için yeterli düzeyde, kalıcı yüklü kapasite mevcuttur (Uptime Institute, 2009-2012).

Operasyonel Etkiler

- Bina, planlı ve plansız faaliyetlerde dağıtıma duyarlıdır. Bina altyapı bileşenlerinde meydana gelebilecek operasyonel hatalar veri merkezinde aksamalara neden olabilmektedir.
- Planlanmamış bir kapasite bileşen hatası kritik bir ortamı etkileyebilir. Plansız bir kesintide, herhangi bir kapasite sisteminin veya dağıtım elemanının hatası kritik bir ortamı etkilemektedir.
- Bina altyapısının, koruyucu bakım ve onarım çalışmasının güvenli bir şekilde gerçekleştirilmesi için yıllık bazda tamamen kapatılması gerekmektedir. Acil durumlar daha sık kapatılmasını gerektirebilir. Düzenli bakımdan kaynaklanan aksamalar, ani aksamaların yanı sıra bozulmalara bağlı olan önemli durumların artışına sebep olmaktadır (Uptime Institute, 2009-2012).

1.4.1.3. Tier III: Bina Altyapısının Eş Zamanlı Bakımı

Temel Özellikler:

- Veri merkezinin eş zamanlı bakımı, yedek kapasite bileşenlerini ve çoklu bağımsız dağıtım yollarını kapsamaktadır. Herhangi bir zamanda kritik ortamın bakımı için tek bir dağıtım yolu gereklidir.
- Tüm BT ekipmanları, Enstitü'nün yayınlamış olduğu 'Hata Toleranslı Enerji Uygunluk Spesifikasyonları, 2.0 Versiyon' ile tanımlanmış ve bina altyapısının topolojisi ile uyumlu olarak düzgün bir şekilde yüklenmiştir. Transfer cihazları, anahtar kullanım noktası gibi spesifikasyonlara uymayan kritik ortamlar için entegre edilmelidir.
- 'N' kapasite için yerinde yakıt depolama 12 saattir (Uptime Institute, 2009-2012).

Performans Doğrulama Testleri:

- Her bir kapasite bileşeni ve dağıtım yollarındaki elementler, herhangi bir kritik ortamı etkilemeden planlı bir şekilde hizmet dışı edilebilir.
- Herhangi bir nedenle yedek bileşenler hizmet dışı edilirse, binanın ihtiyaçlarını karşılamak için yeterli düzeyde kalıcı yüklü kapasite vardır (Uptime Institute, 2009-2012).

Operasyonel Etkiler

- Bina, planlı olmayan faaliyetlerden kaynaklanan aksamalara karşı hassastır. Bina altyapı bileşenlerindeki işlem hataları, bilgisayar bozulmalarına neden olabilmektedir.
- Kapasite sisteminde planlı olmayan bir kesinti veya arıza kritik ortamı etkilemektedir.

- Bir kapasite bileşeninde veya dağıtım elamanında planlı olmayan kesinti veya arıza kritik ortamı etkileyebilmektedir.
- Kalan cihazlar üzerinde güvenle çalışan yedek kapasite bileşenleri ve dağıtım yolları, bina altyapı bakımında kullanılabilirlerdir.
- Bakım faaliyetleri sırasında bozulma riski yüksek olabilmektedir (Uptime Institute, 2009-2012).

1.4.1.4.Tier IV: Bina Altyapısı Hata Toleransı

Temel Özellikler:

- Hata toleranslı bir veri merkezi, yedek kapasite bileşenleri ve farklı aktif dağıtım yollarının eş zamanlı olarak kritik ortama dağıtımını sağlayan, izole edilmiş sistemlerden oluşmaktadır. Yedek kapasite bileşenleri ve dağıtım yolları, herhangi bir altyapı arızasından sonra kritik ortamların gücünü ve soğutulmasını sağlayan 'N' kapasite gibi yapılandırılmalıdır.
- Tüm BT ekipmanları, Enstitü'nün yayınlamış olduğu 'Hata Toleranslı Enerji Uygunluk Spesifikasyonları, 2.0 Versiyon' ile tanımlanmış ve bina altyapısının topolojisi ile uyumlu olarak düzgün bir şekilde yüklenmiştir. Transfer cihazları, anahtar kullanım noktası gibi spesifikasyonlara uymayan kritik ortamlar için entegre edilmelidir.
- Sistem veya dağıtım yollarının ikisini de eş zamanlı olarak etkileyen herhangi bir olayı engellemek için, tamamlayıcı sistemler ve dağıtım yolları fiziksel olarak izole edilmelidir.
- Sürekli soğutma gereklidir.
- 'N' kapasite için yerinde yakıt depolama 12 saattir (Uptime Institute, 2009-2012).

Performans Doğrulama Testleri:

- Kapasite sistemleri, kapasite bileşenleri veya dağıtım elemanlarından herhangi birinin hatası kritik ortamı etkilememektedir.
- Altyapı kontrol sistemleri, kritik ortamda süregelen bir hataya otonom bir tepki göstermektedir.
- Her bir kapasite bileşeni ve dağıtım yollarındaki elementler, herhangi bir kritik ortamı etkilemeden planlı bir şekilde hizmet dışı edilebilmektedir.
- Yedek bileşenler veya dağıtım yolları herhangi bir nedenle hizmet dışı olduğu zaman binanın ihtiyacını karşılayacak kadar yeterli kapasite mevcuttur (Uptime Institute, 2009-2012).

Operasyonel Etkiler:

- Bina, planlı olmayan bir durumdan kaynaklı aksamalardan etkilenmemektedir.
 - Bina, planlı bir şekilde gerçekleştirilen faaliyetlerden kaynaklı aksamalardan etkilenmemektedir.
 - Kalan cihazlar üzerinde güvenle çalışan yedek kapasite bileşenleri ve dağıtım yolları, bina altyapı bakımında kullanılabilirlerdir.
 - Bakım faaliyetleri sırasında yedek kapasite bileşenlerinin ve dağıtım yollarının kapatılması, kritik ortamlarda bakımı süren kısımlarda bir hata oluşması, bozulma riskinin artmasına yol açabilmektedir.
 - Yangın alarmı, yangın söndürme veya gücün kesilmesi durumları veri merkezlerinde aksamalara neden olmaktadır (Uptime Institute, 2009-2012).
- (23)

Tier sınıflarına ilişkin temel özellikler Tablo 1.1’de gösterilmektedir.

Tablo 1.1 Tier Sınıflarının Özellikleri

	Tier 1	Tier 2	Tier 3	Tier 4
Aktif Kapasite Bileşenleri	N	N+1	N+1	N
Dağıtım yolları	1	1	1 Aktif ve 1 Yedek	2 Eş zamanlı Aktif
Eş Zamanlı Bakım	Yok	Yok	Var	Var
Hata Toleransı	Yok	Yok	Yok	Var
Bölümlere Ayrılma	Yok	Yok	Yok	Var
Sürekli Soğutma	Yok	Yok	Yok	Var

Kaynak: (Uptime Institute, 2009-2012)

Tablo 1.2’de Tier sınıflarına ilişkin maliyetler, risk toleransı ve geniş çapta bina altyapı özellikleri gösterilmektedir.

Tablo 1.2 Tier Sınıflarına Göre Veri Merkezlerinin Genel Özellikleri

	Tier I	Tier II	Tier III	Tier IV
Bina Tipi	Kiralanan	Kiralanan	Bağımsız	Bağımsız
Personel Vardiyası	Yok	1 vardiya	1+vardiya	24 saat kesintisiz
Personel/Vardiya	Yok	1/vardiya	1-2/vardiya	2+/vardiya
Kritik yüklemde kullanılabilme	%100 N	%100 N	%90 N	%90 N
Kabine başına ilk yapım kW	<1 kW	1-2 kW	1-2 kW	1-3 kW
Kabine başına en yüksek kW	<1 kW	1-2 kW	>3 kW	>4kW
Yükseltilmiş zemin oranı için destek alanı	%20	%30	%80-90+	%100+
Yükseltilmiş zemin yüksekliği	12 inç	18 inç	30-36 inç	30-42 inç

Zemin yükleme Ibs/ft	85	100	150	150+
Şebeke gerilimi	208, 480	208, 480	12-15 kV	12-15 kV
Tek kırılma noktası hatası	Birden çok+ İnsan hatası	Birden çok+ İnsan hatası	Bazen+ İnsan hatası	Yangın, Acil Güç Kesintisi+İns an hatası
Örnek Planlı bakım kapatılması	2 yılda 12 saat	2 yıldan sonra 3 olayda 12 saat	Gerekli değil	Gerekli değil
Yıllık kesintileri	28.8 saat	22 saat	1.6 saat	0.8 saat
Kullanılabilirlik	%99.67	%99.75	%99.98	%99.99
Planlanması ve yapım süresi (ay)	3	3-6	15-20	15-30
İlk açılma yılı	1965	1970	1985	1995

Kaynak: (Uptime Institute, (2008))

1.4.2. CENELEC EN 50173-5

Veri merkezleri kablolama alt yapısı ile ilgili olan standart 2007 yılında yayınlanmıştır. ISO/IEC 11801 standardı ve EN 50173 standardının diğer bölümleriyle bir arada kullanılmalıdır (Koçak).

1.4.3. ANSI/TIA-606-A-1

Donanım odaları ve veri merkezi bilgisayar odalarının yönetimi ile ilgili 2008 yılında oluşturulmuş standarttır (Fries ve Tyton, 2009, s.2).

1.4.4. ASHRAE TC9.9

Amerikan Isıtma Soğutma ve İklimlendirme Mühendisleri Derneği (ASHRAE), 1984 'de kurulmuş olup, ısıtma, soğutma, iklimlendirme vb. konularda standartları belirleyen, bu konularda araştırma, eğitim vs. düzenleyen bir kuruluştur (Koçak).

2009 yılında oluşturulan ASHRAE TC 9.9 ile 'Veri İşleme Ortamının Isısına İlişkin Kurallar' oluşturulmuştur.

1.4.5. ISO/IEC 24764

2010 yılında oluşturulan standart, veri merkezi içinde kullanılmak üzere geniş bir yelpazedeki haberleşme hizmetlerini destekleyen jenerik kablolamayı tanımlamaktadır. Dengeli kablolama ve fiber optik kablolama içinde yüksek yoğunluklu donanım bağlantısı kullanımı yer almaktadır (ISO, 2010).

1.4.6. ANSI/BICSI-002

CENELEC ve ISO Standartlarındaki başlıklar ve içerikler ile neredeyse aynıdır.

Genel olarak standartlarda geçen başlıklar;

- Alan planlanması,
- Alan seçimi,
- Mimari,
- Yapısal,
- Elektrik sistemleri,
- Mekanik,
- Yangın koruma,
- Güvenlik,
- Bina otomasyon sistemleri,
- Telekomünikasyon,
- Bilgi Teknolojileri,
- Görevlendirme,
- Veri merkezi bakımı,
- Ek başlıklar (Tasarım süreci, Güvenilirlik ve Kullanılabilirlik) (Kepekci, 2004, s.30).

Kepekci (2004,s.30)'e göre BICSI-002'de veri merkezi kullanılabilirlik sınıfları tanımları aşağıdaki gibidir:

- F0 Sınıfı: Ek (tamamlayıcı) donanım yok,

- F1 Sınıfı: Bazı tamamlayıcı donanım mevcut,
- F2 Sınıfı: Kritik bileşende yedeklilik,
- F3 Sınıfı: Kritik ve kritik olmayan bileşenlerde yedeklilik,
- F4 Sınıfı: Yedek bileşeni ile sistem yedekliliği.

1.4.7. ISO 27001

İletişim ortamlarının yaygınlaşması ve kullanımının artmasıyla birlikte bilgi güvenliğinin sağlanması ihtiyacı her geçen gün katlanarak artmıştır (Doğantimur, 2009, s.11).

ISO 27001, bilgi güvenliği standardı BS 7799-2'nin 2005 yılı sonlarında ISO 27001:2005 olarak son halini almasıyla yürürlüğe giren ve kurumların bilgi güvenliği yönetim sistemi kurmaları için gereklilikleri tanımlayan bir standarttır (Anadolu Bilişim, 2013).

Bilginin korunmasının önemli olduğu bütün kurumlarda kullanılan uluslararası bir standarttır. Sahip olunan envanterin varlığı, açıkları, riskleri, yedekliliği, erişim yetkileri, dokümantasyonun tutulması gibi konularla ilgilenmektedir. Sertifika alındıktan sonra her yıl denetleme yapılarak mevcut durumun korunup, iyileştirilmesi için kontrol yapılmaktadır. Türkiye'de denetleme TSE tarafından yapılmaktadır (Koçak).

ISO 27001'in avantajları aşağıdaki gibidir:

- Bilgi varlıklarının tam tespiti yapılır ve böylelikle kurumun elindeki bilgilerin neler olduğu ve bilgilerin değeri analiz edilebilir.
- Bilginin tam güvenliği: ISO 27001'in gerektirdiği kontrol ve güvenlik mekanizmaları bilgileri güvende tutar.
- Bilgi ve verinin güvenliği sağlandığı için iş sürekliliği de teminat altına alınır (Anadolu Bilişim, 2013).

1.4.8. ISO 9001

ISO 9001 Kalite Yönetim Sistemi Standardı, müşteri beklentileri, ihtiyaçları ve mevzuat şartlarını karşılama yolu ile müşteri memnuniyetinin artırılmasını öngören dünyaca kabul görmüş bir kalite yönetimi sistemi biçimidir (Uluslararası Belgelendirme & Denetim).

Kuruluşun organizasyonel yapısından müşterilerinin memnuniyet seviyesine, toplanan verilerin analiz edilmesinden süreçlerin etkin yönetimine, iç denetimlerden ürün tasarımına, satın almadan satışa kadar pek çok noktada Kalite Yönetim Sistemi koşulları belirlenmektedir.

ISO 9001 Standardı, esas olarak bir kontrol mekanizmasıdır. Bu standardın amacı, hata ve kusurları azaltmak, ortadan kaldırmak ve daha önemlisi oluşabilecek hata ve kusurları önlemektir. Standart, direkt olarak ürün ve hizmet kalitesiyle ilgili değil, yönetim sisteminin kalitesi ile ilgilidir. Buradaki temel varsayım, etkin bir Kalite Yönetim Sistemi oluşturulması ve uygulanması halinde müşteri ihtiyaçlarını karşılayacak kaliteli ürün ve hizmetler üretilceğidir (Uluslararası Belgelendirme & Denetim).

ISO 9001 Standardı, zorlayıcı değildir ve genel şartlar içermektedir. Büyük ya da küçük ölçekli ayrımı olmaksızın her sektör için uygulanabilmektedir. Doğru anlaşılıp, doğru uygulandığında güçlü bir yönetim sistemini temsil etmektedir.

ISO 9001 Standardı, Kalite Yönetim Sistemi'nin nasıl oluşturulacağını tamamen kuruluşlara bırakmıştır. Yapılması gereken "standart" bir Kalite Yönetim Sistemi değil, standardın şartlarını karşılayan bir Kalite Yönetim Sisteminin oluşturulmasıdır.

Sonuç olarak ISO 9001 Standardı;

- Etkin bir kalite yönetim sistemi için minimum şartları belirtmektedir.
- Şartları geneldir, ölçek fark etmeksizin her sektör için uygulanabilmektedir.

- Nasıl yapılacağını değil, neyin yapılacağını söylemektedir (Uluslararası Belgelendirme & Denetim).

1.4.9. ISO 20000-1

ISO 20000-1 Standardı Bilgi Teknolojileri Hizmet Yönetim Sistemi Standardı olarak tanımlanmıştır. ISO 20000-1 Standardı bilişim dünyasını içeren 6 veya 7 standardın bir araya getirilerek bilişim firmalarının faaliyetlerini ve kurumsal yapısını oluşturmak için hazırlanmıştır (İntersistem).

ISO 20000-1 Standardı, Bilişim Teknoloji kuruluşlarının ilgili operasyonlarını yönetmelerinde ve hizmet vermelerinde hangi metodların, nasıl uygulanacağına kılavuzluk etmektedir.

ISO 20000-1 Bilişim Teknolojileri BT Standardı Belgelendirmesi yapmak isteyen bilişim teknoloji firmaları bu belgeyi alabilmesi için mutlaka servis sonrası hizmetlerini oluşturmalıdır (İntersistem).

ISO 20000-1 sistemi anlatan standart, ISO 20000-2 ise ISO 9004 gibi kılavuzluk eden standarttır. Bu standartların Güncel sürümü 2005 yılında yayınlanmış olup standardın genel adı ISO 20000:2005' tir (İntersistem).

1.4.10. SSAE16

SAS 70, hizmet organizasyonları Amerika Yeminli Serbest Mali Müşavirler Enstitüsü (AICPA) tarafından hazırlanmış bir üçüncü taraf denetim rapor ve tasdik standardıdır. Bu standart kapsamındaki denetim, hizmet kuruluşunun sunduğu hizmetleri destekleyen bilgi teknolojileri ve ilişkili süreçlerinin ayrıntılı biçimde incelenmesini içermektedir. Müşterilerine ait bilgiyi işleyen veya barındıran servis sağlayıcılar ve diğer hizmet kuruluşları yeterli kontrollerin bulunduğunu ispat etmekle yükümlüdürler. Denetimlerde, ayrıca organizasyonun finansal durumu ve

riskleri, insan kaynakları, iş sürekliliği uygulamaları ve felaketten kurtarma gibi uygulamalarına güvence verilebilmektedir (KPMG,2013).

SAS 70 standardı, 15 Haziran 2011 tarihinden itibaren revize edilerek, SSAE 16 standardına geçilmiştir. AICPA tarafından hazırlanmış ve ISAE 3402 tabanlı ulusal bir denetim ve güvence standardı olan SSAE 16 yaygın olarak kullanılmaktadır (KPMG,2013).

1.4.11. SOC 1, SOC 2 ve SOC 3

ISAE 3402 standardının altındaki farklı denetim konularının ve uygunluk kriterlerinin çeşitli güvence gereksinimlerine uygun olarak kullanımını sağlamak için, AICPA tarafından finansal raporlama ve diğer ilişkili süreçler üzerindeki işletilen kontrollere güvence sunma amaçlı ISAE 3402 standardını baz alan SOC1, SOC2 ve SOC3 rapor çeşitleri geliştirilmiştir (KPMG,2013).

SOC1 raporu, doğrudan firmanın finansal raporlama faaliyetleri ve finansal tablolarından öte, sunulan hizmetin, hizmet alan kuruluşun finansal raporlamasına etkisi üzerinde bir görüş içermektedir. SOC1 raporu, servis sağlayıcının finansal raporlarına ve iç kontrol mekanizmasına ilişkin kontrollerini kapsamaktadır (KPMG,2013).

SOC2 raporları Mutemetlik Hizmetleri prensiplerine dayalı bir şekilde politika, iletişim, prosedür ve izleme modelleri üzerinde şekillenmiştir (KPMG,2013).

SOC2 ve SOC3 raporları ise erişebilirlik, veri güvenliği, gizlilik ve işlem bütünlüğü alanlarına etki eden operasyonel kontrolleri kapsamaktadır. SOC2 ve SOC3 raporları arasındaki fark; SOC3 raporlarının kontrollere ilişkin testler hakkında detay içermemesi, pazarlama amacıyla kullanılabilmesi ve paylaşımı açısından bir engel bulunmamasıdır (KPMG,2013).

1.5. Veri Merkezi Türleri

Veri Merkezleri iki şekilde hizmet sağlamaktadırlar. Bunlar; Şirket Veri Merkezi ve İnternet Veri Merkezi'dir.

1.5.1. Şirket Veri Merkezi

Özel şirket, eğitim kurumları veya devlet kuruluşları tarafından, kendi bilgi teknolojileri ihtiyaçlarını ve web hizmetlerini gidermek için kurulan ve şirketin BT personeli tarafından yönetilen veri merkezleridir (BİLGE, 2009).

1.5.2. İnternet Veri Merkezi

İnternet Veri Merkezleri, kendi veri merkezini oluşturmayan veya kısmi veri merkezi hizmeti almak isteyen şirketlere imkân sağlamak amacıyla ticari telekomünikasyon firmaları tarafından kurulmakta ve işletilmektedir. (BİLGE, 2009).

İnternet veri merkezi tarafından sağlanan ana hizmetler ise yer paylaşımı (co-location) ve barındırma (hosting) olarak adlandırılmaktadır. Bu hizmetler, yönetimin internet veri merkezi işletmesine veya hizmet alan kuruluşa ait olduğu farklı birleşimlerle sunulabilir. Veri merkezlerinde sağlanan diğer hizmetler; veri tabanı yönetimi, web yönetimi, sunucu yönetimi, servis yönetimi, konfigürasyon yönetimi, performans yönetimi, kullanıcı yönetimi, yedekleme/geri yükleme, ek güvenlik duvarı, ağ ve bilgi güvenliği yönetimi, yük dengeleme, veri ambarı, felaket kurtarma hizmeti ve sayısal sertifikadır (UBAK, 2005, s.9-15).

Bugün birçok veri merkezi internet hizmet sağlayıcıları tarafından kendilerine ait veya üçüncü şahıs sunucularını barındırmak amacıyla çalıştırılmaktadır. Bununla birlikte bugüne kadar oluşturulan veri merkezleri sadece bir şirketin kullanımında olabilir, üçüncü şahsa ait sunucuları barındırabilir (co-location) veya ağ bağımsız veri merkezi olarak kullanılabilir (Wikipedia, 2014a).

1.5.2.1. Barındırma (Hosting) Hizmeti

Ev sahipliği hizmeti; internet veri merkezinden hizmet alan kuruluşun kendi işi çerçevesinde kullandığı yazılım, veri ve uygulamalarını internet veri merkezinde bulunan sunucular ve veri depolama birimlerinde çalıştırması ve/veya internet veri merkezi işletmecisi tarafından sağlanan uygulamaları kullanmasıdır (UBAK, 2005, s.11).

1.5.2.2. Yer paylaşımı (Co-location)

Yer paylaşımı hizmeti; internet veri merkezinden hizmet alan kuruluşun kendi işi çerçevesinde kullandığı (kendisine ait) BT sistemlerini internet veri merkezi alanına kurması, internet veri merkezinin temel altyapı olanaklarını ve ağ altyapısını, isteğe bağlı olarak da yönetim hizmetini kullanmasıdır (UBAK, 2005, s.12).

1.6. Veri Merkezinde Olması Gereken Özellikler

Uluslararası standartlara sahip güvenli ve güvenilir bir veri merkezinde olması gereken özellikleri 7 ana başlıkta toplamak mümkündür. Bu başlıklarda yer alan özellikler aşağıdaki gibidir:

1.6.1. Güvenlik Politikaları

Veri merkezinde bulunması gereken güvenlik politikaları; kayıt, veri, fiziksel erişim vb. güvenlik politikası, prosedür ve talimatların hazırlanması, dokümantasyonun periyodik olarak bakımı ve güncellenmesi, personelin bilgi güvenliği eğitimleri alması, tam zamanlı bilgi güvenliği ekibi kurulması, iç denetim ve uyumluluk ekibi kurulması, fiziksel güvenlik ekibi kurulmasıdır (Mataracıoğlu, 2013).

Veri merkezine giriş çıkışlarının belli bir yetkilendirme ile yapılması, her isteyen buraya girememesi gibi kısıtlamalar mutlaka uygulanmalıdır. Dışarıdan gelipte veri

merkezinde çalışma yapacak kişilerin yanında da mutlaka kontrol, bilgilendirme ve uyarı amacıyla bir yetkili personel bulundurulması önemlidir. Oda içinde yapılan değişiklikler veya güncellemeler kayıt altına alınmalı ve ilgisi olan kişilerde bunlardan haberdar edilmelidir (Bilge, 2009).

Fiziksel ve çevresel güvenliğin sağlanmasında aşağıda belirtilen hususlara dikkat edilmelidir:

- Kartlı erişim kontrol mekanizmalarının kullanılması,
- Alarm sistemlerinin kullanılması,
- Kamera sistemlerinin kullanılması,
- Misafir erişimleri için prosedür hazırlanması,
- Veri merkezlerine erişimin kayıt altına alınması,
- Veri merkezinde kritik bileşenlerin belirlenmesi ve bu bileşenlerin ayakta kalabilmesi için birincil ve ikincil güç kaynakları kullanılması,
- Hava soğutma sistemlerinin kullanılması,
- Yangın söndürme sistemlerinin kullanılması,
- Isı, duman ve su sensörlerinin kullanılması, olay durumunda sistemin alarmı çalıştırması,
- Veri merkezi teknisyenlerinin yangın söndürme eğitimi alması (Mataracıoğlu, 2013).

Veri merkezlerinde zorunlu olan yangın söndürme sistemleri elektronik cihazlara ve personele zarar vermeyecek şekilde olmalıdır. Bu yüzden elektriksel iletkenliği olmayan, kokusuz, renksiz, hızla buharlaşıp söndüren çevre dostu gazlar kullanılmalıdır (Gökmen ve Küçüksille, 2013, s.6).

Ayrıca, klimalardan sızan su sızıntıları, sıcaklık, yangın, voltaj değişimleri ve içerde bulunan havanın kalitesi izlenerek anlık bilgilendiren sistemler tarafından takip edilmelidir. Bu bilgilendirmeler mail veya sms yoluyla sorumlu kişiye iletilebilir (Gökmen ve Küçüksille, 2013, s.4).

Veri merkezlerinde altyapı güvenliğinin sağlanmasına ilişkin özellikler aşağıdaki gibidir (Mataracıoğlu, 2013);

- Zararlı yazılımlara karşı sistem taramaları yapılması,
- İç ağ trafiği ve personelin sistemde gerçekleştirdiği aksiyonların izlenmesi,
- Zafiyet yönetimiyle ilgili olarak sızma testleri, kaynak kod analizi ve dış denetimler yapılması,
- Bilgi güvenliği ihlal olayları bildirim mekanizmasının kurulması,
- Personelin sayısal adli analiz konusunda eğitilmesi,
- Ağ güvenliğiyle ilgili olarak ağların ayrılması,
- Değişim yönetimi (change management) ile kontrol edilen güvenlik duvarı ve erişim kontrol listeleri (ACL) konfigürasyonlarının yapılması,
- Ağ cihazlarına erişimin sınırlandırılması,
- Tüm dış trafiğin ön-uç sunuculara (front-end servers) yönlendirilmesi,
- Programlama hatalarına karşı exploit loglarının takip edilmesi,
- OSI taşıma katmanı güvenliği olarak, daha güvenli tarayıcı bağlantıları için HTTPS kullanılması,
- İşletim sistemi güvenliği olarak, sunuculara yamaların, öncelikle bir test ortamında test edildikten sonra, değişim yönetimi çerçevesinde düzenli olarak yüklenmesi.

1.6.2. Veri Yönetimi

Veri Merkezinde veri yönetiminde; bilgi erişiminde kimlik doğrulama ve yetkilendirme zorunluluğu getirilmesine (Bilge, 2009), yönetsel erişimlerin SSH bağlantıları üzerinden yapılmasına, sistemden ayrılacak veri için güvenli imha etme prosedürünün çalıştırılmasına dikkat edilmelidir (Mataracıoğlu, 2013).

1.6.3. Erişim Kontrolü

Veri merkezinde erişim kontrolünün sağlanmasında aşağıda belirtilen hususlara dikkat edilmelidir:

- Her personel için tekil kullanıcı adı kullanılması,
- Güçlü bir parola politikasının uygulanması,
- 2 faktörlü kimlik doğrulama mekanizmalarının kullanılması,
- Personelin iş tanımına ve bilmesi gereken prensibine göre erişim haklarının düzenlenmesi,
- Her türlü yönetimsel erişimin kayıt altına alınması (logging),
- Personelde bilgi güvenliği farkındalığının oluşturulması,
- Personelin gizlilik anlaşması imzalaması,
- Bilgi güvenliği ihlal olayları bildirim mekanizmasının kurulması (Mataracıoğlu, 2013).

1.6.4. Sistem Geliştirme ve Bakımı

Veri merkezinin sistem geliştirmesi ve bakımında aşağıdaki özelliklere dikkat edilmelidir:

- Uygulama, sistem ve servis güvenliğine ilişkin politika oluşturulması,
- Proje tasarımı risklerini ve karşı önlemlerinin düzenli olarak gözden geçirilmesi,
- Kodların implementasyon seviyesinde güvenlik değerlendirmesinin yapılması,
- Güvenlik riskleriyle ilgili sürekli danışmanlık veren ekibin kurulması,
- Güvenli yazılım yaşam döngüsünün oluşturulması,
- Güvenlik eğitimlerinin verilmesi,
- İmplementasyon seviyesinde güvenlik testleri ve gözden geçirmelerin yapılması (Mataracıoğlu, 2013).

1.6.5. İş Sürekliliği ve Felaket Kurtarma

İş sürekliliğin sağlanması ve felaket durumları için;

- Verinin, veri merkezi içerisinde senkronizasyonunun (eşitleme) yapılması,
- Veri merkezleri arasında yüksek hızlı bağlantının oluşturulması,

- İş sürekliliđi politikası ve iş sürekliliđi/felaket kurtarma planlarının oluşturulması gerekmektedir (Mataraciođlu, 2013).

2. ÖRNEK VERİ MERKEZLERİ

2.1. Türkiye’de Veri Merkezleri

Türkiye’de telekomünikasyon alanındaki ilerlemelerle internet kullanıcı sayısının artmasıyla doğru orantılı olarak veri merkezi alanında da büyük gelişmeler yaşanmıştır (Yalçıntaş, 2013, s.75).

Hızla artan internet kullanım oranı ve veri trafiği Türkiye’yi veri merkezleri yatırımlarında birinci konuma getirmiştir.

Kullanıcı sayısındaki artış, telekomünikasyon alanındaki yoğun rekabet ve Bankacılık Düzenleme ve Denetleme Kurulu (BDDK)’nın bankalara ait veri merkezlerinin Türkiye’de inşa edilmesi için getirdiği zorunluluklar üzerine Türkiye veri merkezi alanında 2011 yılında %60’lık büyüme göstermiştir. (Yalçıntaş, 2013, s.75).Türkiye veri merkezi sektörü finansal anlamda ise % 74’ lük bir büyüme kaydetmiştir. 2011 yılı sonu itibariyle Türkiye’deki toplam veri merkezi yatırımı 35 milyar dolar olarak tahmin edilmektedir. Bu göstergeler Türkiye’de veri merkezi sektörünün gelişme aşamasında olduğunu ve gelişme potansiyelinin bulunduğunu göstermektedir (Özatay, 2012, s.8-9).

Türkiye’deki önemli İnternet veri merkezleri ve Pazar payları aşağıdaki Tablo 2.1’de gösterilmektedir.

Tablo 2.1 Türkiye’de İnternet Veri Merkezleri

Hosting Sıralaması	Türkiyedeki Hosting Firmaları	2010 Türkiye Hosting Pazar Payları	Firmaların Host Ettikleri Alan Adı Sayısı
1	NATROHOST.COM	8,64%	78545
2	ISIMTESCIL.NET	8,01%	72750
3	TURKTICARET.NET	7,56%	68684
4	IHS.COM.TR	5,39%	48961
5	SADECEHOSTING.COM	2,95%	26768
6	MARKUM.NET	2,40%	21777
7	DORUK.NET.TR	1,99%	18037
8	WEBSAHIBI.COM	1,76%	15998
9	NIOWEB.NET	1,75%	15913
10	TURHOST.COM	1,62%	14676
11	KRIWEB.COM	1,39%	12617
12	TURKISHOST.COM	1,36%	12342
13	KEBIRHOST.COM	1,24%	11281
14	NETDIREKT.COM.TR	0,78%	7051
15	MYNET.COM	0,74%	6685
16	VIT.COM.TR	0,73%	6672
17	ALANTRON.COM	0,72%	6531
18	KAREGEN.COM	0,71%	6489
19	KOBILINE.COM	0,67%	6079
20	VARGONEN.COM	0,66%	5991
21	GARANTIWEB.COM	0,53%	4843
22	LINESIS.COM	0,48%	4361
23	ANADOLUDNS.COM	0,48%	4337
24	KOC.NET	0,48%	4316
25	SISTEMHOST.COM	0,45%	4070

Kaynak: (Özatay, 2012, s.9)

Türkiye’de veri merkezleri Pazar büyümesi sıralaması Tablo 2.2 ‘de gösterilmiştir.

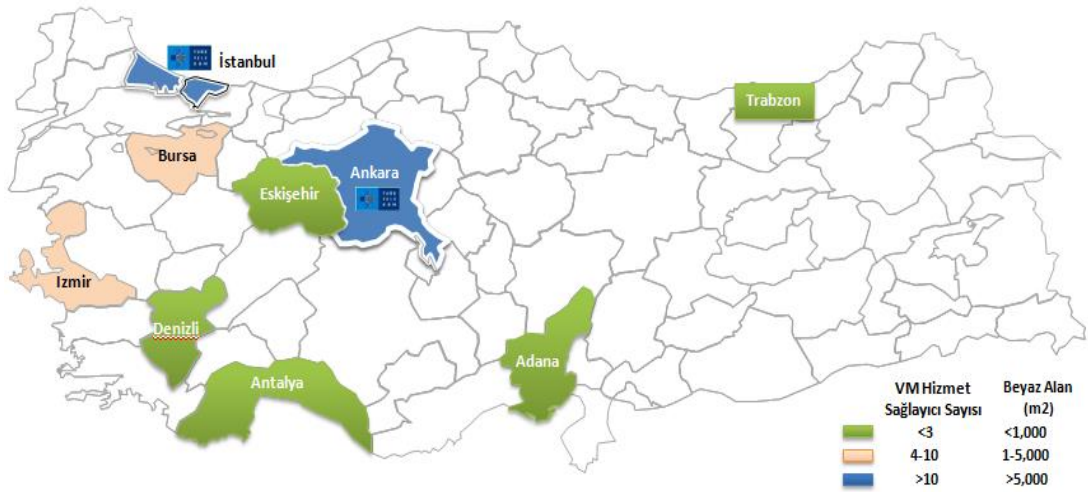
Tablo 2.2 Türkiye Veri Merkezleri Pazar Büyümesi

Sıra	Tesis profilinde büyüme %’si 2011-2012		Yatırımda büyüme %’si 2011-2012		2012 yatırım değeri (milyar) \$	
1.	Türkiye	60%	GD Asya	118%	Batı ABD	3.5
2.	Brezilya	45%	Türkiye	74%	İngiltere	3.35
3.	Kolombiya	40%	Rusya	59%	Çin	3.1
14.	Orta ABD	12%	İngiltere	25%	Türkiye	1.8

Kaynak: (Uyanık,2013)

Türkiye’de 9 şehir üzerine yayılmış toplamda yaklaşık 50-60 bin m² beyaz alana sahip 50-60 VM hizmet sağlayıcısı bulunduğu tahmin edilmektedir (Şekil 2.1). 1.000 m² beyaz alanı geçen veri merkezine sahip hizmet sağlayıcı sayısını 10’ un altındadır (Uyanık, 2013).

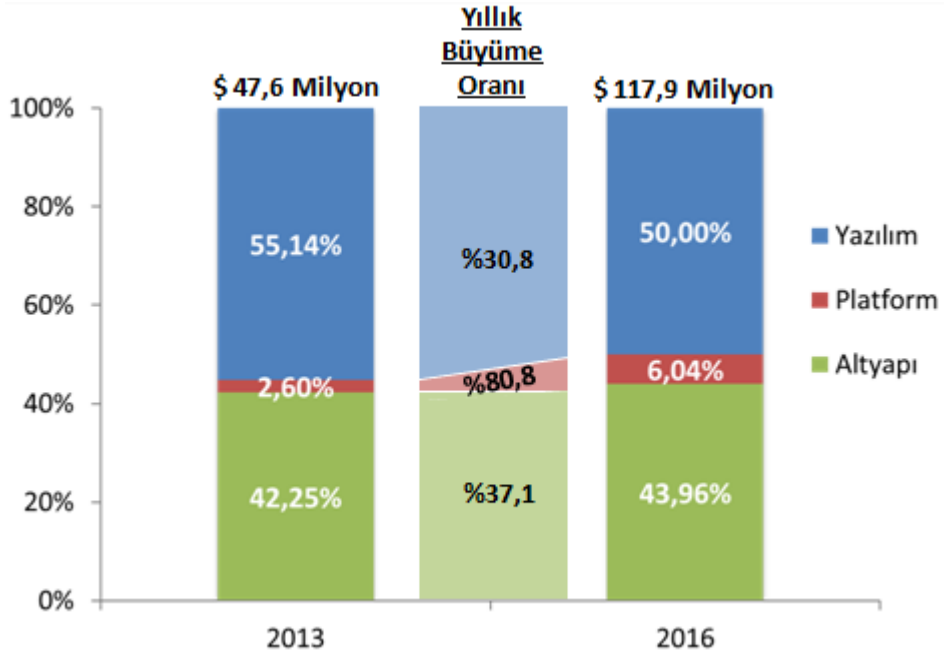
Şekil 2.1 Türkiye’deki Veri Merkezi Hizmet Sağlayıcıları



Kaynak: (Uyanık, 2013)

Şekil 2.2’de Türkiye’deki Bulut bilişim istatistiklerine baktığımızda, pazarın yıllık büyüme oranının %30’un üzerinde bir hızla büyümesi öngörülmektedir. 2016 yılı verilerine baktığımızda, bulut bilişimde platform ve altyapı pazarlarında artış beklenmektedir.

Şekil 2.2 Türkiye Bulut Pazarı



Kaynak: (IDC, 2012-2016)

2.1.1. Türk Telekom Veri Merkezi

Türk Telekom, Ankara ve İstanbul olmak üzere iki lokasyonda, Tier III sertifikasına sahip veri merkezi hizmeti sunmaktadır.

Türk Telekom veri merkezinde uzman kadrosuyla teknik desteğin sağlanmasının yanında, sunucularının bulunduğu fiziksel ortama sadece manyetik kartlı ve parmak izi kontrollü giriş imkanı ile yüksek güvenlik sağlanmaktadır.

Türk Telekom'un Ankara, Ümitköy'de bulunan veri merkezine ilişkin özellikler aşağıdaki gibidir:

- 2X10 Gbps Metro Ethernet,
- 2X622 Mbps (STM4 POS bağlantı),

- 2X622 Mbps ATM bağlantı ile kullanıcılarına oldukça yüksek seviyelerde bant genişliği hizmeti,
- Uluslararası standartlara göre, Tier IV mimarisine göre yedeklenmiş UPS, jeneratör ve trafo sistemleri,
- Yangın tespit ve önleme sistemi,
- Yedekli iklimlendirme sistemi,
- 7/24 gözlemlene (monitoring),
- Manyetik kartlı ve parmak izi kontrollü fiziksel giriş,
- 7/24 bina güvenliği ve teknik personel bulunmaktadır (Türk Telekom).

Türk Telekom'un İstanbul, Gayrettepe'de bulunan veri merkezine ilişkin özellikler aşağıdaki gibidir:

- 40 Gbps Metro Ethernet internet,
- 1 Gbps Metro Ethernet, noktadan noktaya bağlantılar ile kullanıcılarına hizmet vermektedir.
- Tier III Veri Merkezi;
 - Altyapı bileşenleri ve dağıtım yolları yedeklidir.
 - Sunucu sistemlerinde çift güç kaynağı bulunur.
 - Bakım çalışmaları için yedek bileşenler ve dağıtım yolları kullanılır.
 - Hata toleransı yoktur. Öngörülen ayakta kalma oranı %99,782'dir.
 - IT servislerini 7/24 kullanan şirketler için çok uygun bir altyapı sağlanmaktadır.
- Uluslararası standartlara göre, Tier IV mimarisine göre yedeklenmiş UPS, jeneratör ve trafo sistemleri,
- Akıllı patch panel sistemi,
- Yedekli iklimlendirme,
- Yangın tespit ve önleme sistemi,
- Yapısal kablolama,
- Soğuk koridor kapaması,
- Yükseltilmiş döşeme, 80 cm,
- Tavandan kablolama,

- Çevreci yeşil veri merkezi,
- Kabin kilit sistemi,
- ITIL süreçlerine uyumluluk,
- ISO 27001 kalite sertifikası,
- Orta gerilim hattından trafo, jeneratör, ATS, UPS, STS, PDU'ya kadar tamamen 2N yedeklilik,
- Akıllı PDU'lar sayesinde tüketilen enerji kadar ücretlendirme,
- Standart güç kapasite 5kW/rack ve 5000 MW / 600 m2
- 7/24 bina güvenliği ve gözlemeleme (monitoring) ve teknik personel bulunmaktadır (Türk Telekom).

Türk Telekom Veri Merkezlerinin diğer önemli özellikleri de aşağıda yer almaktadır;

Erişim

- Yedekli fiber güzergahı
- Yedekli ağ altyapısı
- Yüksek kapasiteli ana omurga bağlantısı.

Enerji

- Orta gerilim hattından (Trafo, jeneratör, ATS, UPS, STS, PDU 'ye kadar tamamen 2N yedeklilik)
- Akıllı PDU'lar sayesinde tüketilen enerji kadar ücretlendirme.

Klima

- Yedekli İklimlendirme sistemi
- Yükseltilmiş taban
- Soğuk koridor kapama
- Free Cooling Klima.

Donanım

- Bulut Bilişim servisleri için Türkiye'nin en büyük sanallaştırma altyapısı

- Merkezi depolama ağı
- Merkezi yedekleme yapısı
- Felaket kurtarma çözümleri için uzak mesafe replikasyon altyapısı.

Yangın-Güvenlik

- Gazlı yangın söndürme sistemi
- CCTV, kartlı ve parmak izi kontrollü giriş sistemi
- 7x24 Güvenlik personeli
- 7x24 Sistem takibi.

Sistem Yönetim

- Altyapının 7x24 gözlenmesi
- 7/24 destek.

Türk Telekom'da Yeşil Veri Merkezi ile enerji tasarrufu yapılarak iklim değişikliğine neden olan karbon türevi gazların tüketiminin aza indirgenmesi hedeflenmektedir. Bu konuda;

- Soğuk ve sıcak koridor uygulaması,
- Tavandan kablolama, yükseltilmiş döşeme,
- Dinamik soğutma uygulanmaktadır (Türk Telekom).

2.1.2. Superonline Veri Merkezi

Superonline, İstanbul, Ankara ve İzmir olmak üzere 3 şehirde toplam 4660 m²'lik alanda veri merkezi hizmeti sunmaktadır. Gebze yatırımı ve Global İletişim ile birleşmesi ile birlikte toplam 8560 m²'lik alanda veri merkezi hizmeti verilmesi planlanmaktadır.

Superonline Veri Merkezleri standartları aşağıdaki gibidir:

- 2N+1 Enerji ve N+2 İklimlendirme Altyapısı ile tüm enerji ve iklimlendirme altyapısı birebir yedekli bir yapıda tasarlanmıştır.

- Turkcell SOL yedekli fiber altyapısı ile müşterilere yüksek SLA sunulmaktadır.
- IP& Transmisyon seviyesinde donanım yedekliliği ile ağ ekipmanlarında ve hizmetlerinde yedeklilik ile hizmet sürekliliği sağlanmıştır.
- 7/24 güvenlik ve birinci seviye destek personeli ile operasyonlar için uygulanan güvenlik ve destek seviyesinde hizmet sağlanmaktadır.
- ISO 27001, ISO 10002, ISO 20000, ISO 90001 standartlarına sahiptir (Superonline, 2012,s.6-7).

İstanbul Kartal, Yenibosna ve Dudullu, Ankara Söğütözü ve İzmir Bornova, Superonline veri merkezi hizmetinin verildiği yerlerdir. Kartal, Yenibosna ve Dudullu veri merkezlerinin özellikleri aşağıda açıklanmıştır.

Kartal Veri Merkezi'nin genel özellikleri aşağıdaki gibidir:

- 349 m² Müşteri Alanı,
- Gazlı Yangın Söndürme Sistemi,
- Yükseltilmiş Döşeme,
- 2 x 1200 KVA Masterguard UPS,
- 4 x 2250 KVA Çukurova Jenaratör,
- 1100 Kw Hiross İklimlendirme Sistemi.

Kartal Veri Merkezi altyapısı ve bina detayları aşağıda belirtilmiştir.

- APC Marka Sistem Kabinetleri (42 U 600 x 1070)
- Kabinetler üzerinde 3 ayrı kablo yönetim yolu (bakır, fiber ve enerji)
- 2 ayrı UPS grubundan enerji beslemeleri,
- Gazlı yangın söndürme sistemleri (FM200-ClassA-%7,90)
- Yerden tavan yüksekliği 3.25 metre,
- 750 Kg m² taşıma kapasitesi,
- Duma dedektörleri, ısı ve nem dedektörleri,

- DC içinden direk bağlantılı çalışma ofis alanı,
- 7/24 sistem destek ekibi,
- 7/24 bina fiziksel güvenlik ekibi.

Yenibosna Veri Merkezi'nin genel özellikleri aşağıdaki gibidir:

- 110 m² ,
- Gazlı yangın söndürme sistemi
- 2 x 400 KVA Tescom UPS,
- 1 x 800 KVA + 1 x 1100 KVA Aksa Jenaratör
- 240 Kw Stultz İklimlendirme Sistemi.

Yenibosna Veri Merkezi altyapısı ve bina detayları aşağıda belirtilmiştir.

- Estap Marka Sistem Kabinetleri (42 U 600 x 1700)
- Kabinetler üzerinde 3 ayrı kablo yönetim yolu (bakır, fiber ve enerji)
- 2 ayrı UPS grubundan enerji beslemeleri
- Gazlı yangın söndürme sistemleri (Stat-X) (36)
- Yerden tavan yüksekliği 2.75 metre,
- 1600 Kg m² taşıma kapasitesi,
- Duman dedektörleri, ısı ve nem dedektörleri,
- DC içinden direk bağlantılı çalışma ofis alanı,
- 7/24 Sistem destek ekibi,
- 7/24 Bina teknik destek ekibi,
- 7/24 Bina fiziksel güvenlik ekibi.

Dudullu Veri Merkezi'nin genel özellikleri aşağıdaki gibidir:

- 1050 m²,
- Gazlı yangın söndürme sistemi,
- Yükseltmiş döşeme,
- 10 x 275 KVA Tescom UPS,

- 1 x 16000 KVA Jenaratör,
- 390 KW BTU İklimlendirme Sistemi.

Dudullu Veri Merkezi altyapısı ve bina detayları aşağıda belirtilmiştir.

- APC Marka Sistem Kabinetleri (42 U 600 x 1070),
- Kabinetler üzerinde 3 ayrı kablo yönetim yolu (bakır, fiber ve enerji),
- 2 ayrı UPS grubundan enerji beslemeleri,
- Gazlı yangın söndürme sistemleri (FM200-ClassA-%7,90)
- Yerden tavan yüksekliği 3.25 metre,
- 750 Kg m² taşıma kapasitesi,
- Duman dedektörleri, ısı ve nem dedektörleri,
- DC içinden direk bağlantılı çalışma ofis alanı,
- 7/24 Sistem destek ekibi,
- 7/24 Bina fiziksel güvenlik ekibi (Superonline,2012,s.8-10).

Superonline Veri Merkezi Hizmetleri:

- Sunucu Barındırma:
 - Sunucu Kiralama
 - Sanal Sunucu Kiralama
- Alan Adı Barındırma
- Web Alanı Barındırma
 - SSL
 - Veritabanı
- Ek hizmetler
 - Veri Depolama
 - Veri Yedekleme.

Superonline Sunucu Barındırma hizmetleri, büyük ve orta ölçekli firmaların sunucularına özel bir yer ayrılarak fiziksel ve elektriksel olarak güvenli ve

emniyetli bir ortamda tutulması ve sunucuya kaliteli internet erişimi sağlanması kapsamında aşağıdaki hizmetleri içermektedir:

- Sunucu için yer kiralama,
- Güvenli elektrik altyapısı (yedekli UPS ve kesintisiz güç kaynakları),
- Sunucu data ve elektrik kabloları,
- Elektronik ve fiziksel güvenlik,
- Sunucuya fiziksel seviyede temel müdahale.

Sunucuya yedekli ve güvenli (firewall ile) internet bağlantısı sağlanmasıdır (Superonline,2012,s.13). Superonline Veri Depolama hizmetleri, veri merkezinde bulunan şirketlerin sunucularına ek olarak mevcut veri kapasitelerini arttırabilmek amacıyla Superonline veri depolama alanlarından yer ayrılarak sağlanan hizmettir. Aşağıda belirtilen hizmetleri kapsamaktadır:

- FATA veya FC diskler sağlanabilmektedir.
- RAID 0, RAID 5, RAID 6, RAID 10 seviyeleri desteklenebilmektedir.
- “0” ilk yatırım maliyeti,
- Yüksek seviye güvenlik,
- Dinamik yapıdan kaynaklanan yüksek verimlilik,
- Yüksek performans,
- Kurulum ve işletim kolaylığı,
- 1. ve 2. Seviye 7/24 kurumsal destek sağlanmaktadır (Superonline,2012,s.14).

Şekil 2.3 Superonline Veri depolama hizmet paketleri



Kaynak: (Superonline, 2012, s.14)

Superonline Veri Yedekleme hizmeti ile sunucular üzerindeki uygulamalar dahil her türlü veri istenilen periyotlarda yedeklenmektedir. Aşağıda belirtilen hizmetleri kapsamaktadır:

- “0” ilk yatırım maliyeti,
- Yüksek seviye güvenlik,
- Sunucuların daha etkin kullanımı,
- Sunucularda daha yüksek performans,
- Kurulum ve işletim kolaylığı,

1. ve 2. Seviye 7/24 kurumsal destek sağlanmaktadır (Superonline, 2012, s.15).

Şekil 2.4 Superonline Veri Yedekleme Hizmet Paketleri

Yedekleme Sıklığı		
HER AY	HER HAFTA	HER GÜN
GB / TB ihtiyacınıza yönelik aylık hizmet bedelleri		
1	4	10
Saklanan Versiyon		

Kaynak: (Superonline,2012,s.15)

Superonline Veri Merkezi'nin güvenlik ürünleri;

- DDoS Atak Önleme,
- Merkezi Güvenlik Yönetimi,
- 5651 Loglama'dır.

Superonline Veri Merkezi'nin yüksek kapasiteli sunucularda, özelleştirilmiş sanal sunucuları;

- CPU,
- RAM,
- Disk,
- İşletim Sistemi,
- Veritabanı'dır (Superonline,2012,s.16-17).

Superonline veri merkezine uzaktan bağlantının yapılması ve uzaktan verilerin ve sunucuların yedeklenmesi sağlanmaktadır.

Uzaktan Sunucu Yedekleme Hizmetleri ile;

- Kullanıma bağlı aylık ücretlendirme,
- Otomatik yedekleme,
- SLA'ları ölçülebilen, raporlanan hizmet,
- Yüksek seviyede güvenlik sağlanmaktadır (Superonline, 2012, s.19).

Şekil 2.5 Superonline Uzaktan Sunucu Yedekleme Hizmetleri



Kaynak: (Superonline, 2012, s.19)

Superonline Olağanüstü Durum Merkezi, deprem, sel vb. felaket durumlarından etkilenmeksizin iş sürekliliğinin sağlanmasına yardımcı olmaktadır. Herhangi bir felaket durumunda Olağanüstü Durum Merkezi'nde yedeklenen sunucular üzerindeki tüm uygulama ve verilerin kullanımında hiçbir kayıp olmamaktadır. Superonline Olağanüstü Durum Merkezi'nde;

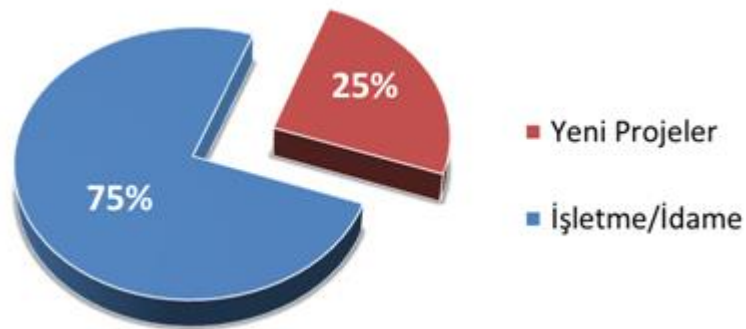
- Veriler yedeklenerek fiziksel olarak güvenli bir alanda saklanmakta,
- İş sürekliliğinin ve performansın garanti altına alınmakta,
- Bilgi kaybının önlenmekte,
- Yönetimi ve işletimi Turkcell kalite standartlarında uzman bir ekip tarafından yürütülmekte,
- Olağanüstü durumlar nedeniyle yaşanacak kesintilerin yaratacağı riskler elimine edilmektedir (Superonline, 2012, s.21).

2.2. Dünya Uygulamaları

Veri merkezinin yönetiminin ve sürekliliğinin sağlanması için veri merkezi bileşenlerinin (sunucular, soğutma, güç kaynağı ve aküler, enerji, yönetim merkezi, jeneratör, depolama üniteleri, güvenlik, nitelikli insan kaynağı) düzgün işleyen bir yapıda olması gerekmektedir. Bu bileşenlerde karşılaşılan hatalar, hizmetin sağlanmasını güçlendirdiği için, bilgi işlem yöneticileri veri merkezini ayakta tutabilmek için zamanının ve mali kaynakların büyük bir kısmını veri merkezi bileşenleri için ayırmaktadır. Bu sebeple, veri merkezine ilişkin önemli harcamalar gündeme gelmektedir.

2012 verilerine göre dünya’da veri merkezi harcamaları 1.5 Trilyon Dolar’a ulaşmaktadır. Bu tutarın %75’i işletme masraflarına, %25’i ise veri merkezine ilişkin yeni projelere aktarılmıştır (Afyonluoğlu, 2014).

Şekil 2.6 Dünya’da Veri Merkezi Harcamaları



Kaynak: (IBM)

2014 yılında ise dünyada veri merkezi harcamalarının 3.8 Trilyon Dolara ulaşacağı tahmin edilmektedir (Stamford, 2014).

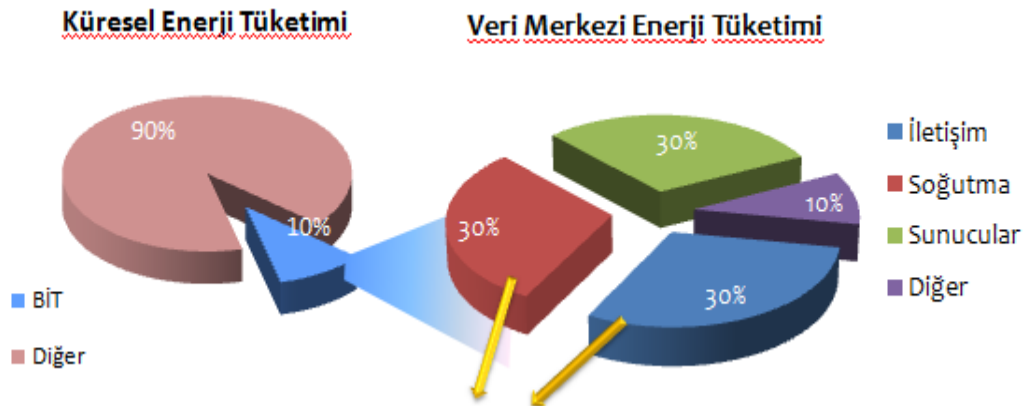
Tablo 2.3 Dünyada BT harcamalarının tahmini (Milyar Dolar)

	2013	2013	2014	2014
	Harcama	Büyüme (%)	Harcama	Büyüme (%)
Cihazlar	669	-1.2	697	4.3
Veri Merkezi Sistemleri	140	-0.3	143	2.6
Yazılım Yatırımları	300	5.2	320	6.8
BT Hizmetleri	922	1.8	963	4.5
Telekom Hizmetleri	1,633	-0.5	1,653	1.2
Toplam	3,663	0.4	3,777	3.1

Kaynak: (Stamford, 2014)

ABD Veri Merkezlerinde yılda 100 Milyar KWh elektrik (7.4 Milyar \$'lık enerji) tüketilmektedir. Dünyada IT tarafında tüketilen yıllık enerji 1.500 TeraWh'dır. Bu da toplam tüketimin %10'udur.

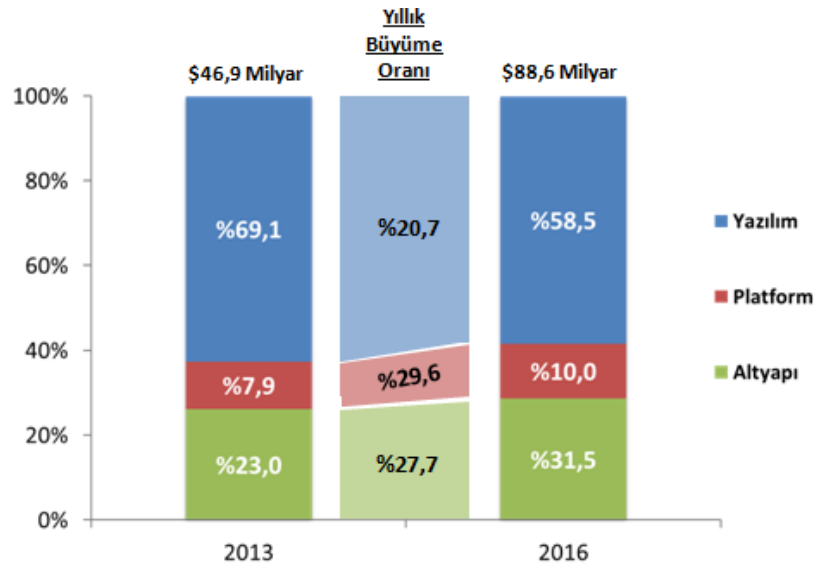
Şekil 2.7 Küresel Enerji Tüketimi ile Veri Merkezi Enerji Tüketimi



Kaynak: (U.S. Environmental Protection Agency, 2007)

Dünyada Bulut bilişim istatistiklerine baktığımızda, pazarın yıllık büyüme oranının %25'e varan bir hızla büyümesi öngörülmektedir. 2016 yılı verilerine baktığımızda, bulut bilişimde platform ve altyapı pazarlarında artış beklenmektedir.

Şekil 2.8 Dünyada Bulut Pazarı



Kaynak: (IDC,2012-2016)

2.2.1. Güney Kore Veri Merkezi ve Bulut Bilişim Yapısı

2.2.1.1. Güney Kore KEVM'nin Tanımı

2.2.1.1.1. Amaç

2000'li yılların başında, bakanlıklarda kurulan ve yönetilen e-Devlet sistemlerinde ve e-Devletin genişleme sürecinde, bilgi sistemlerinde gereksiz yatırımlar, güvenlik önlemlerinde eksiklikler ve kalitesiz bilgisayar ortamları gibi sorunlar ortaya çıkmıştır.

Kore devleti,

- Güvenlik saldırıları ve doğal afetlere karşı, sistematik bir şekilde müdahale stratejilerinin oluşturulması gerekliliği,

- İstikrarlı ve tutarlı hizmetler için taleplerin artması,
- Kurumlar arasındaki idari hizmet kalitesinde boşlukların oluşması,
- BT yatırım ve programlama işlemleri başına artan maliyete karşılık düşük verim elde edilmesi,
- Gereksiz yatırımlar,
- Sistem kullanımında farklılıklar,
- Yetersiz güvenlik düzeyi

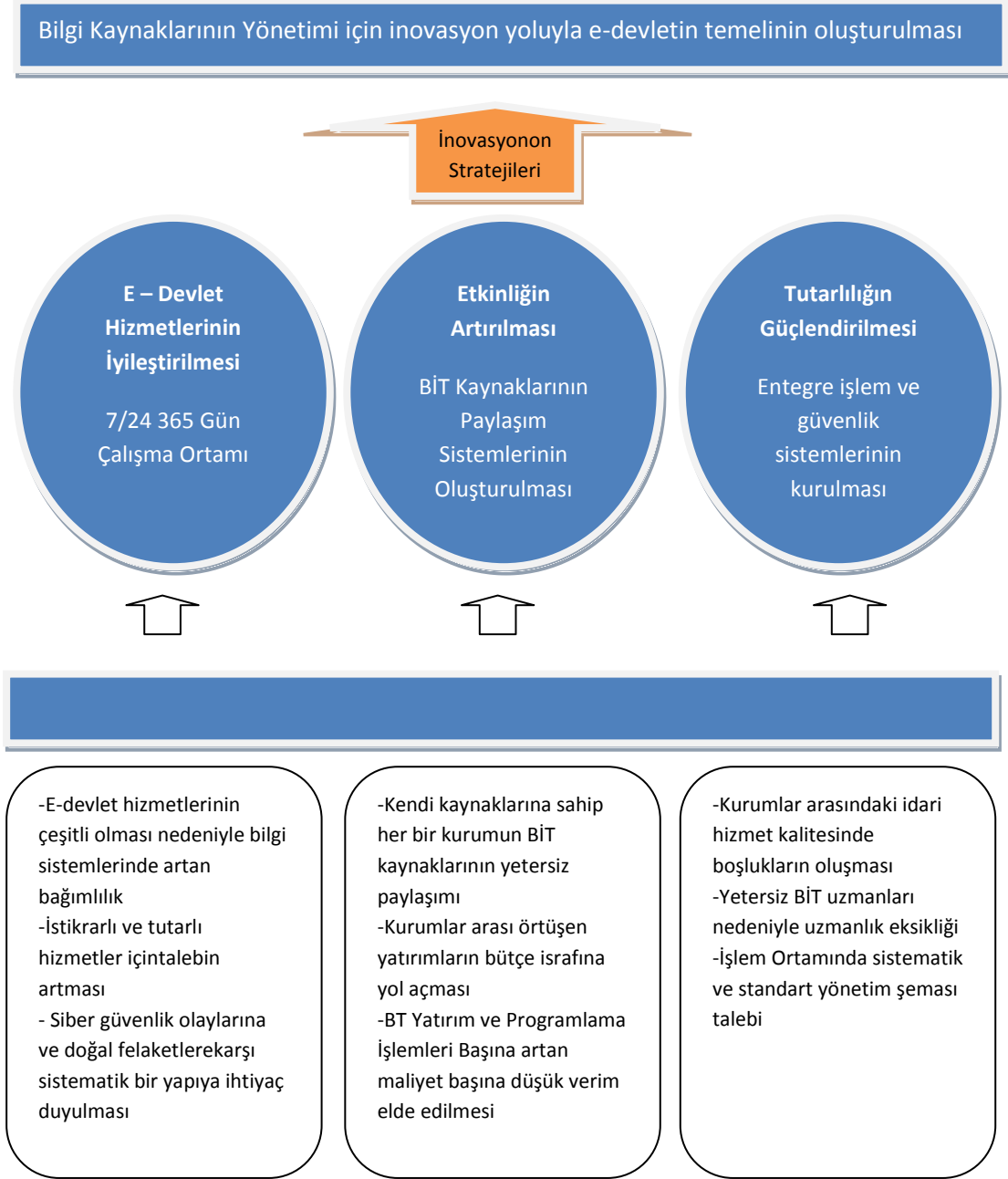
gibi amacı yukarıda belirtilen sorunların çözülmesi, güvenilir ve sürdürülebilir bir e-Devlet hizmeti verilmesi için 2003 yılında, dünyada ilk kez tüm kamu kurumlarına hizmet vermesi için Entegre Veri Merkezi'ni kurmuştur.

Güney Kore KEVM'nin kurulmasının amacı, BİT kaynakları yönetiminin inovasyonu ile e-Devlet için bir temel oluşturmaktır.

Veri merkezi kuruluşu için oluşturulan stratejiler;

- Halk için yönetim hizmetlerinin geliştirilmesi için 7/24/365 gün çalışma ortamının yaratılması,
- BİT kaynakları operasyonlarının, verimliliğinin artırılması için devlet içinde bilgi kaynaklarının geniş ölçüde paylaşımı için bir sistem kurulması,
- BİT kaynakları operasyonlarının tutarlılığının güçlendirilmesi için entegre işlem ve güvenlik sistemlerinin kurulması (e-Government of Korea,2011).

Şekil 2.9 Güney Kore KEVM Amaç ve Stratejiler Kavram Haritası



Kaynak: (e-Government of Korea,2011)

İnovasyon stratejileri dışında; bilgi sistemleri, bilgisayar olanakları ve insan kaynaklarını içeren BİT kaynaklarının paylaşım sistemi, bilgi koruma sistemleri ve

teknoloji birikiminde yoğun yatırım ile tam bir bilgi güvenliği sisteminin oluşturulması planlanmıştır.

Tablo 2.4 Güney Kore Veri Merkezi'nin Faydaları

GÜNEY KORE VERİ MERKEZİ	
KURULMADAN ÖNCE	KURULDUKTAN SONRA
Her bir kurumun kendi bilgi sistemlerinin kurması ve yönetimi	Milli BİT kaynaklarının tümleşik ve etkili yönetimi
BİT kaynakları ve sistemlerinde mükerrer yatırımlar nedeniyle milli BT bütçesinin yetersiz kullanımı	Ortak görev ve hizmetlerin entegre gelişimi ve BİT kaynaklarının paylaşımı ve toplu satın alma ile bütçe tasarrufu
Mesai saatleri dışında ve tatil günlerinde sistemin kesilmesi	7/24 izleme ve Bilgisayar Acil Müdahale Ekibi (CERT) ile siber tehditlere karşı ani karşılık verme
Özel grupların ve personelin yokluğunda siber tehditlere karşı savunmasız olması	7/24 izleme ve Bilgisayar Acil Müdahale Ekibi (CERT) ile ani savunma
İnsan kaynaklı hatalar ve doğal felaketlere karşı önleyici sistemin yetersiz olması	İş Sürekliliği Planı (BCP) kurularak felaketler için hazırlık yapılması

Kaynak: (e-Government of Korea,2011)

2.2.1.1.2. Tarihçe

Güney Kore Kamu Entegre Veri Merkezi'nin sistem gelişim süreci aşağıdaki gibidir:

FAZ 1: 2002-2004 PLANLAMA:

Stratejik planlar, bölümlerin ve uzmanların görüşleri alınarak ve diğer ülkelerle kıyaslanarak geliştirilmiştir.

- İş Sürecinin Yeniden Yapılanması (BPR) devletin bilgisayar ortamında verimli çalışmasını sağlamak için yapılmıştır.(2002)
- KEVM'nin kurulması, e-Devlet yol haritasınının 31 adımından biri olarak belirlenmiştir.(2003)
- Bilgi Stratejisi Planı (ISP) KEVM'nin kurulması için geliştirilmiştir. (2004)

FAZ 2: 2004-2006 KURULUM:

KEVM'nin kurulumu için master plan hazırlanmıştır. BİT için dünya standartlarında altyapı ve çalışma ortamı Daejeon ve Gwangju'da inşa edilmiştir.

- KEVM binası için tesisler yapılmış ve kamu içi iletişim ağı oluşturulmuştur. (2005)
- İlk KEVM, Daejeon'da kurulmuştur. (2005)
- İkinci KEVM'nin Gwangju'da kurulmasına karar verilmiştir. (2006)

FAZ 3: 2005-2007 YER DEĞİŞTİRME:

Her bir kurumda kurulan ve işletilen bilgi sistemleri KEVM'ne taşınmıştır.

- 25 kurumun bilgi sistemleri Daejeon Merkezi'ne taşınmıştır. (2006)
- Standart ve otomatik KEVM yönetim sistemi olan, Ulusal Yönetim Platformu Sistemi (nTops) geliştirilmiştir. (2006)
- İkinci KEVM, Gwangju'da kurulmuştur.(2007)
- 22 kurumun bilgi sistemleri Gwangju Merkezine aktarılmıştır.

FAZ 4: 2008- DEVAM EDEN SÜREÇ:

Mobil e-Devlet hizmetlerinin sağlanması ve bulut bilişime geçiş için toplu alım yapılması ile BİT kaynaklarının paylaşımı için;

- Kamu kurumları çapında bilgi işlem kaynaklarının birleştirilmesine başlanmıştır. (2008)
- Kamu Bulut Bilişim Platformu (G-bulut), uygulanmaya başlanmıştır.(2011)
- “e-ANSI” ile kapsamlı e-Devlet güvenli izleme sistemi kurulmuştur. (2011)
- Mobil e-Devlet Servis Destek Merkezi açılmıştır (2012) (e-Government of Korea, 2011).

2.2.1.1.3. KEVM Tanım

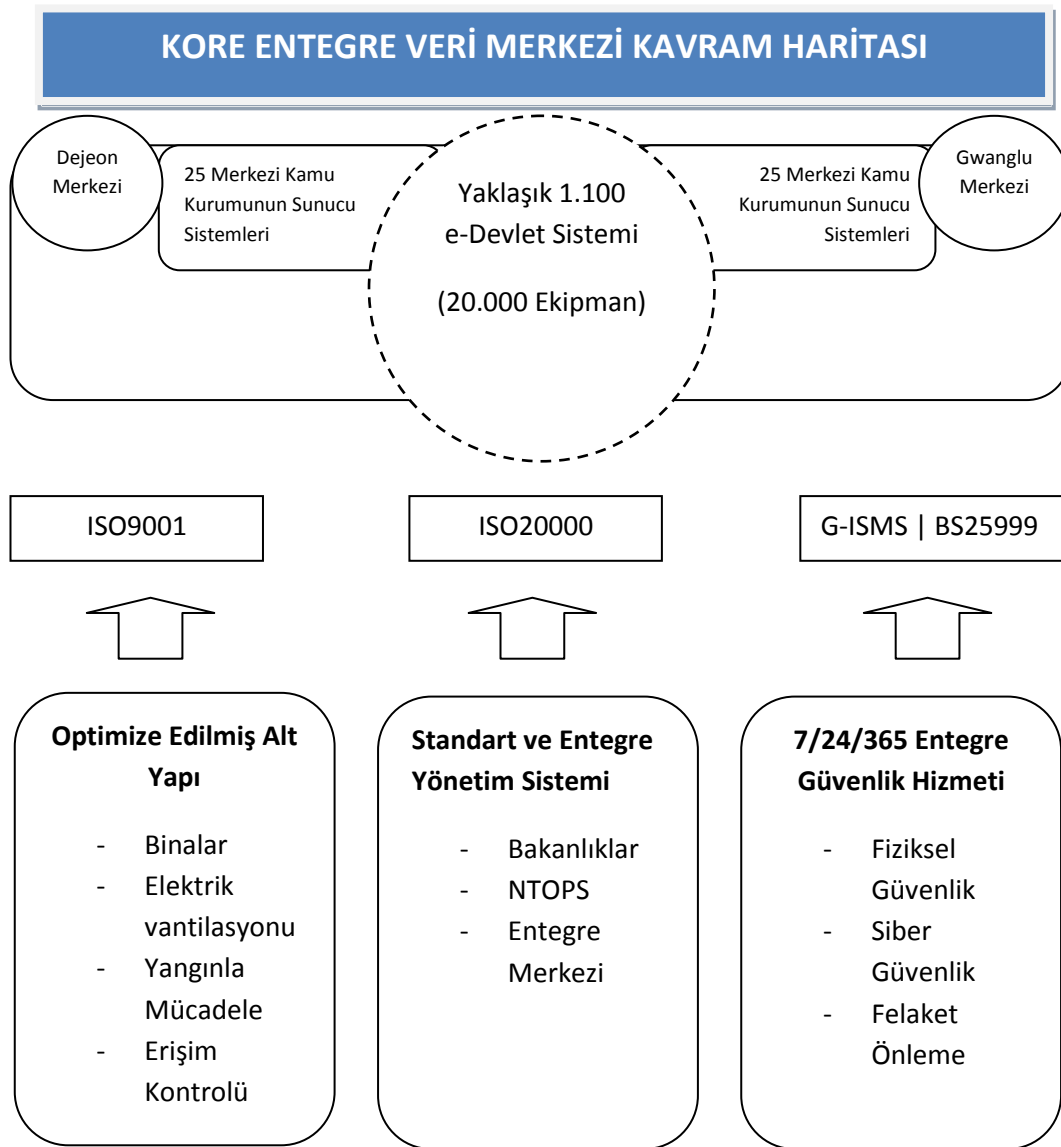
Kamu Entegre Veri Merkezi, konusunda uzmanlaşmış ve entegre bir şekilde elektronik bir ortamdaki iş süreçleri için gerekli her türlü BİT kaynaklarını sağlayan, sadece kamu için oluşturulmuş veri merkezidir.

Teknolojik altyapı ve Kore e-Devlet temel altyapısı olarak hizmet veren, Ulusal Bilişim ve Bilgi Ajansı (NCIA), KEVM'nin yönetiminden sorumludur.

- 47 merkezi kamu kurumları tarafından geliştirilmiş 1000'den fazla e-Devlet sistemlerini istikrarlı ve entegre bir şekilde yönetmektedir.

- e-Devlet hizmetlerini 7/24/365 gün kamuya kesintisiz bir şekilde sunmaktadır (e-Government of Korea, 2011).

Şekil 2.10 Güney Kore Kamu Entegre Veri Merkezi



Kaynak: (e-Government of Korea, 2011)

2.2.1.1.4. Önemli Özellikler

BİT Sistemlerinin Çalışması İçin Optimize Edilmiş Altyapı Tesisleri

- Çift güç kaynağı ve çift sistem ile Richter ölçeğinde 6.0 şiddetindeki depreme dayanacak şekilde tasarlanmıştır.

Ulusal Yönetim Platformu Sistemi, “nTops” Vasıtasıyla Ulusal Bilgi Kaynaklarının Entegre Yönetimi

- Devletin 47 kurum ve kuruluşuna ait 1.100’ü aşkın iş alanında, sunucu, depolama, network ve güvenlik ekipmanlarını içeren yaklaşık 20.000 bilgi sistemi birimi, BT hizmet yönetimi için uluslar arası standart olan, ISO 20000’e uygun bir şekilde yönetilmekte ve işletilmektedir.

Entegre Kurulum ve BİT Kaynaklarının Paylaşımı (Donanım, Yazılım, vs.)

- Devlet için BT ekipmanlarının toplu satın alınması yoluyla, BİT kaynakları havuzu oluşturulmuştur.
- BİT kaynaklarının paylaşımı ile bütçede %30 oranında tasarruf edilmiştir.

‘e-ANSI’, Güvenlik İzleme Sistemi ile Dış Tehditlere Karşı E-Devlet Hizmetlerinin Korunması

- Hacking (bilgisayar korsanlığı), virüs gibi siber tehditlere ve fiziksel hasara karşı e-Devlet hizmetlerini korumak için, entegre güvenlik yönetim sistemi kurulmuştur.

İş Sürekliliği Planı ve Felaket Kurtarma Sisteminin Kurulmasıyla, Doğal Afetler veya İnsan Kaynaklı Afetlere Karşı Temel Yönetim Hizmetlerinin Sağlanması

- BT tabanlı kamu yönetimi için yedekleme ve kurtarma hedeflerinin belirlenmesi ve detaylandırılması ile iş sürekliliği yönetimi için uluslararası bir standart olan BS25999'a dayanan sistemler kurulmuştur.

'K-net' ile Sadece Devlet İçin, İstikrarlı ve Ekonomik Bir İletişim Ağının Sağlanması

- K-net'i kullanan kurum sayısı yaklaşık 700'dür (2011) (e-Government of Korea, 2011).

2.2.1.2. Güney Kore Veri Merkezi'nde Verilen Önemli Hizmetler

2.2.1.2.1. E-Devlet Sistemlerinin Entegre Yönetimi

Sunucu, depolama, ağ ve güvenlik donanımları dahil olmak üzere kamu kurumlarının bilgi kaynaklarının entegre bir şekilde işletilmesi ve yönetimi sağlanmaktadır.

E-Devlet sistemlerinin entegre yönetimi aşağıdaki konuları kapsamaktadır:

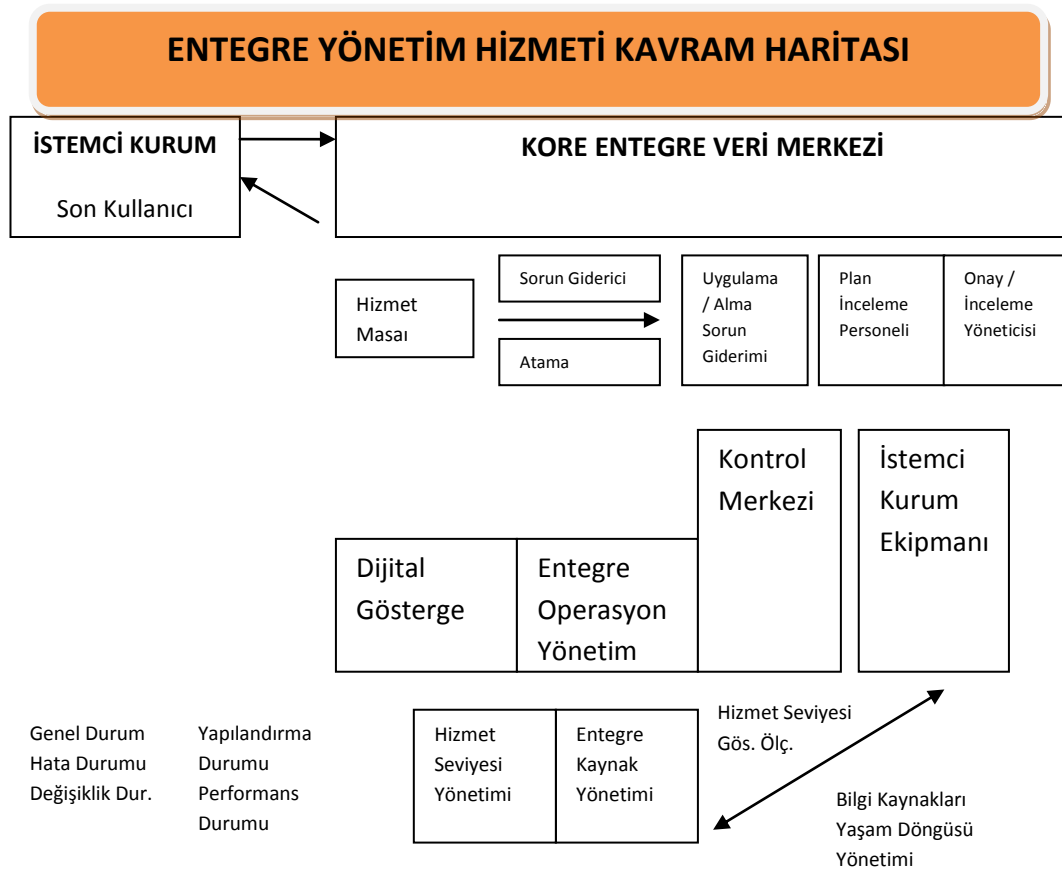
- Her bakanlığın bilgi kaynaklarını yönetmek için ITIL'a dayalı standart operasyon prosedürlerinin oluşturulması ve tasarımı,
- Entegre yönetim için bir araç olan Ulusal Yönetim Platformu Sistemi "nTOPS"un kullanılması ve geliştirilmesi ile entegre bir şekilde devlet sistemlerinin yönetilmesi,
- Hizmet Seviyesi Anlaşması (SLA)'na göre hizmet seviyesinin ölçülmesi ve yönetilmesi.

E-Devlet sistemlerinin entegre yönetimi fonksiyonları; hizmet masası, dijital gösterge paneli, kontrol birimleri (sunucu, ağ, siber saldırı), servis seviyesi yönetimi, entegre kaynak yönetimi ve bilgi yönetimi portalıdır.

E-Devlet sistemlerinin entegre yönetimi aşağıdaki özelliklere sahiptir:

- Entegre sistem yönetimi için ITIL'a dayalı standartların ve Ulusal Yönetim Platformu Sistemi "nTOPS"un kullanılması ve geliştirilmesi,
- BT hizmet yönetimi için ISO 20000 sertifikasına sahip olunması (e-Government of Korea, 2011).

Şekil 2.11 Entegre Yönetim Hizmeti Kavram Haritası



Kaynak:(e-Government of Korea, 2011)

2.2.1.2.2. E-Devlet Sistemlerinin Entegre Güvenlik Yönetimi

Entegre Güvenlik Yönetimi ile fiziksel ve siber tehditlere karşı bilgi sistemleri korunmaktadır.

E-Devlet sistemlerinin Entegre Güvenlik Yönetimi aşağıdaki konuları kapsamaktadır:

- Fiziksel güvenlik sistemi;
 - Çift güvenlik duvarı, CCTV, araç giriş kontrolü ve 24 saat kontrol edilmesi
 - Tehlikeli maddelerin ve depolama cihazlarının elle yüklenmesi/ bırakılması yasaklanarak, yasak bölgelerin oluşturulması, kimlik kartı ve biyometrik tanımlama sistemi ile giriş kontrolünün güçlendirilmesi
- Siber tehdit yönetimi sistemi;
 - DDoS ve bilgisayar korsanlığı gibi dış saldırıların engellenmesi ve tespiti için yapı tasarımı
 - Bilgi sistemlerinin kontrolü ve zayıf noktalarının ortadan kaldırılması dahil olmak üzere siber saldırıları önleme ve takip yönetimi sağlayan güvenlik yönetiminin, 7/24/365 gün uygulanması
- Bilgi sistemi erişim kontrolü;
 - Kullanıcı kimlik doğrulaması ve veri tabanı kodlama aracılığıyla sistemlerin, veri ve ağların korunması

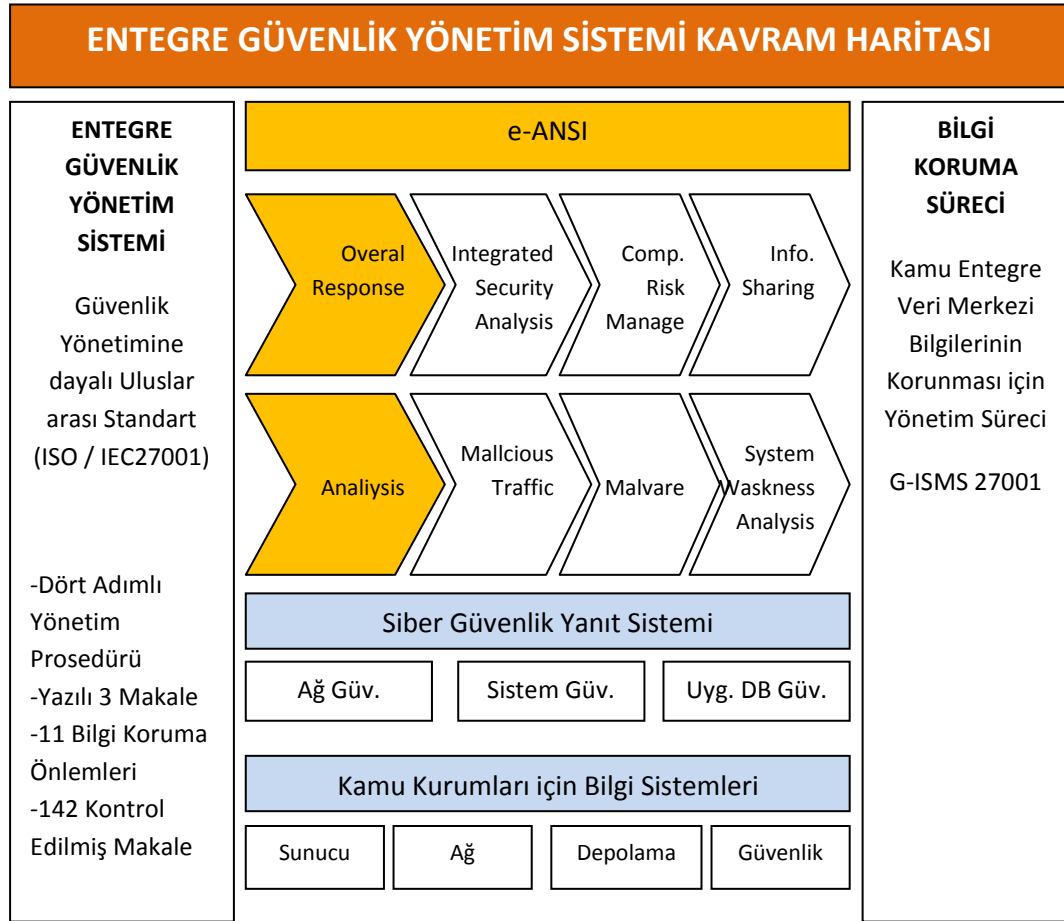
E-Devlet sistemlerinin entegre güvenlik yönetimi fonksiyonları aşağıdaki gibidir:

- 8 Katmanlı Savunma Sistemi: DDoS azaltma sistemi, anti-spam/virus sistemi, saldırı önleme sistemi, saldırı tespit sistemi, siber koruma, web güvenlik duvarı, sunucu güvenliği ve DB güvenlik
- 4 Sınıf Analiz Sistemi: Zararlı Yazılım Analizi, zararlı trafik analizi, zayıflık analizi ve entegre güvenlik analizi

E-Devlet sistemlerinin entegre güvenlik yönetimi aşağıdaki özelliklere sahiptir:

- Fiziksel güvenlik, siber güvenlik ve erişim kontrolünü içeren kapsamlı güvenlik yönetim sistemi, Elektronik Gelişmiş Milli Güvenlik Altyapısı (e-ANSI)'nın kurulması,
- Kamu Bilgi Güvenliği Yönetim Sistemi (GISMS) sertifikasının elde edilmesi. (e-Government of Korea, 2011).

Şekil 2.12 Entegre Güvenlik Yönetim Sistemi Kavram Haritası



Kaynak: (e-Government of Korea, 2011)

2.2.1.2.3. Entegre Bilgi Teknolojileri Kaynakları Yönetimi

Yazılım ve donanım gibi BT kaynaklarının toplu alımı planlanmakta ve uygulanmaktadır.

Entegre BT kaynakları yönetimi aşağıdaki konuları kapsamaktadır:

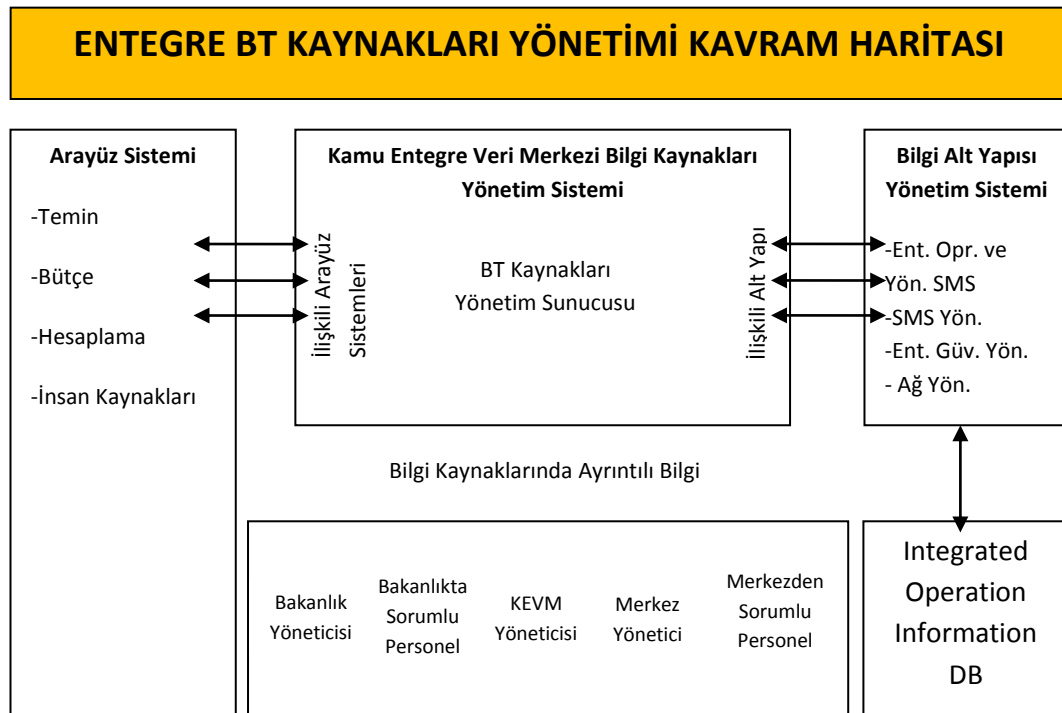
- Devletin çeşitli BT kaynaklarını sistematik bir şekilde yöneten BT kaynakları yönetim sistemi,
- BT kaynaklarının her aşamasında yönetim süreci,

- Sadece devlet için BT Kaynak Havuzu oluşturularak etkin kaynak tahsisi.

Entegre BT kaynakları yönetiminin özellikleri;

- BT kaynaklarının her aşamasında entegre yönetimin sağlanması (planlama-satın alma→ bekleme-tahsis→kullanım-yönetim→kaldırma-yenileme)
 - Yinelenen yatırımların önlenmesi, BT kaynaklarının etkili bir şekilde dağıtılması ile yatırım verimliliğinin artırılması sağlanmıştır.
- Sanallaştırma ve otomasyon teknolojisi kullanılarak, BT kaynaklarının geliştirilmesi ve dönüşümün kolaylaştırılması için bulut bilişim (G-bulut) teknolojisi kullanılmıştır (e-Government of Korea, 2011).

Şekil 2.13 Entegre BT Kaynakları Yönetim Kavram Haritası



Kaynak: (e-Government of Korea, 2011)

2.2.1.2.4. Özel Kamu İletişim Ağı

Özel Kamu İletişim Ağı'nın kurulması ve bütün kamu kurumlarında uygulanması amaçlanmıştır.

Özel Kamu İletişim Ağı'nın konuları aşağıdaki gibidir:

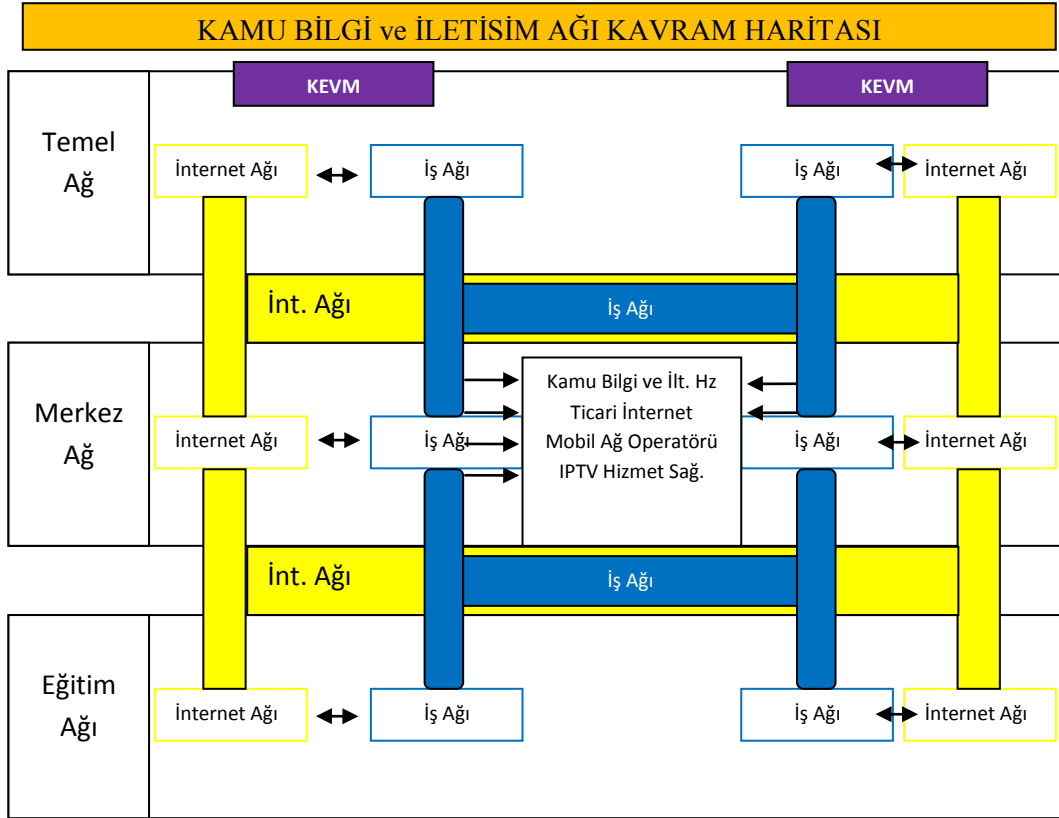
- Ticari ağlardan ayrı bir şekilde sadece kamu içi iletişim ağı olan "K-net"nin kurulması,
- İş ağı ile internet ağını ayıran güvenlik seviyesinin artırılması,
- Çift yönlü ve ikili iletişim cihazları, gönderme kanalı ve 7/24 izleme sisteminin kurulması ile güvenliğin sağlanması,
- IPTV, IPv6 ve UBcN (Ultra Genişbant Yakınsama Ağı) gibi yeni teknolojilerin etkili bir şekilde uygulanması.

Özel Kamu İletişim Ağı'nın fonksiyonları; temel ağ hizmeti (ATM, özel hat, Ethernet, İnternet) ve VoIP hizmetidir.

Özel Kamu İletişim Ağı'nın özellikleri aşağıdaki gibidir:

- Merkezi kamu kurumları, yerel yönetimler ve kamu kurumları için güvenli ve ölçeklenebilir iletişim hizmetinin sunulması,
- İletişimin kalitesi ve dengelenmesine ilişkin SLA'nın uygulanması ile kaliteli hizmetin sağlanması (e-Government of Korea, 2011).

Şekil 2.14 Kamu Bilgi ve İletişim Ağı Kavram Haritası



Kaynak: (e-Government of Korea, 2011)

2.2.1.2.5. Veri Merkezi Yönetimi için En Uygun Ortam

E-Devlet sistemlerinin istikrarlı çalışmasını sağlayan optimum altyapının oluşturulması amaçlanmıştır.

Veri merkezi altyapısının özellikleri aşağıdaki gibidir:

- 100 kg/m² üzerindeki yüklere ve Richter ölçeğinde 6.0 şiddetindeki depremlere dayanabilen veri merkezi binalarının tasarlanması,
- Kesintisiz güç kaynağı için UPS, piller ve jeneratörlerden oluşan çift güç kaynağı ekipmanlarına sahip olması,

- Giriş kontrolü ve 24 saat izleme yoluyla dış fiziksel tehditlerin engellenmesi,
 - Biyometrik tanımlama sistemi, CCTV, kimlik kartı ve merkezin 24 saat izlenmesi ile erişim kontrolünün sağlanması,
- Sabit ve uygun sıcaklık ile nemin korunması için havalandırma sisteminin kurulması, (25±2°C, %30~50)
- Otomatik yangın ve duman kaçağı algılama sistemi ile yangın söndürme ekipmanlarına sahip olmasıdır.

Veri merkezi altyapısının fonksiyonları; güç kaynağı yönetimi sistemi, yangın güvenlik yönetim sistemi, havalandırma yönetimi sistemi, erişim kontrol sistemi, akıllı bina sistemi (IBS), CCTV, UPS, piller, jeneratörlerdir (e-Government of Korea, 2011).

Şekil 2.15 Veri Merkezi Alt Yapı Yönetimi Kavram Haritası



Kaynak: (e-Government of Korea, 2011)

2.2.1.2.6. İş Sürekliliği Garanti Hizmeti

Doğal afetlerde dahil kesintisiz stabil BT tabanlı kamu hizmetinin verilmesi amaçlanmıştır.

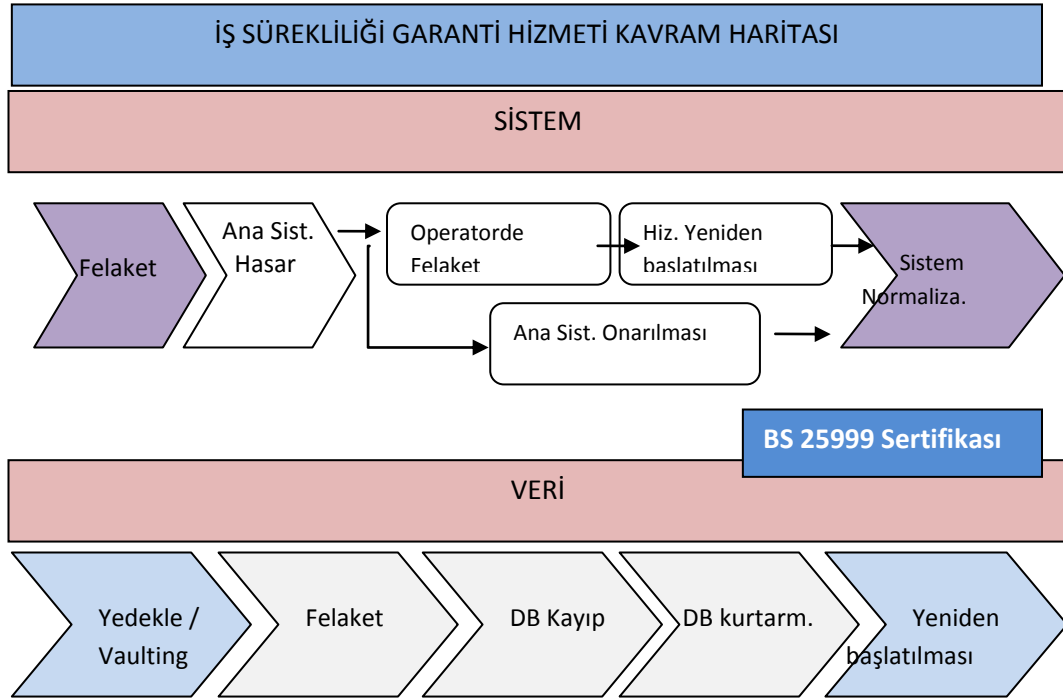
İş Sürekliliği Garanti Hizmeti kapsamında yapılması gerekenler aşağıdaki gibidir:

- Felaket (yangın, deprem, kesinti, terör, vb.) durumlarında müdahale prosedürlerinin ayrıntılı bir şekilde açıklanması ile İş Sürekliliği Planı (BCP)'nın formüle edilmesi,
- İşlem hatalarına hazırlıklı olunması için sunucu, depolama, ağ ve güvenlik ekipmanları gibi önemli sistemlerin dualize edilmesi,
- Veri yedekleme, geçiş sistemi ve Felaket Kurtarma Sisteminin (DRS) oluşturulması,
- Düzenli olarak afet tatbikatlarının düzenlenmesi

İş sürekliliği garanti hizmetinin fonksiyonları; felaket kurtarma sistemi, çevrimiçi geçiş sistemi, entegre yedekleme sistemi ve BCP yönetim sistemidir.

Afetlere karşı hazırlık yapılmasında, iş sürekliliği sistemi için BS25999 sertifikası alınmıştır (e-Government of Korea, 2011).

Şekil 2.16 İş Sürekliliği Garanti Hizmeti Kavram Haritası



Kaynak: (e-Government of Korea, 2011)

2.2.1.2.7. Kamu Platformu Paylaşım Hizmeti

Kamu Platformu Paylaşım hizmeti, Bakanlıklar tarafından kullanılan modüler platformların, geliştirilmesi ve sunulması hizmetlerini kapsamaktadır.

Geçerliliği sağlanmış standart bir platform ile e-Devlet hizmetinin geliştirilmesi için devlet kurumlarına destek verilmektedir.

Kamu Platformu Paylaşım hizmetine dahil olan hizmetler aşağıdaki gibidir:

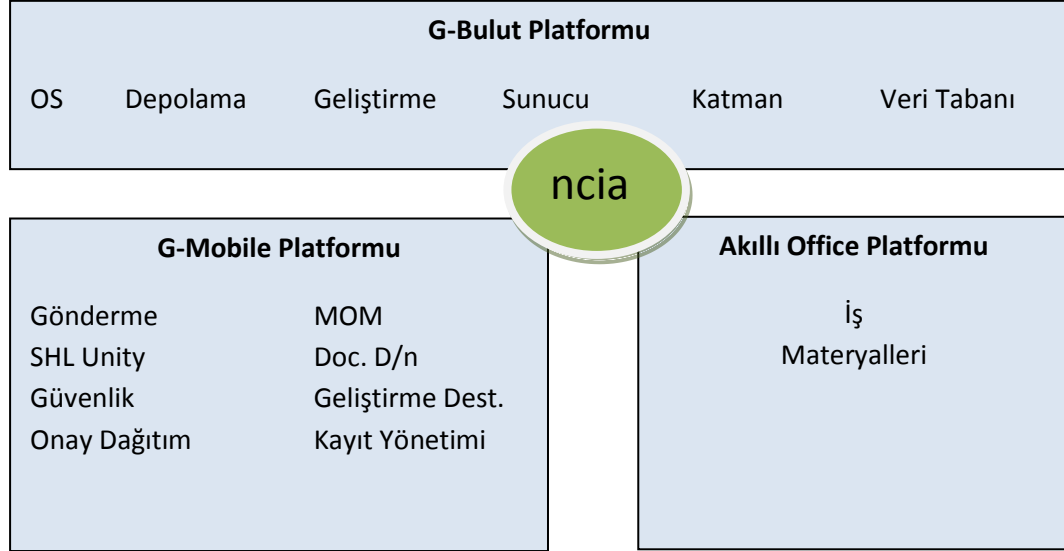
- G-Bulut Platform Hizmeti
 - Sanallaştırılmış bir ortamda sunucu, depolama ve ağ kurulumu ve gerektiğinde kamu kurumlarında sağlanması,

- Operasyon ve bakımı kolaylaştırmak için e-Devlet çerçevesinde hizmet verilmesi,
- G-Mobil Platform Hizmeti
 - Kamu mobil hizmetinin geliştirilmesi için ortak sistemlerin ve test ortamının oluşturulması,
 - Mobil uygulamaların veya web'in geliştirilmesi için gerekli olan temel sistemlerin (bağlantı, güvenlik, kimlik doğrulama) sağlanması,
- Akıllı Ofis Platformu Hizmeti
 - Mobil çalışanların esnek çalışması için akıllı bir ofis ortamının tasarlanması ve yapımı,
 - Bulut PC altyapı mimarisi tasarımı ve kurulumu,

Kamu Platformu Paylaşım hizmetinin fonksiyonları:

- G-Bulut: operasyon yönetimi-denetim çözümü, işlem otomasyon çözümü ve ölçme çözümü,
- G-Mobil: Mobil destek merkezi, uygulama veya web geliştirme sistemi, işlem otomasyon çözümü,
- Akıllı Ofis: yönetim otomasyon çözümü, donanım altyapısı ve VDI çözümüdür (e-Government of Korea, 2011).

Şekil 2.17 Kamu Platformu Paylaşım Hizmeti



Kaynak: (e-Government of Korea, 2011)

Ayrıca, hem kamu, hem de bilişim sektörünü destekleyecek olan bulut tabanlı bir altyapı oluşturmak amacıyla Güney Kore İletişim Komisyonu'nun Bilgi Ekonomisi Bakanlığı ve Kamu Yönetimi ve Güvenliği Bakanlığı ile işbirliği halinde, 500 milyon ABD doları tutarında bir yatırım bütçesi ayırdığı ifade edilmektedir. Söz konusu inisiyatifin, 2014 yılına kadar kamu BİT harcamalarında %50 tasarruf sağlanması ve ülkede bulut bilişim sektörünün gelişimine katkıda bulunulmasının yanı sıra, yerli işletmecilerin ülke dışına hizmet sunacak seviyeye gelmesine katkıda bulunarak ülkenin küresel bulut bilişim pazarının %10'una sahip olma hedefini de destekleyeceği öngörülmektedir (Mirzaoğlu, 2011).

2.2.1.3. Sistemin Başarısı

2.2.1.3.1. Önemli Başarılar

Güney Kore KEVM ile 2010 yılında toplam 550 milyon \$ tasarruf edilmiştir.

Şekil 2.18 Güney Kore KEVM Kazanımları

TASARRUF BAŞLIĞI	Merkezileşme Öncesi	Entegre Veri Mrk Kurulunca
Ortalama Kesinti Süresi	67 Dakika	4,8 Saniye
Siber Saldırı Hafifletme Süresi (Ayda 62.000 Saldırı)	---	20 Saniye
Maliyet Tasarrufu	-	%30
Enerji Tasarrufu	---	3.75 MW/saat
Çevre Kazanımı	---	30 Ton/Yıl CO ₂
BT Ürün Satınalma Tasarrufu	---	112 Milyon \$
Hizmet Müşteri Memnuniyeti	%64	%90,4
Satınalma ve Bakım Tasarrufu	---	%30
Uluslararası Sertifikasyon	---	ISO20000, 9010, 25999, G
Siber Güvenlik Altyapısı	7.000 Kural	13.000 Kural
Sunucu Sayısı Azaltılması	1994 Sunucu	315 Sunucu Kamu bulutu, Büyü kveri
Sağlanan Platformlar	---	51 Ülke
Okyanus Ötesi Ziyaretler	4 Ülke, 43 Ziyaretçi	450 Ziyaretçi
Projelere KOBİ Katılımı	%26,8	%55,7
Siber Saldırı Önleme Katmanları	0	8 (e-ANSIS)

Kaynak: (NCIA, 2012)

KEVM'nin kurulmasından sonraki 7 yıl içerisinde, yatırım getirisinin sürekli artmasıyla yatırım karşılanmıştır.

- Güvenlik, operasyon, kaynak entegrasyon, bakım alanlarında da yatırımın getirisini yükselmektedir.

Şekil 2.19 TCO/ROI Analizi



Kaynak: (e-Government of Korea, 2011)

Şekil 2.20 Alanlara Göre ROI



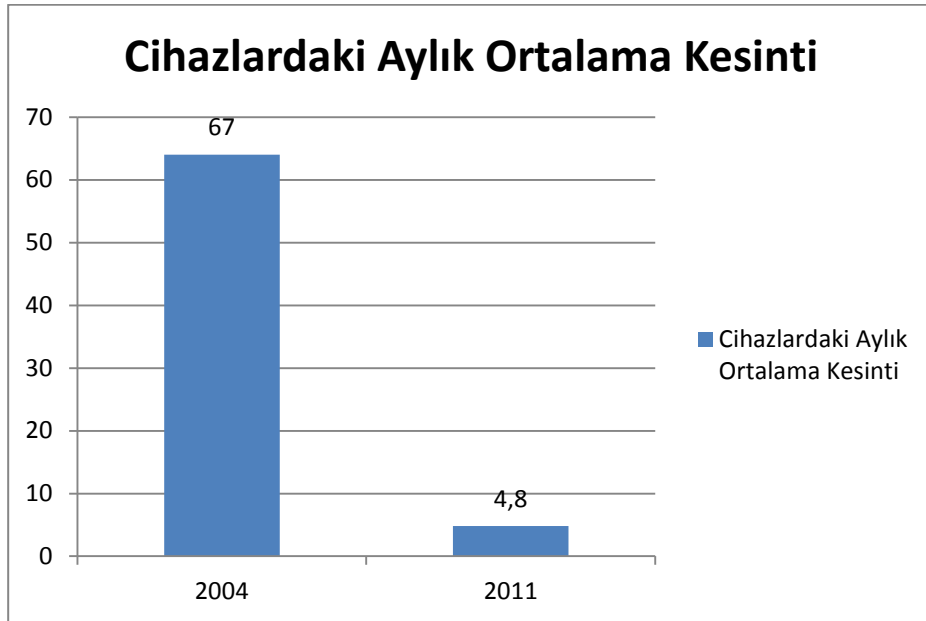
Kaynak: (e-Government of Korea, 2011)

Sistem yönetiminin istikrarının sağlanması ve müşteri memnuniyetinin geliştirilmesi için,

- Bilgi teknolojileri cihazlarındaki kesinti azaltılarak; cihazlardaki aylık ortalama kesinti 2004 yılında 67 dakika iken 2011 yılında 4.8 saniyeye düşmüştür.
- Kullanıcı kurumlar ile yapılan hizmet seviyesi sözleşmesi ile kaliteli hizmetin sunulmasıyla, kullanıcı kurumların memnuniyet derecesi 2006

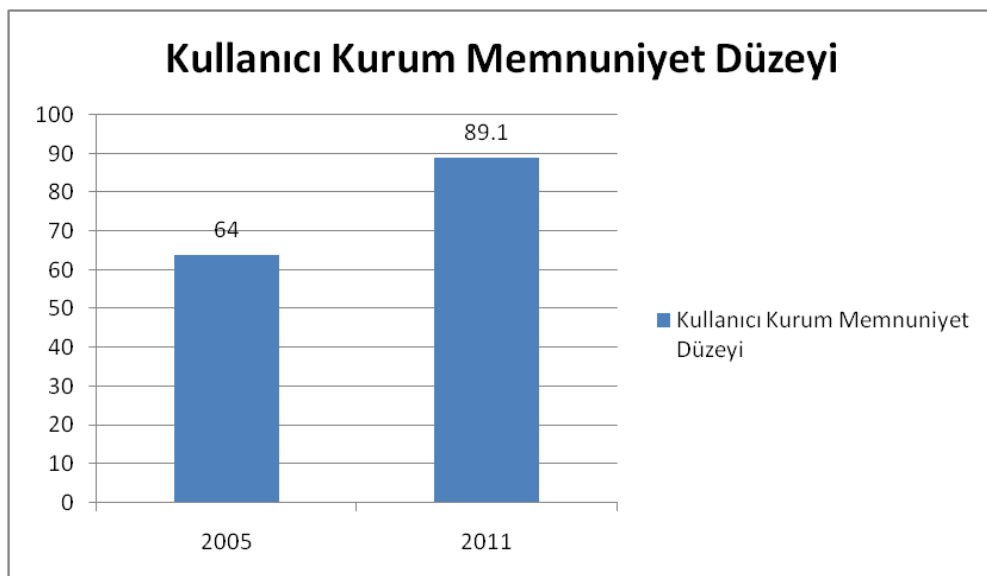
yılında 64 Puan iken 2011 yılında 89.1 Puan olmuştur (e-Government of Korea, 2011).

Şekil 2.21 Cihazlardaki Aylık Ortalama Kesinti



Kaynak:(e-Government of Korea, 2011)

Şekil 2.22 Kullanıcı Kurum Memnuniyet Düzeyi

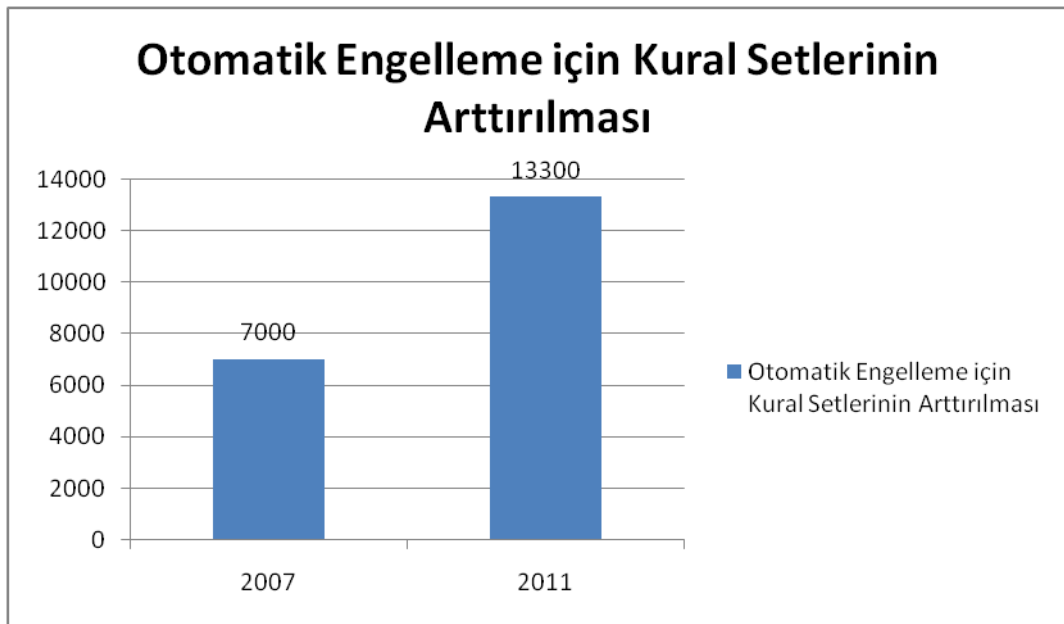


Kaynak:(e-Government of Korea, 2011)

Siber saldırıların önlenmesi ve iş sürekliliği planının güçlendirilmesi konularında;

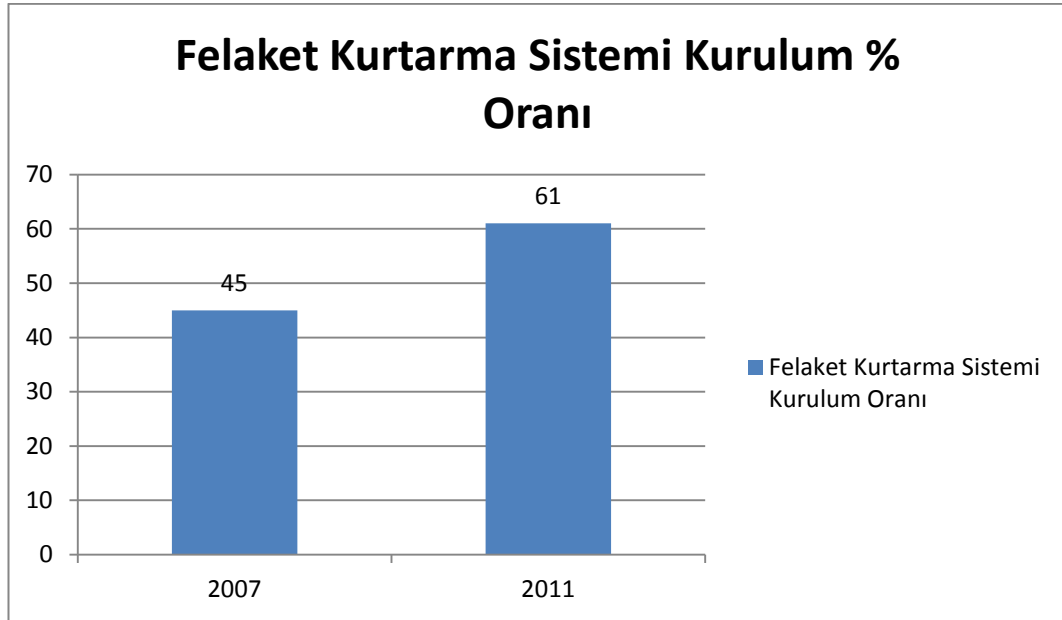
- Dışarıdan gelen saldırıların otomatik olarak algılanması ve engellenmesi için kural setleri geliştirilmiştir. 2007 yılında yaklaşık 7.000 kural-seti varken, 2011 yılında yaklaşık 13.300 kural seti oluşturulmuştur. Kural setleri kullanılarak saldırı girişimleri % 99'un üzerinde kesilmiştir.
 - DDoS saldırıları saptanarak engellenmiş ve 10 dakika içinde bilinmeyen saldırılara kural setleri uygulanmıştır (e-Government of Korea,2011)

Şekil 2.23 Otomatik Engelleme İçin Kural Setlerinin Artırılması



Kaynak:(e-Government of Korea, 2011)

Şekil 2.24 Felaket Kurtarma Sistemi Kurulum Oranı

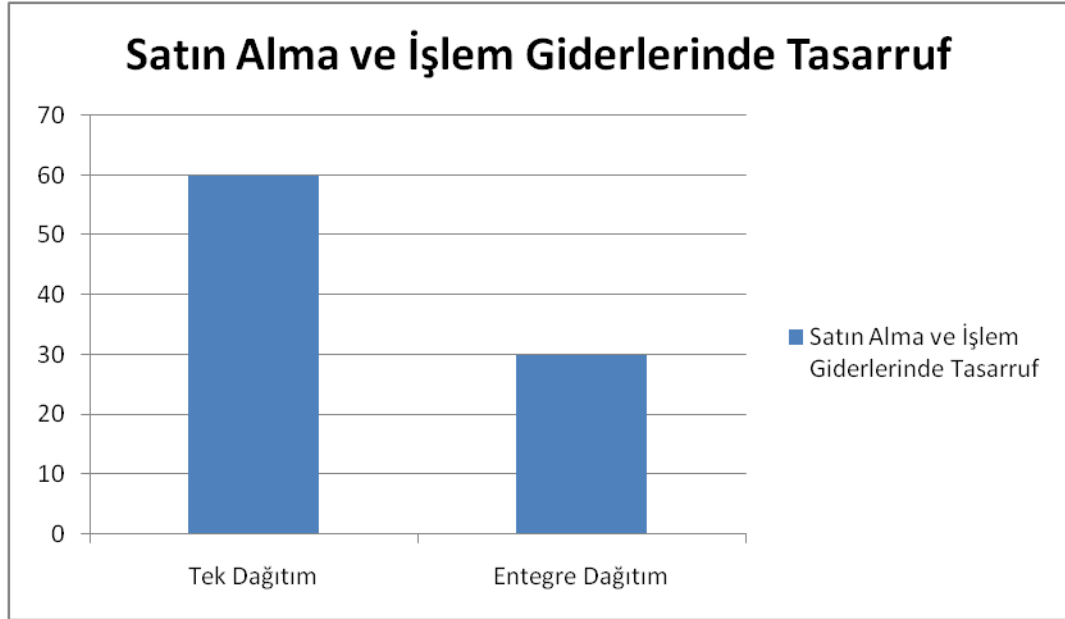


Kaynak:(e-Government of Korea, 2011)

Bakanlıkların BİT kaynakları entegre edilerek bütçe tasarrufu sağlanmış ve yeşil veri merkezleri oluşturulmuştur. Bu kapsamda;

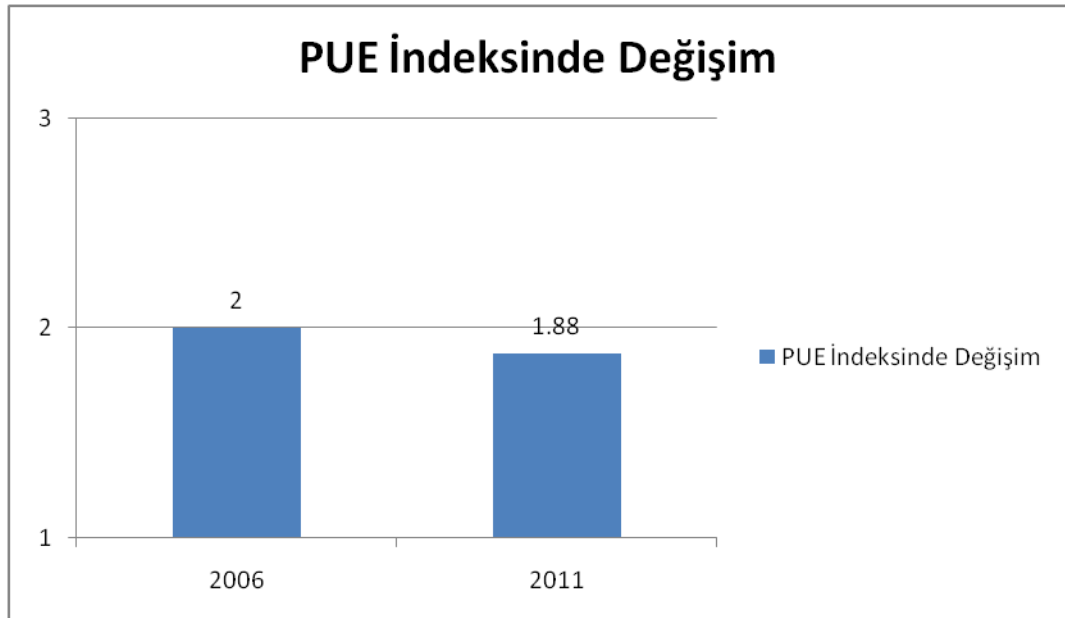
- BİT kaynaklarının işletilmesi ve satın alınması için Bakanlıkların bütçesi, BİT kaynaklarının entegre dağıtımı ile %30 oranında azalmıştır.
- Sistem kurulum alanında tasarruf ve enerji verimliliğinin geliştirilmesi ile Güç Kullanımı Etkinliği İndeksi (PUE) 2006 yılında 2.0 iken 2011 yılında 1.88 olmuştur.
- PUE 1.7 ile 1.9 arasında olduğu zaman 5 seviye arasında 2. seviyede veri merkezi “çok iyi” olarak sınıflandırılır (e-Government of Korea, 2011).

Şekil 2.25 Satın Alma ve İşlem Giderlerinde Tasarruf



Kaynak:(e-Government of Korea, 2011)

Şekil 2.26 PUE İndeksinde Değişim



Kaynak:(e-Government of Korea, 2011)

Çift taraflı büyüme ve yurt dışı pazarın geliştirilmesi için bilişim şirketleri desteklenmiştir. Bu kapsamda;

- NCIA projelerinde kobilerin katılımının artırılması için,
 - İlgili projede yazılım satın alımının ayrılması ve bir takım kobilerden oluşan konsorsiyuma ikramiye verilerek NCIA projelerinde daha çok kobinin teşvik edilmesi sağlanmıştır. Kobilerin katılım oranı, 2010 yılında %26.8 iken 2011 yılında %44.5 olmuştur.
- Yabancı devletlerle işbirliğinin teşvik edilmesi ve Kore Entegre Veri Merkezi ilgili çözümlerin ihraç edilmesi ile yurtdışı pazarlarının geliştirilmesi için bilişim şirketleri desteklenmiştir.
 - Moğolistan, Nepal ve Vietnam'a, Güney Kore Kamu Entegre Veri Merkezi Modeli ihraç edilmiştir.
 - Yıllık yabancı ziyaretçi sayısı, 2007 yılında 4 ülkeden 43 kişi iken 2011 yılında 62 ülkeden 335 kişi olmuştur (e-Government of Korea, 2011).

2.2.1.3.2. Uluslararası Toplumlardaki Etkisi

Birleşmiş Milletler (BM) tarafından 2 yılda bir yayımlanan E-Devlet Değerlendirme Raporu'na göre (Ulusal Bilgi Toplumu Ajansı, [NIA], 2011); Güney Kore 2010 yılında gerek e-Devlet hizmetlerinin gelişmişlik düzeyi, gerekse vatandaşların e-Devlet hizmetlerine katılımı yönünden BM üyesi ülkeler arasında ilk sırada yer almıştır. Güney Kore ayrıca Uluslararası Telekomünikasyon Birliği (ITU) tarafından 2 yılda bir yayımlanan Bilgi Toplumu Değerlendirilmesi Raporu'na göre (ITU, 2011) ise; 2008 ve 2010 yıllarında BİT'in gelişmişlik düzeyi ve BİT kullanım oranı bakımından ITU üyeleri arasında ilk sırayı elde etmiştir (Mirzaoğlu, 2011).

Güney Kore Veri Merkezi'nin uluslararası alanda almış olduğu ödüller;

- Kore Bilgi Teknolojileri Hizmet Yönetimi Forumu, "BT Yönetişim Mükemmellik Ödülü" (2011)
- "Veri Merkezleri" kategorisinde FutureGov Ödülü (2010)
- En iyi Demo, Stant Ödülü (2009) (e-Government of Korea, 2011).

Veri merkezi sertifikaları ve standartları;

- G-ISMS: Devlet Bilgi Güvenliği Yönetim Sistemi Sertifikası (2010)
- İş sürekliliği yönetimi, BS25999 standardı (2010)
- BT-tabanlı altyapı yönetimi standardı, ISO9001 (2009)
- BT hizmet yönetimi standardı, ISO20000 (e-Government of Korea, 2011).

2.2.1.3.3. Küresel Birliktelik

ODA projeleri birlikte Güney Kore KEVM modelinin ihracatı teşvik edilmiştir. Bu kapsamda, Güney Kore KEVM modelinin, Moğolistan ve Nepal’da kurulumu tamamlanmış olup, Vietnam’da kurulum süreci devam etmektedir. Endonezya, Kenya ve Filipinler’de Güney Kore KEVM modelinin alınması için görüşmeler devam etmektedir.

Karar verme, kurulma ve operasyon süreçlerinde gereken bilgilerin sağlanması için çalışma turları, danışmanlık ve proje fizibilite çalışmaları desteklenmektedir (e-Government of Korea, 2011).

2.2.2. İngiltere Veri Merkezi ve Bulut Bilişim Yapısı

İngiltere’de, kamu sektöründe bulut bilişim modelinin kullanılması 2009 yılında yayımlanan Dijital İngiltere Raporunda (BIS ve DCMS, 2009), “Kamu bulutu” (G-Bulut) adlı bir programın uygulanması önerilerek, teşvik edilmiştir. İlk kez bu rapor ile gündeme gelen G-Bulut programı, 2010 yılında yayımlanan Kamu BİT Stratejisinde detaylandırılmıştır (Mirzaoğlu, 2011, s.61-62).

Raporun söz konusu bölümünde, bulut bilişim kısaca tanımlanmakta ve bulut bilişim yaklaşımı kullanılarak kamu hizmetleri ağına özel sektör uygulamalarının da eklenmesi suretiyle G-Bulut olarak nitelendirilen özel bir kamu bulutu oluşturulması gerektiği belirtilmektedir.

Kamu BİT Stratejisinde 2013-2014 itibarıyla yıllık kamu harcamalarında 3,2 milyar sterlin tasarruf sağlanması hedeflenmiş ve bu hedefe ulaşmak amacıyla;

- SaaS, PaaS ve IaaS hizmet sunum modellerinin tümünü ihtiva edecek olan G-Bulut’un gerçekleştirilmesi,
- Kamu kurumlarının kullandıkça ödeyebilecekleri yazılım uygulamalarını barındıran ABD’nin “Apps.gov” benzeri bir “Kamu Yazılım Uygulamaları

Mağazası'nın Kamu BT tedarikinde SaaS modelini uygulamaya koyarak, oluşturulması,

- Merkezi G-Bulut veri merkezlerinde saklanan yazılım uygulamalarının, mevcut durumda kamu kurumlarının benzer birimlerinin ihtiyaçlarına hizmet eden benzer yazılımlar satın aldıkları veya benzer BT altyapıları oluşturdukları gerçeğinden hareketle, farklı kamu kurumları tarafından paylaşılması sayesinde BT yazılım yatırımlarının azaltılması,
- Mevcut durumda 8.000 adet olan kamu veri merkezlerinin birleştirilerek 12 adede indirilmesi ve bu sayede yaklaşık %75 oranında enerji tasarrufu yapılması,
- Kamu kurumlarının internet sitelerinin farklı yer sağlayıcılar tarafından barındırılması yerine daha stratejik bir kararla G-Bulut'unda barındırılması,
- Tüm kamu kurumlarının güvenli ve ortak bir elektronik haberleşme ağı aracılığıyla birbirlerinin elektronik haberleşme altyapılarını paylaşmalarının sağlanması vb. tedbirler alınması planlanmıştır.

2011 yılının Mart ayında yayımlanan yeni Kamu BİT Stratejisinde de G-Bulut adı zikredilmeksizin kamuda bulut bilişim kullanımı teşvik edilmektedir. 2010 yılına göre daha makul hedefler ortaya koyan söz konusu stratejide,

- Mevcut durumda yaklaşık 8.000 adet olan kamu veri merkezlerinin birleştirilerek maliyetlerin %35 oranında düşürülmesi,
- Kamu Yazılım Uygulamaları Mağazası'nın 24 ay içinde uygulamaya konulması,
- 1 yıl içinde bulut bilişimle ilgili zorunlu açık teknik standartların kabul edilmesi,

vb. hedefler bulunmaktadır.

Son yıllarda, İngiltere’de kamu BT tedarikinde bulut bilişim hizmet modeline geçişin devlet politikası düzeyinde benimsendiği görülmektedir. (Mirzaoğlu, 2011, s.62-63).

2.2.3. ABD Veri Merkezi ve Bulut Bilişim Yapısı

Amerika Birleşik Devletleri (ABD), kamu sektöründe bulut bilişim modelini uygulamaya yönelik somut adımlar atan öncü ülkelerdendir.

ABD’de Bulut bilişim, “Önce Bulut” Politikası, Federal Bulut Bilişim Stratejisi ve İnisiyatifi ile bunlara binaen çeşitli kamu kurumları tarafından çeşitli uygulama adımlarını kapsamaktadır.

“Önce Bulut” Politikası, ABD Yönetim ve Bütçe Dairesi tarafından hazırlanan, ülke çapında BT yönetiminde reform yapmaya yönelik 25 maddelik planın bir parçasıdır.

2010 yılında tanıtılan,“Önce Bulut” Politikası, devletin, kamuda daha düşük maliyetli teknolojilerin ve ortak hizmetlerin kullanımını teşvik ederek operasyonel verimliliği arttırmayı amaçlayan reform çalışmalarının önemli bir parçası olarak sunulmuştur (Mirzaoğlu, 2011, s.56-57).

Kundra (2010)’ya göre, 25 maddelik BT reform planında yer alan diğer eylem maddelerinden bazıları ise şunlardır:

- 2015 yılı itibariyle mevcut veri merkezlerinden bir kısmının birleştirilerek toplam veri merkezi sayısının 800 azaltılması,
- BT satın alma sürecinde en iyi uygulamaların belirlenerek bunların tüm kamu kurumları ile paylaşılmasının sağlanması,

- Kamu kurumları ile özel sektör kuruluşları arasında proje tekliflerinin hazırlık aşamasında işbirliği yapılmasına imkân veren interaktif bir platform oluşturulmasıdır (Mirzaoğlu, 2011, s.57).

Söz konusu reform planının uygulanması ile harcamaların gereksiz, düşük kapasiteyle kullanılan kaynaklardan görev öncelikli sistemlere kaydırılacağı ve BT altyapı harcamalarında 24 milyar ABD doları tutarında tasarruf yapılacağı belirtilmekte, ayrıca “Önce Bulut” yaklaşımı sayesinde isteğe bağlı hizmet tedariklerinde birim maliyetlerde %50’ye yakın azalma olacağı tahmin edilmektedir (Mirzaoğlu,2011,s.57).

2011 yılının Şubat ayında ABD Bilişim Kurulu tarafından yayımlanan Federal Bulut Bilişim Stratejisi, kamu kurumlarının veri merkezlerinde gözlenen;

- Kaynak kapasite kullanım oranlarının düşüklüğü,
- Tedarik sürelerinin uzunluğu,
- Kaynak yönetiminin güçlüğü,
- Talep yapısının parçalı oluşu,
- Gereksiz tekrarlanan sistemlerin bulunması

gibi sorunların kamu hizmetlerini olumsuz yönde etkilediği ve bulut bilişimin söz konusu sorunların giderilerek kamu hizmetlerinin iyileştirilmesinde etkili olabilecek potansiyele sahip olduğu düşüncesinden hareketle hazırlanmıştır.

Kundra (2011)’ya göre, söz konusu stratejinin amacı,

- Bulut bilişimin getirilerini, güçlüklerini ve bunların dengesini ortaya koymak,
- Kamu kurumlarının bulut bilişime geçişine yardımcı olacak bir karar modeli ve çeşitli uygulama örnekleri sunmak,

- Bulut bilişim uygulama kaynaklarını vurgulamak,
- Bulut bilişimin benimsenmesini kolaylaştırma hususunda yürütülen çalışmaları belirtmek ve kurum ve kuruluşlara düşen rol ve sorumlulukları belirlemektir (Mirzaoğlu, 2011, s.58).

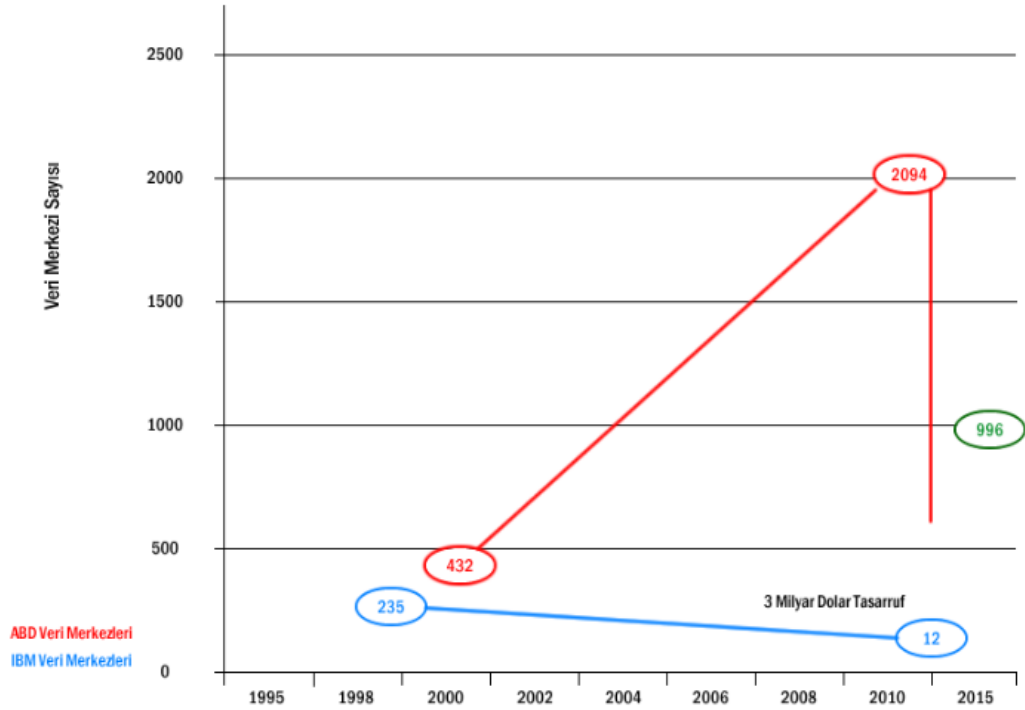
ABD’de veri merkezleri yapısına bakacak olursak; 1998 ve 2010 yılları arasında, Federal Devlet veri merkezleri sayısını dörde katlamıştır. Ayrıca, veri merkezleri tüm altyapı, taşınmaz mallar ve enerji tüketimi için bilgisayar gücünün ortalama yüzde 27’sini kullanmaktadır (Whitehouse, 2011).

Veri merkezleri, çevresel kontroller (klima, yangın söndürme, vb) ve özel güvenlik cihazlarının yedek güç kaynaklarına ihtiyaç duyması nedeniyle standart ofis alanlarından 200 kat daha fazla elektrik tüketmektedir (Whitehouse, 2011).

ABD Veri Merkezlerinde yılda 100 Milyar KWh elektrik (7.4 Milyar \$’lık enerji) tüketilmektedir (U.E.P.Agency, 2007, s.7).

Veri merkezlerine yapılan fazla harcamaların önlenmesi, özellikle zorlayıcı bütçe dönemlerinde önemli hale gelmektedir. Veri merkezi kullanım alanlarında yapılacak daralma ile altyapı, taşınmaz mallar ve enerji maliyetlerinin azalması, vergilerde tasarruf sağlayacaktır. Aynı zamanda, daha iyi bir 21. yüzyıl modeline geçilmesiyle hizmetlerin sunulması ve güvenliğin sağlanması daha az kaynakla gerçekleştirilmiş olacaktır.

Şekil 2.27 ABD ve IBM Veri Merkezi Konsolidasyonu



Kaynak: (Renda, 2011, s.4)

ABD’de, 01 Mart 2014 itibarıyla 746 veri merkezi kapanmış olup, 352 veri merkezinin 30.09.2014’e kadar kapatılması planlanmıştır. Böylece 2015 yılına kadar 1098 veri merkezinin kapatılmasıyla 3 milyar dolar tasarruf edilmesi beklenmektedir (Whitehouse, 2011).

Kapatılması planlanan, çeşitli bölgelere dağıtılmış olan kamu veri merkezlerinin alanı, her biri en az 1.000 m² ile 57.000 m²,ye (Savunma Bakanlığı binası) kadar değişmektedir. Maryland, Lanham’da bulunan Hazine Bakanlığı binasının yaklaşık 13.000 m²’lik alanı kapatılacaktır. Bu binada 75 raf, 250 sunucu barındırmakta ve kira ve elektrik giderleri için yıllık 400.000 \$’dan fazla harcama yapılmaktadır. Federal devletin genelinde her bir kurum ve bakanlıkta fazla harcamaların engellenmesi amaçlanmıştır (Whitehouse, 2011).

ABD’de Federal Bulut Bilişim İnisiyatifi, kurumlarda ortak olarak kullanılan hizmetlerin ve çözümlerin tespit edilmesi ve bulut bilişim modelinin kullanılması suretiyle BT hizmetlerinin modernize edilmesini amaçlayan ve Başkanlık düzeyinde kabul gören bir inisiyatiftir. ABD Yönetim ve Bütçe Dairesi ile Federal Bilişim Kurulu tarafından başlatılan bu inisiyatifte bulut bilişim kilit bir rol üstlenmektedir.

ABD Genel Hizmetler Dairesi (GSA), Federal Bulut Bilişim İnisiyatifinde görev alan kuruluşlardan biridir. GSA, kamu hizmetlerinde operasyonel verimliliğin artırılması, ortak hizmet ve çözümlerin kurumlar arasında paylaşılması ve şeffaflığın, işbirliğinin ve katılımcılığın sağlanmasına katkıda bulunacak bulut bilişim çözümlerinin tedarik edilmesi ve kullanılmasına yönelik projeler yürütmektedir (Mirzaoğlu, 2011, s.59).

Aynı zamanda, 25 maddelik BT reform planında, kamu kurumları ile özel sektör kuruluşları arasında proje tekliflerinin hazırlık aşamasında işbirliği yapılmasına imkân veren interaktif bir platform oluşturulmasını öngören eylem maddesinin sorumluluğu da GSA’ya verilmiştir. GSA, söz konusu sorumluluğa binaen, 2010 yılında “Apps.gov” alan adlı internet sitesini oluşturmuştur (Mirzaoğlu, 2011, s.59).

Kamu kurumlarının kendi bünyelerinde veri merkezi oluşturma ihtiyacını ortadan kaldırmak ve ilgili maliyetlerden kaçınmalarına yardımcı olmak amacıyla kamu kurumlarının bulut bilişim hizmet ihtiyaçlarının tek merkezden tedarik edilmesini “Apps.gov” sağlamaktadır. Brookings Enstitüsü tarafından, Apps.gov’un kullanılması ile elektrik faturalarının düşmesi sayesinde kamu harcamalarında %50 civarında tasarruf edileceği tahmin edilmektedir (Mirzaoğlu, 2011, s.59-60).

2.2.4. Japonya Veri Merkezi ve Bulut Bilişim Yapısı

Kamuda bulut bilişim kullanımına öncelik veren ülkelerden biri de Japonya’dır. 2008 yılında yaşanan küresel finansal ve ekonomik kriz sonrasında, Japonya’da Dijital Japonya adlı bir proje hazırlanmış ve 2009 yılının Mart ayında, Japonya

İçişleri ve İletişim Bakanlığı (MIC) tarafından yayımlanan ve projeyi ana hatlarıyla özetleyen bir belge ile tanıtılmıştır. MIC'e göre, 2008 yılında yaşanan küresel ekonomik kriz, pek çok ülkede olduğu gibi, dünyanın en büyük ekonomilerinden birine sahip olan Japonya'da da yaklaşık %40'ı BİT sektöründen kaynaklanan ekonomik büyümeyi olumsuz etkilemiştir. Bunun üzerine, gerek bu olumsuz etkilerden hızlı şekilde kurtulabilmek, gerekse orta ve uzun vadede özel sektöre dayalı sürdürülebilir kalkınmayı sağlamak amacıyla, 3 yıl içinde hızlandırılmış şekilde yapılması öngörülen BİT yatırımları ve kamunun gizli kalmış ekonomik potansiyelini ortaya çıkarmak üzere alınması gereken BİT'e dayalı tedbirleri kapsayan söz konusu proje hazırlanmıştır (Mirzaoğlu, 2011, s.65).

Bahse konu hızlandırılmış çalışmalar için bir öncelik politikası ortaya koyan bu proje, aynı zamanda Hatoyama BİT Planı olarak da adlandırılmakta olup, projenin yürütülmesinden MIC'in yanı sıra, diğer bakanlıklar da sorumludur. Projede yer alan 9 ana eylem maddesinden biri 2015 yılına kadar, "Kasumigaseki-1 Bulutu" olarak nitelendirilen bir kamu bulutu oluşturmak, bir başka ifadeyle, tüm kamu kurumlarına ait veri merkezlerini tek bir veri merkezi halinde birleştirmek suretiyle e-Devlet hizmetlerinde yenilikçiliği sağlamaktır. Kasumigaseki, Japonya'nın başkenti Tokyo'da, pek çok bakanlık ve kamu kurumunun bulunduğu bölgenin adı olup, Japon bürokrasisini niteleyen bir mecaz olarak kullanılmaktadır (Mirzaoğlu, 2011, s.66).

Farklı bakanlıkların, kullandıkları BT donanımlarını birleştirmelerini ve ortak iş ve işlemlerinde kullanabilecekleri platformlar oluşturmalarını sağlaması öngörülen Kasumigaseki bulutunun, e-Devlet uygulamalarının bir yandan geliştirme ve işletim maliyetlerini azaltırken, diğer yandan da birlikte çalışabilirliğini, güvenliğini ve hizmet sunma hızını artırması beklenmektedir (Mirzaoğlu, 2011, s.66).

Dijital Japonya projesi kapsamında oluşturulması planlanan Kasumigaseki-1 bulutunun, bir başka ifadeyle kamu veri merkezinin tesis edilmesinde enerji tüketimini asgari düzeyde tutan çevreci bir yaklaşımın benimseneceğini belirtmektedir. Söz konusu yaklaşıma göre, veri merkezleri genellikle rüzgâr veya

güneş enerjisinden faydalanılabilen, depreme dayanıklı, sıcaklıkların kararlı seyrettiği, enerji tüketim bedelinin ve soğutma ihtiyacının düşük olduğu soğuk bölgelerde konumlandırılmaktadır (Mirzaoğlu, 2011, s.67).

2.2.5. Google Veri Merkezi

İnternet devi Google, veri merkezleri konusunda uzmanlaşarak bu konuda önemli bir konuma gelmiştir (Chip, 2012). Google'ın ABD, Asya ve Avrupa'nın farklı yerlerinde bulunan veri merkezleri, merkez kampüsünde olmamasına rağmen sistemin en önemli parçası olarak nitelendirilmektedir (Radore).

Kuzey Karolina'da bulunan Berkeley County veri merkezi, çevresinde halka açık dev bir Wi-Fi hizmeti vermesiyle bilinmektedir. Veri merkezi iklimlendirmesi için inşa edilen dev su tankları 240,000 galon (900.000 litre) su kapasitesine sahiptir (Radore).

Şekil 2.28 Google Berkeley County Veri Merkezi



Kaynak: Radore

Council Bluffs, Iowa'da 10.650 m²'lik bir alana yayılan veri merkezinde, kullanılan fiber optik ağlar tipik bir ev internet bağlantısından 200.000 kat daha hızlı çalışmaktadır (Radore).

Şekil 2.29 Google Council Bluffs Veri Merkezi



Kaynak: Radore

Arama motoru Google Douglas County, Georgia'daki veri merkezini Youtube ile paylaşmaktadır.

Google'ın diğer veri merkezleri; Şili'deki Quilicura; Oklahoma'da bulunan Mayes County; Kuzey Karolina'daki Lenoir ve Oregon'daki The Dalles'tır. Google'ın Asya'da Tayvan ve Singapur'da iki ayrı veri merkezi bulunmaktadır. Avrupa'da ise, Hamina (Finlandiya), St Ghislain (Belçika) ve Dublin'de (İrlanda) veri merkezleri bulunmaktadır (Google).

Binlerce server'ın belki yüz binlerce kablonun bulunduğu Google veri merkezinde borular taşıdıkları kablo türüne ve tipine göre renklendirilmiştir. Örneğin; Su borularındaki renklendirmede mavi borular soğuk suyun geçtiği, kırmızı renktekiler ise tekrar soğutulacak olan suların geçtiği borulardır. Ayrıca, Switch kabloları da farklı renklerde. Çalışanlar kabloların hangi server'lara yönlendirildiğini bilmekte ve arıza anında gerekli müdahaleyi kolaylıkla yapabilmektedir.

Şekil 2.30 Google Veri Merkezi



Kaynak: Radore

Özel Yüksek Etkili Sunucu Yapısı

Google sunucuları tipik sunuculardan farklı olup her zaman yüksek performansta çalışan bilgisayarlardan oluşmaktadır. 2001 yılından beri sunucuların daha etkili olması çalışmalar devam etmektedir.

Veri merkezinin temelini oluşturan bilgisayarlar, güç kaybı en aza indirilerek gereksiz parçaların çıkarılmasıyla mümkün olduğunca en az enerji kullanacak şekilde tasarlanmıştır. Bu sayede, sunucu başına yıllık 500 kWh enerji, tipik bir sunucunun %25'i kadar tasarruf yapılabilmektedir (Google).

Google veri merkezinde uygulamaların çalıştırılması için sadece gerekli olan donanım kullanılmaktadır. Sunucular ve raflar, en az fan gücü kullanılmak üzere optimize edilmiştir. Fanlar, sadece makineleri çalıştıracak düzeyde serin tutmak için hızlı dönmektedir (Google).

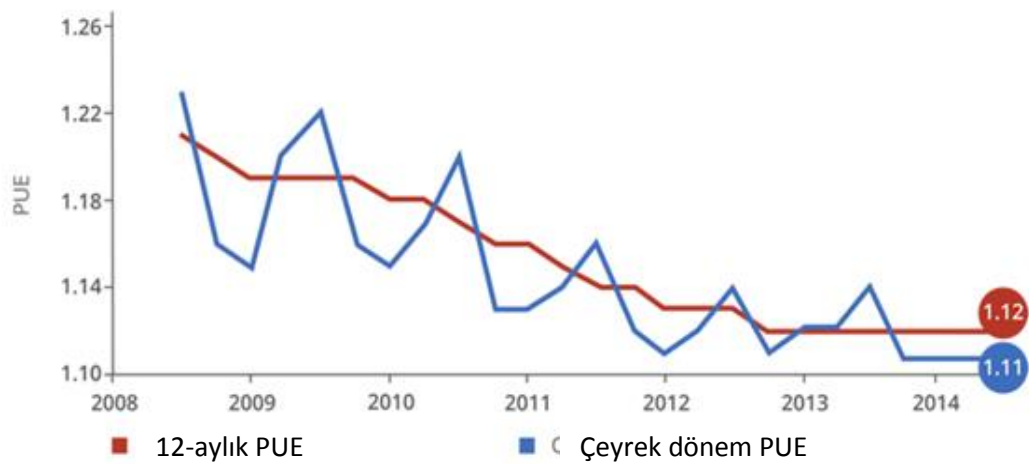
Enerji Kullanımının Ölçülmesi ve Geliştirilmesi

Google, büyük oranda artan internet hizmetiyle birlikte enerji kullanımının düşürülmesine yoğunlaşmıştır. Çoğu veri merkezi, sunucularını çalıştırmak için soğutucu ve güç dönüşümü gibi ek yük gerektiren enerjiyi kullanırken, Google'da bu ek yüklerin %12'si azaltılmıştır. Bu yolla, enerjinin çoğu direk Google'ın araştırma ve ürün hizmetleri için kullanılmaktadır. Google, daha az enerji harcayarak, daha çok kullanıcıya hizmet edilmesi için detaylı önlemler almaktadır (Google).

Google Veri Merkezi PUE Performansı

Açıklanmaya başlandığı 2008 yılından beri PUE değeri düşmektedir. 2014'ün 2. çeyreğinde enerji ağırlıklı ortalama PUE değerinin 1.12 olması, Google veri merkezini dünyanın en verimli veri merkezi yapmaktadır. Uptime Enstitüsü'nün 2014 yılı veri merkezleri araştırmasına göre, dünyada büyük çaptaki veri merkezlerinin PUE değerinin ortalaması 1.7'dir (Google).

Şekil 2.31 Veri Merkezleri PUE değeri ortalaması



Kaynak: Google

Google veri merkezlerinde farklı iklimlere göre farklı güç ve soğutma sistemleri bulunmaktadır. Soğuk mevsimlerde düşük olması gibi mevsimsel hava PUE değerini etkilemektedir. Google, nemli Atlanta yazları gibi sıcak havalarda bile bütün veri merkezlerinde düşük PUE ortalamasını sürdürmek için çalışmalar yapmaktadır (Google).

Sıcaklık Kontrolü

Cihazlarda optimum enerji tasarrufu ile birlikte veri merkezlerindeki makinalarda sıcaklık ve hava akımı, maliyeti etkin bir şekilde ayarlanmaktadır.

Veri merkezlerinde enerjiden tasarruf edilmesinin en basit yöntemlerinden biri de sıcaklığın yükseltilmesidir. Uzman önerileri ve BT ekipmanları üreticileri şartnamelerine göre veri merkezi operatörleri soğuk koridoru 80°F veya daha fazla dereceye yükseltebilir. Böylelikle, tesisin enerji kullanımı önemli ölçüde azaltılabilir. Enerji tasarrufunu sağlamak ve soğutma maliyetlerini düşürmek için sunucu rafı önündeki soğuk hava koridoru ile sunucu rafı arkasındaki sıcak hava koridorunun karışması önlenmektedir. Google büyük veri merkezlerinde “kanallama” ve kalıcı kaplama (enclosures) kullanılmaktadır (Google).

Soğutucu değil Su ile Soğutma

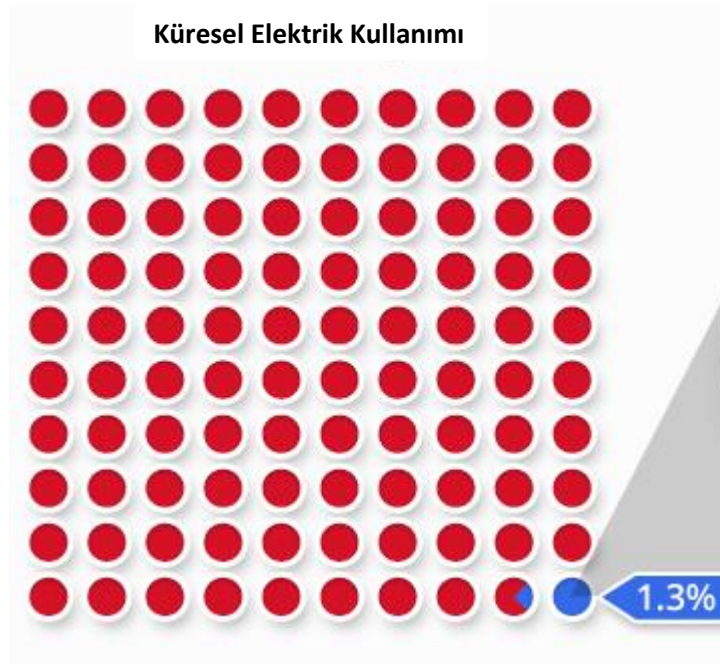
Çoğu veri merkezinin soğutma işlemleri için soğutucu veya klima kullanması %30-70 oranında ek enerji kullanımı gerektirmektedir. Google veri merkezlerinde su ile soğutma yapılarak verimli enerji kullanımı yapılmaktadır.

Finlandiya'daki Hamina Veri Merkezi'nde soğutucular olmadan deniz suyu ile soğutma yapılmaktadır. Soğuk iklim ve Finlandiya Körfezindeki konumu nedeniyle veri merkezi burada kurulmuştur (Google).

Veri Merkezi Elektrik Tüketimi

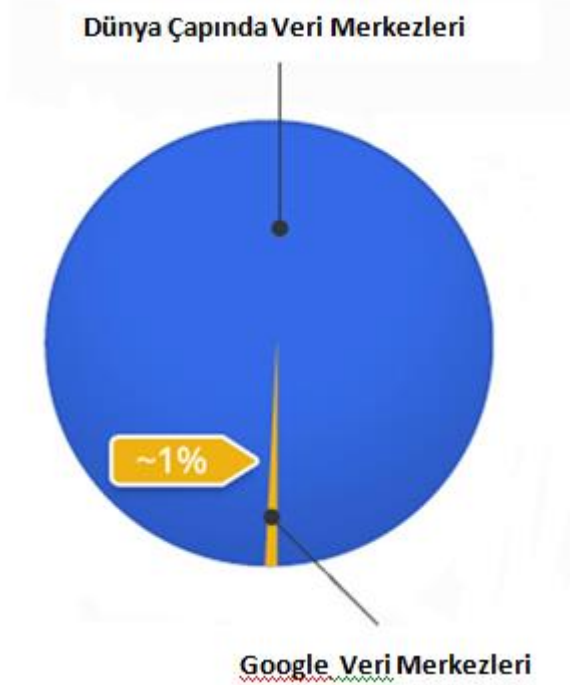
Google, küresel elektrik tüketiminin çok küçük bir parçasını kullanmaktadır. Stanford Danışmanlık Profesörü Jonathan Koomey'in bağımsız raporunda, veri merkezlerinin, toplam elektrik tüketiminin % 1,1-% 1.5 arasında elektrik tükettiği tahmin edilmiştir. Google'ın hesaplarına göre, Koomey'in küresel elektrik tüketimi tahmininin %1'ni Google kullanmaktadır. Buna göre küresel elektrik tüketiminin %0.01'inden Google sorumludur (Google).

Şekil 2.32 Küresel Elektrik Tüketiminde Veri Merkezleri'nin Yeri



Kaynak: Google

Şekil 2.33 Veri Merkezleri Elektrik Tüketiminde Google'ın Yeri



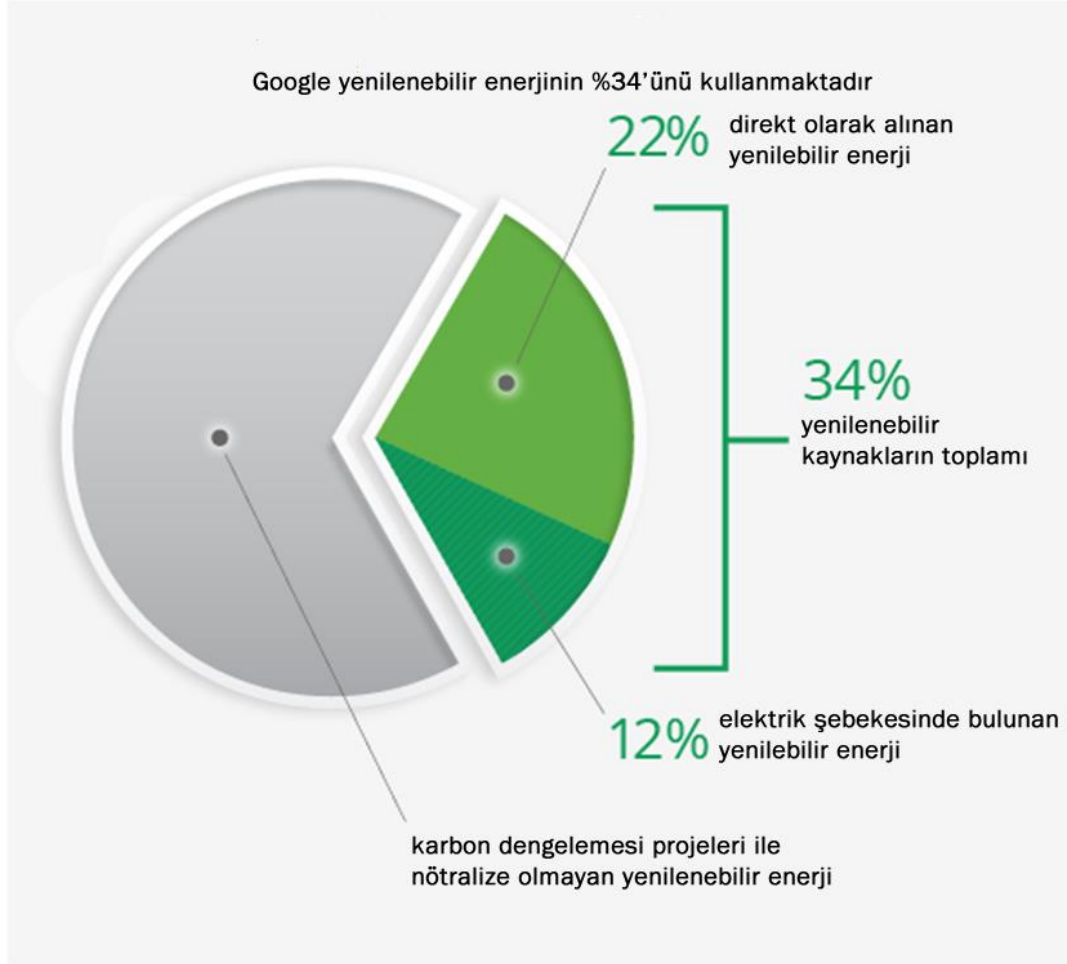
Kaynak: Google

Google Yeşil Veri Merkezleri

Günümüzde, dünyadaki enerjinin çok az bir kısmı rüzgar ve güneş gibi yenilenebilir enerjiden oluşmaktadır. Google, veri merkezlerinin yanında Rüzgar Santralleri'nin kurulması üzerinde çalışmaktadır.

Google tarafından üretilen veya direkt olarak alınan yenilenebilir enerji %22, elektrik şebekesinde bulunan yenilenebilir enerji %12 olmak üzere; Google, yenilenebilir kaynakların toplam %34'ünü kullanmaktadır (Google).

Şekil 2.34 Google'ın Yenilenebilir Enerji Kullanımı (%) (2012)



Kaynak: Google

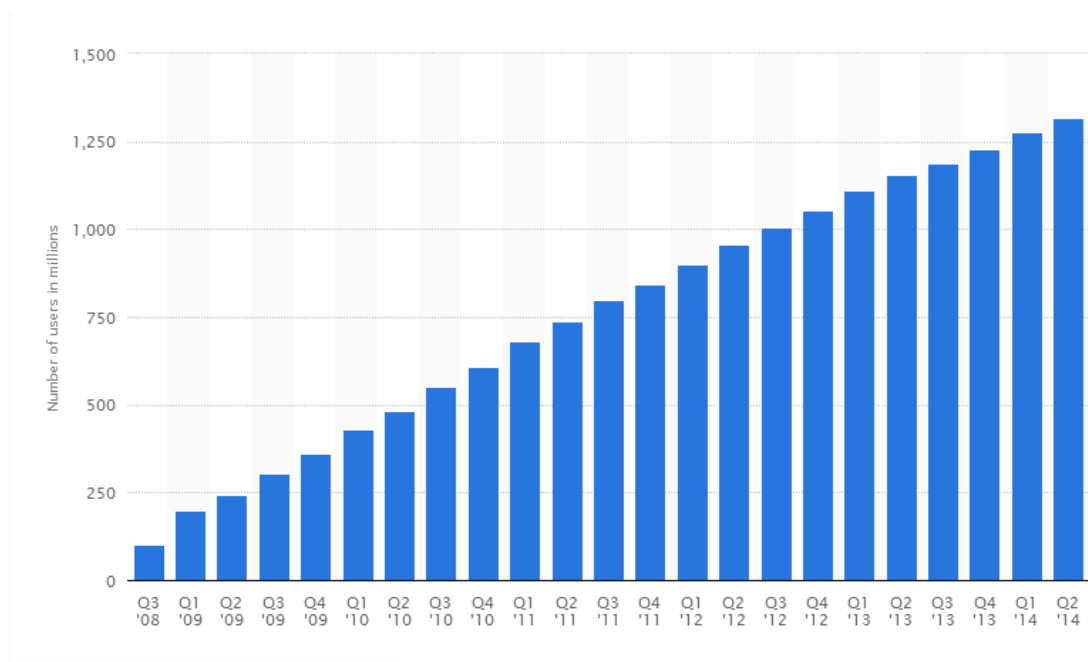
Google'ın dünya çapındaki tüm ofislerinde çevre üzerindeki etkinin azaltılması için çalışmalar yapılmaktadır. Google'un çatıya güneş panellerinin konulması, işe bisikletle gidilmesi gibi yeşil girişimleri kapsamında CO₂ salınımını yılda 21.500 tondan fazla azaltmaktadır (Google).

Google veri merkezlerindeki verimlilik çalışmaları ile enerji kullanımını %50 düşürmüştür. Yenilenebilir enerjinin kullanılması ve karbon dengelenmesi ile emisyonun 0'a indirilmesi amaçlanmaktadır (Google).

2.2.6. Facebook Veri Merkezi

Alexa istatistiklerine göre Facebook, 31 Ağustos 2014 itibarıyla; Dünya'nın en fazla ziyaret edilen 2. sitesidir (Alexa, 2014). Facebook 2014 yılının ikinci çeyreğinde aktif kullanıcı sayısı 1.32 milyar olmuştur (Statistica, 2014).

Şekil 2.35 Facebook Aktif Kullanıcı Sayısı (2008-2014) (Milyon)



Kaynak: Statistica (2014)

Construction.com'un 2011 yılında yayınladığı raporuna göre ABD'nin en büyük veri merkezleri sıralamasında, 800 milyon aktif internet kullanıcısının sınırsız veri paylaşımını yöneten Facebook'un Prineville, Oregon'daki veri merkezi listenin 4. sırasında yer almaktadır (Demirel, 2012)

Facebook, ABD dışında ilk veri merkezini İsveç'in Lulea kasabasında açmıştır. Baltık Denizi'nin kuzeyinde kalan kasabada açılan tesis, Avrupa'nın sahip olduğu en büyük veri merkezlerinden bir olma özelliği taşımaktadır (Ntvmsnbc).

Facebook'un, üçüncü veri merkezi için Lulea'yı seçmesinin nedenleri;

- 1961'den bu yana sıcaklığın 30 derecenin üzerine çıkmadığı kentte ortalama sıcaklığın 2 derece olmasıyla kasabanın mükemmel bir doğal soğutucu özelliğine sahip olması,
- Lulea nehriindeki barajların çok yüksek oranda yenilenebilir elektrik üretmesiyle bu elektriğin yarısından fazlası ihraç edilebiliyor olması
- Veri merkezi için kullanılabilir olması ve İsveç'in Avrupa'daki en iyi fiber optik ağlardan birine sahip olmasıdır.

Lulea şehri dışındaki 300.000 metrekarelik tesis Avrupa'daki sosyal ağ performansını geliştirmek için hizmet vermektedir. Open Compute Projesi çerçevesinde tasarlanan tesiste, kuzeyin soğuk havasının yanı sıra su soğutma sistemi de fotoğraf, video ve mesaj gibi aktiviteleri depolandığı binlerce sunucuyu soğutmak için kullanılmıştır. Tesiste oluşan aşırı ısınma ofisleri ısıtmak için kullanılırken, Facebook'un dünya çapındaki veri trafiğinin büyük bir kısmı da Lulea'daki tesise aktarılmıştır (Ntvmsnbc).

Lulea veri merkezi dünyanın dört bir yanından gelen trafiği düzenlemede büyük önem taşımaktadır. Veri merkezindeki tüm enerji yerel olarak üretilen hidro-elektrikten sağlanmaktadır. Yüzde 100 yenilenebilir olan bu enerji, aynı zamanda jeneratör ihtiyacını yüzde 70 azaltmaktadır. Milyarca fotoğraf, video ve diğer verilerin saklandığı sunucuların, İskandinavya'nın soğuk havasıyla doğal olarak soğutulması enerji ihtiyacını azaltmaktadır.

Facebook, Luella veri merkezini, kendi girişimi olan ve veri merkezi altyapılarına ait tasarımları paylaşmayı öngören Open Compute Project (OCP) tabanına kurmuştur. Bu proje kapsamında, merkezin soğutma sisteminden mimarisine kadar her türlü özelliği paylaşılmaktadır (Ntvmsnbc).

Şirketin diğer iki dev veri merkezi sırasıyla Prineville, Oregon ve Forest City, Kuzey Carolina'da bulunmaktadır (Ntvmsnbc).

Silikon Vadisi devi Facebook'un 30.000 m²'lik bir alanda kurulmuş olan Oregon Prineville'deki dev tesisi 800 milyon etkin kullanıcıya hizmet etmektedir (Radore).

Şirketin dördüncü veri merkezini Altoona, Iowa'da kurması beklenmektedir. Des Moines Register raporlarına göre Facebook Altoona, Iowa'da büyük bir veri merkezi inşaa etmektedir. Facebook tarafından inşaa edilen veri merkezi toplamda 130.000 metrekarelik bir alanın üzerine kurulacak ve şirketin kendi adı altında inşaa ettiği dördüncü veri merkezi olacaktır (Çevrim, 2013).

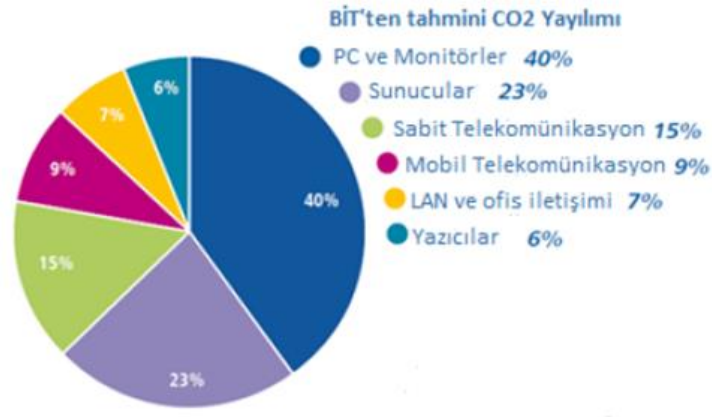
2.3.Yeşil Veri Merkezleri

"Yeşil Veri Merkezleri", veri merkezleri için, enerji farkındalığı olan, enerji verimliliğini amaçlayan ve CO₂ salınımını en aza indiren tasarımlar, protokoller, cihazlar, altyapılar ve algoritmalar anlamına gelmektedir (Çavdar ve Alagöz, 2013, s.1).

Gartner'in raporuna göre, BİT'in küresel sera gazına katkısı % 2-3 arasındadır. Avrupa Birliği tahminlerine göre toplam elektrik tüketiminin % 7,8'i BİT tarafından tüketilmektedir ve 2020 yılında bu oranın % 10,5 olması beklenmektedir. Yine AB çalışmaları AB 25 ülkelerindeki toplam CO₂ emisyonunun 2005 yılında % 1,9'unun bu durumdan kaynaklandığını göstermektedir ve 2020 yılında bu oranın % 4,5'e çıkacağı tahmin edilmektedir (BTK, 2010, s.28).

BİT sektörünün kendisi sera gazı emisyonunun % 2-2,5'ine sebep olmaktadır. Bu oran yaklaşık 1 gigaton CO₂'ye denk gelmektedir. ITU (2008) raporuna göre, şekil 2.20'de görüleceği üzere bu CO₂ emisyonunun temel bileşeni bilgisayar ve monitörlerin enerji ihtiyacıdır, ikinci sırada ise % 23 ile veri merkezleri yer almaktadır. Sabit ve mobil telekomünikasyon sektörleri % 24 oranında katkı sağlamaktadır (BTK, 2010, s.28).

Şekil 2.36 BİT Tarafından Yayılan CO2 (Tahmini)

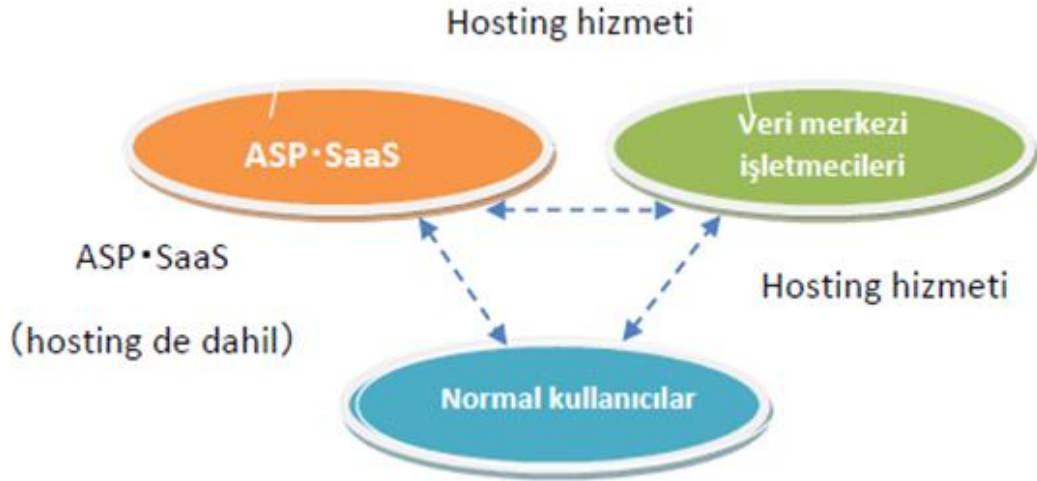


Kaynak: (BTK, 2010, s.29)

2.3.1. Veri Merkezlerinin Enerji Tasarrufu

Veri merkezlerinin çevre dostu bir şekilde faaliyet göstermesi için veri merkezi işletmecileri tarafından kabul görmüş önlemlerin bir an önce hayata geçirilmesi gerekmektedir. Sunuculuk hizmetinin özel ve kurum kullanıcıları tarafından doğrudan kullanılmasının yanında kullanıcılar bu hizmetleri ASP/SaaS işletmecileri üzerinden de alabilmektedir. Söz konusu ilişki Şekil 2.29'da görülmektedir (BTK, 2010, s.38).

Şekil 2.37 Veri Merkezi İşletmecileri, ASP/SaaS İşletmecileri ve Kullanıcılar Arasındaki İlişki



Kaynak: (BTK, 2010, s.38)

2.3.2. Veri Merkezi Kullanımı

Kişiler veya şirketlerin sahip oldukları sunucular kullanımda olmayan veri alanları ve zamanlar içermektedir ve bu durum gereksiz güç tüketimine sebep olmaktadır. Bu sunucuları veri merkezlerindeki sanal sunuculara birleştirmek, sera gazı emisyonunu azaltmaktadır. Birleştirilmiş faaliyetler aynı zamanda soğutma faaliyetleri için de enerji tasarrufu sağlamakta ve bu sebeple oluşan sera gazı emisyonunu da azaltmaktadır (BTK, 2010, s.39).

2.3.3. Veri Merkezi Tasarımı

Daha verimli soğutma yöntemleri ve cihazları ile daha temiz elektrik kaynakları kullanımı soğutma işlemlerinde enerji tasarrufu sağlayacaktır. Gücün verimli kullanımı ve güç kaybının azaltılması göz önünde bulundurulması gereken alanlardır. Bir veri merkezinde enerji tüketimine yönelik yapılan analizlere göre dağılım aşağıdaki gibi gerçekleşmektedir:

- Bilgisayar odası havalandırma sistemi %50
- Sunucu/depolama %26

- Çevirme %11
- Şebeke %10
- Işıklandırma %3 (BTK, 2010, s.39-40)

2.3.4. Enerji Tasarrufu Sağlayan Cihazların Kullanımı

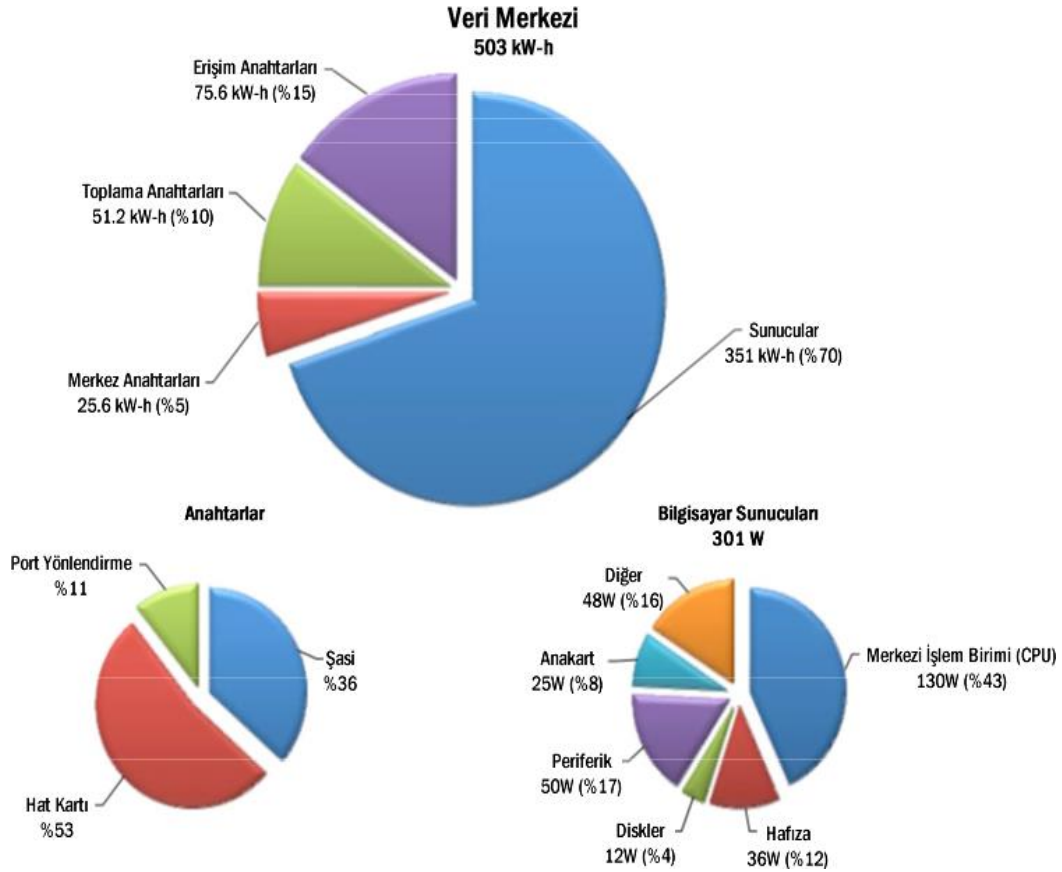
Enerji tasarrufu sağlayan sunucular, depolama, şebeke cihazları, enerji koruyucu cihazlar ve yöntemler enerji tüketimini azaltmaktadır (BTK,2010,s.40).

Yeşil teknolojiler, enerjinin siyasi, ekonomik ve çevresel yönleri nedeniyle hükümetler ve sanayi için önemli bir konu haline gelmiştir. Enerji ve çevre açısından bakıldığında, BİT toplam küresel CO₂ salınımının %2'sini ve küresel enerji tüketimi %3'ünü oluşturmaktadır. Veri merkezleri ise BİT enerji tüketiminde birincil enerji tüketicileridir. Video kullanımındaki artış ve bulut bilişim servisleri, tüm dünyada birçok yeni veri merkezleri açılmasına neden olmuştur. Veri merkezleri yüksek kullanılabilirlik sağlamalı ve aynı zamanda hataya dayanıklı olmalıdır. Bu gereksinimler veri merkezlerinde yüksek enerjinin tüketilmesine neden olmaktadır (Çavdar ve Alagöz, 2013, s.1).

ABD Çevre Koruma Ajansı'nın ENERGY STAR Programı raporuna göre, ABD'de veri merkezleri yılda 100 Milyar kWh elektrik veya 7.4 milyar dolarlık enerji tüketmektedir. Bir veri merkezinin ana enerji tüketim birimleri; soğutma, bilişim kaynakları ve ağ elemanlarıdır. Soğutma için tüketilen enerji bir veri merkezinde tüketilen toplam enerjinin yaklaşık %30'unu oluşturmaktadır (Çavdar ve Alagöz, 2013, s.1).

Şekil 2.30'da, 3-katmanlı veri merkezi için simülasyon ortamı ile elde edilmiş içinde yaklaşık enerji tüketimi (soğutma hariç) dağılımını gösterilmektedir. Bu şekil sunucuların enerji tüketiminde en önemli bir kaynak olduğunu göstermektedir. Ayrıca, bir veri merkezinde bilişim için kullanılan toplam enerjinin yaklaşık %30'u erişim anahtarları, toplama anahtarları ve merkez anahtarları tarafından tüketilmektedir (Çavdar ve Alagöz, 2013, s.1-2).

Şekil 2.38 Veri Merkezinde Enerji Tüketiminin Dağılımı



Kaynak: (Çavdar ve Alagöz, 2013, s.2)

Veri merkezleri için yeşil öneriler; ağ, bilişim, soğutma, bulut ve sanallaştırma, olarak sınıflandırılabilir. Sunucular, birincil enerji tüketiciler olduğundan, sunucuların enerji verimliliği için önemli sayıda öneri bulunmaktadır. Sanallaştırma ve dinamik iş yükü birleştirme ile sunucular, daha verimli kullanılabilir. Ancak, yeşil veri merkezi ağları için çok az sayıda öneri bulunmasının nedeni, katmanlı veri merkezlerinde, ağ elemanlarının sunuculara oranla daha az enerji tüketiyor olmasıdır (Çavdar ve Alagöz, 2013, s.2).

Günümüzde hesaplama ve depolama işlemlerinin bulut bilişime kaymaya başlamasıyla, internet trafiğinin büyük bir kısmını veri merkezleri üzerinde yoğunlaşmıştır. Yazılım ve donanım uzmanları, yeni veri merkezleri tasarlarırken, veri merkezlerinin enerji tüketimini dikkate almalıdır. Veri merkezleri, bilgi işlem

kaynakları, ağ elemanları ve enerji orantılılık ilkesine göre tasarlanmalıdır. Enerji oransal tasarımlar, aktivite düzeyi ile orantılı olarak enerji tüketmekte, dolayısıyla, boştaiken enerji harcamamaktadırlar. Pratikte, veri merkezi tasarımları için, ideal bir enerji orantılılık elde etmek zordur. Bu nedenle, bir yaklaşım olarak, uyku modlarında farklı enerji harcamaları olan, çoklu uyku modları bulunan, bilgisayar ve ağ aygıtları tasarlanması, iyi bir strateji olarak düşünülebilir (Çavdar ve Alagöz, 2013, s.4).

2.3.5. Japonya Yeşil Veri Merkezi Uygulamaları

Japonya'da faaliyet gösteren büyük şirketler de Yeşil BT Girişimine destek vermekte ve yenilikçi projeler üretmektedir. Bilişim şirketleri tarafından yürütülen yenilikçi yeşil teknolojiler ile CO₂ salınımının ve enerji tüketiminin düşürülmesi amaçlamıştır (BTK, 2010, s.76).

Japonya'da faaliyet gösteren büyük şirketlerin yeşil BT alanında yapmış olduğu yeşil teknolojiler:

Hitachi 2025 yılından önce şirket olarak CO₂ salınımını yılda 100 milyon ton oranında düşürmeyi hedeflemektedir. Şirketin bir diğer hedefi ise "Cool Centre 50" girişimi ile 2013 yılına kadar veri merkezlerindeki enerji tüketimini %50 oranında azaltmayı hedeflemiştir.

NEC 2007 yılında NEC "Real IT Cool" projesini başlatmıştır. Bu proje ile NEC, enerji tasarruf platformu ve enerji tasarruf kontrol yazılımı aracılığı ile enerji tüketimini düşürmeyi planlamaktadır.

Fujitsu, 2007 yılı sonunda Japon teknoloji şirketi Fujitsu "Yeşil Yenilikçi Politika" isimli bir proje başlatmıştır. Projenin amacı 2007 ile 2010 yılları arasında CO₂ salınımını 700 milyon ton düşürmektir (BTK, 2010, s.76-77).

2.3.6. İngiltere Yeşil Veri Merkezi Uygulamaları

Kamu hizmetlerinin sunumunda dünyanın en gelişmiş bilgisayar sistemlerinden birini kullanan İngiltere; bilgi ve iletişim teknolojilerinin karbon salınımındaki artışın farkına vararak ve çevre ve iklim değişikliği üzerindeki olumsuz etkilerini azaltmak üzere 2008 yılında “Yeşil Devlet Bilişim Stratejisi”ni oluşturmuştur (BTK, 2010, s.69).

İngiltere Yeşil Bilişim Stratejisi'nin temel amaçları arasında; 2009 yılı Ocak ayı itibariyle tüm kamu kurumlarının bilişim ekipmanları tedariki esnasında karbon salınımı etkilerini göz önünde bulundurmaları ve oluşturulan standartlara uyumlu hareket etmeleri, 2012 yılı itibariyle tüm kamu kurumlarının karbon nötr hale getirilmesi ve 2020 yılı itibariyle tüm bilişim yaşam döngüsü içerisinde sürdürülebilirliğin sağlanması ilkeleri yer almaktadır (BTK, 2010, s.70).

İngiltere'de bilişim ekipmanlarının karbon ayak izini azaltmak üzere başta kamu kurum ve kuruluşları olmak üzere tüm kullanıcılar için uyulması gereken bir liste hazırlanmıştır. Bu listede veri merkezlerine ilişkin maddeler aşağıdaki gibidir.

Veri merkezleri için;

- i. Sunucu optimizasyonu,
- ii. Veri merkezlerinde soğutma sistemlerinin uygun seviyelere ayarlanması,
- iii. Hizmet sunmayan sunucu ve veri disklerinin belirlenmesi,
- iv. Düşük enerji tüketen düşük voltajlı güç ünitelerinin tercih edilmesi,
- v. Artık ihtiyaç duyulmayan ancak çalışır durumda olan cihazların gözden geçirilmesi,
- vi. Veri merkezi denetimleri (BTK, 2010, s.71-72).

İklim deęişiklięi ve bilişim ekipmanlarının çevre üzerindeki olumsuz etkilerinin öneminin ortaya çıkması ile birlikte oluşturulan hükümet politikalarının yanı sıra özel şirketler de bir yandan karbon ayak izlerini düşürmeye bir yandan da düşük karbon üreten ürün ve hizmetler sunmaya başlamıştır. İngiltere'nin yerleşik işletmecisi British Telekom yaklaşık on yıldır enerji tüketimini azaltacak yeni teknolojiler üzerinde çalışmakta ve karbon salınımını düşürmek için uğraşmaktadır (BTK, 2010, s.72).

British Telekom, şirket içi enerji kullanımını sürekli izlemekte ve denetlemektedir. Veri merkezlerinde kullanılmayan sunucuların devre dışı bırakılması, ısıtma soğutma sistemlerinin düzeltilmesi, enerji verimli aydınlatma sisteminin kurulması, kullanılmayan ekipmanların kapatılması gibi önlemler alınarak enerji tüketimi yılda 53 GWh azaltılmış ve 20.000 ton CO₂ salınımının önüne geçilmiştir (BTK, 2010, s.74).

3. SANALLAŐTIRMA

3.1. Sanallaőtırma Nedir?

Sanallaőtırma, mevcut bulunan fiziksel donanımın sanal makineler yardımıyla çok daha verimli kullanılabilmesini saęlayan, çeőtli yazılım ve donanım baęımlılıklarını ortadan kaldıran, bu sayede de yeni ürün ve servis geliştirme maliyetlerinde büyük tasarruflar saęlayan bir yazılım çözümdür (Alparslan, s.2).

Sanallaőtırma ilk IBM tarafından Ocak 1967’de bulunmuőtur. IBM Mainframe sistemleri olarak geçer. Ana bilgisayar belirli bir yazılım ile bölünerek birden fazla kullanıcıya aynı anda hizmet saęlar (Gökcen, 2010).

Sanallaőtırma, biliőtım kaynaklarının (iőtlemci, depolama, aę, bellek, platform, sunucu, masaüstü, uygulama vb.) gerçekte var olan kaynaęın deęil de, gerçekte kaynaęa dayandırılarak tanımlanmış olan soyut halinin, kullanıcılara sunulması olarak tanımlanabilir. Böylece gerçekte kaynak, göreceli olarak daha az kapasiteli çok sayıda sanal kaynak olarak kullanılabilir (TBD Kamu BİB, 2010, s.17).

Bilgisayar biliminde, sanal makine programları gerçekte bir bilgisayar sistemindeki gibi çalıőtıran mekanizmaların yazılım uyarlaması olarak tanımlanmıştır. Sanal makine, iőtletim sistemi ile bilgisayar platformu arasında bir sanal ortam oluőturur ve bu sanal ortam üzerinde yazılımların çalıőtırılabilmesine olanak saęlar (Wikipedia, 2013).

İlk sanal makine Gerald J. Popek ve Robert P. Goldberg tarafından 1974 yılında “Formal Requirements for Virtualizable Third Generation Architectures” isimli makale ile tanımlanmıştır (Wikipedia, 2014b).

Popek ve Goldberg (1974), sanal makineyi tanımlarken gerçekte makinenin soyut ve etkili bir kopyası olduęunu ifade etmektedirler. Sanallaőtırma teknolojileri

günümüzde çok farklı şekillerde kullanılmakta ve yeni kullanım alanları gelişmektedir. Yaygın olarak kullanılan sanallaştırma türleri; sistem sanal makineleri ve proses sanal makineleridir (Wikipedia, 2014c).

3.2. Sanallaştırma Çeşitleri

Sanal makineler işlevlerine göre; Sistem Sanal Makineleri ve Proses Sanal Makineleri olmak üzere 2 grupta incelenebilir.

3.2.1. Sistem Sanal Makineleri

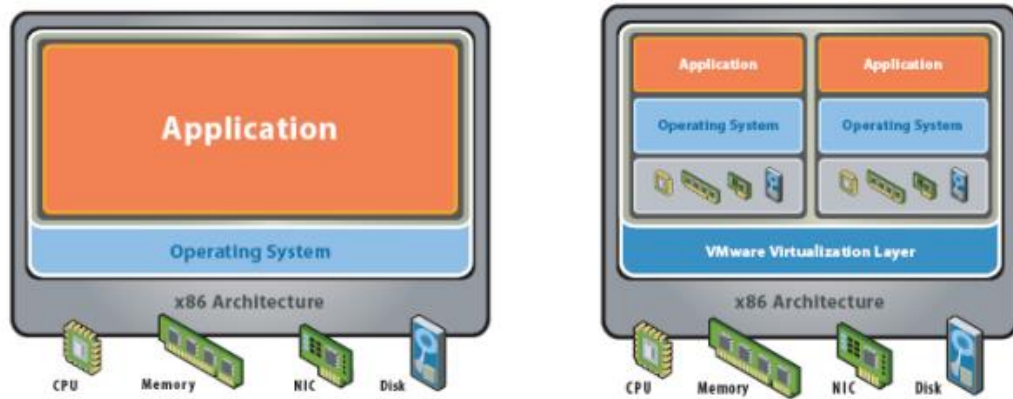
Bu tip sanal makineler kullandıkları fiziksel kaynağı (gerçek makine kaynaklarını) paylaşımlı olarak kullanırlar. Her bir sanal makine kendi işletim sistemine sahiptir. Bir arayüz yardımı ile donanımsal paylaşımlar ayarlanır. Bu tip sanal makineler donanım seviyesinde çalışabileceği gibi mevcut bir işletim sisteminin üzerinde, işletim sistemi kaynakları üzerinden de çalışabilir. Bu makalede ele almayı planlanan VMware ürünleri de bu sınıfta değerlendirilebilir (Alparslan, s.2).

3.2.2. Proses Sanal Makinesi

Herhangi bir işletim sistemi üzerinde modül olarak çalışır ve tek bir prosesin işletilmesine olanak sağlar. Kullanılmasındaki amaç platform bağımsız bir ortam sağlayarak üzerinde çalışacak programcıkların donanım ya da işletim sistemi limitlerine göre yeniden dizayn edilmesinin önüne geçmektir. Bu sanal makineyi aslında JAVA ve .NET platformlarından tanıyoruz. Java uygulamaları JVM (Java Sanal Makine), .NET uygulamaları ise CLR (Ortak Dil Çalışma-Zamanı) kullanırlar. Örneğin bizim yazdığımız bir java kodu derlendikten sonra hangi işletim sisteminde olduğuna bakılmaksızın konak işletim sistemi üzerinde kurulu olan JVM modülü tarafından çalıştırılır. Bu sayede yazılımcı Linux tabanlı makinelerde ayrı, Windows tabanlı makinelerde ayrı çalışacak uygulamalar yazmak zorunda bırakılmaz (Alparslan, s.2).

Sanallaştırma yazılımı, üzerinde yüklü olduğu donanımı, sanal makinelerin sanal kaynakları olarak organize eder ve paylaşır. İşte sanallaştırma yazılımları bu paylaşımı ne kadar etkin, akıllı ve sorunsuz yapabilirlerse o derece başarılı sayılırlar (Alparslan, s.2).

Şekil 3.1 Genel Sanallaştırma Mimarisi



Kaynak: (Alparslan, s.3)

3.3. Sanallaştırmanın Avantajları

Sanallaştırmanın avantajları aşağıda belirtilmiştir:

- i. Sunucu kapasitesini yüksek verimle kullanma imkanı sağlar.
- ii. İhtiyaç duyulduğunda çok hızlı bir şekilde yeni sunucu oluşturulabilir.
- iii. Kuruluşun ölçeğine göre donanım maliyetlerinde %50'ye varan düşüş sağlanır.
- iv. İhtiyaç olduğu anda test veya yazılım geliştirme için yeni sunucular oluşturma olanağı sağlanmış olur.
- v. Operasyonel kurulum ve bakım maliyetlerinde %80'e varan azalma görülür.
- vi. Herhangi bir problem anında, sanal sunucuları çok hızlı bir şekilde yeniden çalışır duruma getirebilme imkanı vardır.

vii. Merkezi yönetim ile tüm sunucuları tek bir merkezden izleme ve raporlama imkânı sağlanır.

viii. Sanal işletim sistemine kurulmuş olan herhangi bir uygulamayı, yeni bir ana bilgisayara geçilirken sanal işletim sistemini durdurup, işletim sistemi dosyasını yeni bilgisayara taşıdıktan sonra tekrar çalıştırarak kalınan yerden devam etme kolaylığı sağlanmış olur.

ix. Windows altında eski sürüm Windows, Linux, Mac veya Linux altında Windows, Mac (vs ...) çalıştırılabilmiş olur (Alparslan, s.3).

3.4. Sanallaştırma Yazılım Çeşitleri

Sanallaştırmada kullanılacak Yazılımlar “Sistem sanal makineleri” açık kaynak kodlu olanlar ve olmayanlar olarak iki gruba ayrılabilir.

3.4.1. Açık Kaynak Kodlu Sanal Makina Yazılımları

Açık kaynak kod mantığı ve lisansı ile dağıtılan bu yazılımlar başlıca VirtualBox, Xen, Bochs, CoLinux, FAUmachine, Hercules emulator , KVM, LilyVM, QEMU, SheepShaver olarak sıralanabilir.

3.4.2. Ticari Sanal Makina Yazılımları

Ticari anlamda başlıca kullanılan yazılımlar arasında VMware, Microsoft Virtual PC, VM/CMS, Parallels Workstation, vThere, Parallels Desktop for Mac, SVISTA, Trango, Virtual Iron Software gösterilebilir.(Alparslan, s.4).

3.5. Sanallaştırma Çözümlerine Geçen Kurumlar

Türkiye’de sanallaştırma çözümlerini kullanmaya başlayarak buna öncülük eden kurumlardan birisi Sosyal Yardımlaşma ve Dayanışma Genel Müdürlüğü olmuştur.

Sanallaştırma süreçleri ile ilgili kurumun resmi web sitesinden yapılan açıklamalara göre;

Sanallaştırma yapılırken mevcut uygulamalar olduğu gibi taşınmayıp güvenlik ve performans politikaları yeniden gözden geçirilerek uygulamaların güncel sürümleri ile yeni kurulumların yapıldığı belirtilmiştir. Sanallaştırma ile hizmet seviyesi performansında, erişilebilirlikte ve RAM, CPU kullanımlarında artış olduğu, sunucu sayısı ile paralel olarak altyapı ve bakım maliyetlerinde ise azalma sağlandığı ifade edilmiştir. 10 tane tam dolu kabin sanallaştırma projesi sonrasında tek kabin içinde birleştirilerek daha yönetilebilir bir yapıya kavuşulmuştur. SYDGM, sanallaştırma çözümleri ile daha yönetilebilir bir yapı kurmanın yanı sıra yedekli bir yapı oluşturmuştur. Sanallaştırmanın yüksek erişilebilirlik çözümü ile iş sürekliliği ve sistem kaynaklarının dinamik kullanılması çözümü ile kaynakların etkin kullanımı ve performans artışı sağlandığı da ifade edilmiştir (SYDGM, 2009).

Tablo 3.1 Sosyal Yardımlaşma ve Dayanışma Genel Müdürlüğü Sanallaştırma Öncesi ve Sonrası Genel Durum

	Sanallaştırma Öncesi	Sanallaştırma Sonrası
Kabin Sayısı:	10	2
Fiziksel Sunucu Sayısı:	40	8
Toplam Network Kablo Sayısı:	120	8
Toplam Enerji Kablo Sayısı:	20	4
Toplam Enerji Kullanımı:	43 KW	13 KW
İşletim Sistemi Kurma Süresi:	1 - 2 Saat	10 - 15 Dakika

Kaynak: (SYDGM, 2009)

Ayrıca Sosyal Güvenlik Kurumu, dünyanın en büyük ikinci Avrupa'nın ise en büyük sanallaştırma altyapısını kurmuştur. BT Haber yazarlarından Yusuf Çağlayan'ın haberine göre; Sun çözümleriyle gerçekleşen proje ile kurumun veri merkezi harcamalarını ciddi oranda azaltan bir yatırım sağladığı, yapılan tasarrufla

kurulum maliyeti SGK'ya kendini 1 yılda geri ödeyecektir. Medula, e-eczane, e-bildirge gibi uygulamalarda vatandaşların kesintisiz ve daha hızlı hizmet almasını sağlayan projede, Sun iş ortağı Servus da bütünleştirici şirket olarak yer almıştır. SGK sanallaştırma teknolojisiyle, 2400 fiziksel sunucunun getireceği toplam maliyetin yüzde 5'ine, daha büyük ölçekte bir yatırım gerçekleştirmiştir. Proje kapsamında SGK'nın Kızılay ve Mamak şubelerinde de sistem odaları kurulmuş ve olası bir felaket durumunda iş sürekliliğini sağlayacak yedekleme ve geri alma noktalarının da kurulduğunu ifade etmiştir (Çağlayan, 2009).

Sanallaştırma çözümlerinin yapılan yatırımlarda enerji tasarrufu sağlaması ve toplam satın alma maliyetlerinin düşük olması sebebiyle çok kısa sürelerde yapılan yatırımların kuruma geri döneceği ortadadır. Buradan hareketle, eğitim kurumlarımızda ve okullarımızda BT laboratuvarlarının yenilenmesinde ya da yeni yatırımlarda, sanallaştırma çözümleri göz önünde bulundurulmalıdır (Gürol ve Yavuzalp, 2011, s.5).

4. BULUT BİLİŞİM

4.1. Bulut Bilişim Nedir?

Bulut, İngilizce cloud kelimesinin çevirisi olup Türkçe'ye genellikle bulut olarak çevrilmekle beraber küme, yığın gibi anlamlara da gelmektedir. Telefon şebekelerinin altyapı bileşenlerinin giderek daha karmaşık hale gelmesi ile beraber, altyapının karmaşıklığının gizlenmesi amacıyla, şebeke diyagramlarında şebekelerin bazı kısımları bulut ile sembolize edilmeye başlanmış ve daha sonra bu sembol geniş ve karmaşık bir ağ olarak ifade edebileceğimiz internetin tümünün veya bir kısmının sembolize edilmesi için de kullanılır olmuştur (Özdaş, 2014, s.5).

Bulut bilişim; uygulamaların internet ortamında bulunan bir uzak sunucu üzerinden çalıştırılması ya da kullanıcıya ait verilerin uzak sunucu üzerinde her an erişilebilir şekilde bulundurulmasını sağlayan bir servis yapısı olarak tanımlanabilir. Web ara yüzü bilgiyi her yerde ve herkes için ulaşılabilir hale getirirken; bulut bilişim, bilgi işlem gücünü her yerde ve herkes için kullanılabilir hale getirmiştir (Henkoğlu ve Külcü, 2013, s.64).

Bulut bilişimin ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yapılan tanımı şu şekildedir;

Bulut bilişim, yapılandırılabilir bilişim kaynaklarından oluşan ortak bir havuza, uygun koşullarda ve isteğe bağlı olarak her zaman, her yerden erişime imkân veren bir modeldir. Söz konusu kaynaklar (bilgisayar ağları, sunucular, veri tabanları, uygulamalar, hizmetler vb.) asgari düzeyde yönetsel çaba ve hizmet alıcı-hizmet sağlayıcı etkileşimi gerektirecek kolaylıkta tedarik edilebilmekte ve elden çıkarılabilmektedir (BTK, 2013, s.9).

Bulut bilişim ile ilgili birçok tanım yapılmakla birlikte bulut bilişimin yeni bir bilişim hizmet modeli olması ve bu modelin hizmet alıcı tarafa BİT yatırımlarını

dilediği zaman arttırabilme veya azaltabilme ve BİT kaynaklarını kullandığı kadar ödeme (pay per use) imkanı sunması her tanımın ortak noktasıdır (BTK, 2013, s.3).

Çeşitli kuruluşlar tarafından bulut bilişimin karakteristik özelliklerine ilişkin bir takım standartlar belirlenmiş olup NIST (Mell and Grance, 2011) tarafından ortaya konan karakteristik özellikler listesi dünya genelinde yaygınlıkla kabul görmüştür. Bu karakteristik özellikler şunlardır (Özdaş, 2014).

Kaynakların ihtiyaca göre belirlenebilmesi: Müşteri tek taraflı olarak sunucu zamanı ve depolama alanı gibi bilişim kapasitelerini, ihtiyaç duyduğu anda hizmet sağlayıcısıyla iletişime geçmeden otomatik olarak artırıp azaltabilir. Bu sayede müşterilerin uygulamaları için ne kadar güçlü bir altyapıya ihtiyaç duyacaklarını önceden analiz etmeleri gerekmez.

Geniş ağ erişimi: Bilişim kapasitesi ağ üzerinden, mobil telefonlar, tabletler ve dizüstü bilgisayarlar gibi farklı platformlardan standart mekanizmalarla erişilebilecek şekilde sunulur.

Kaynak havuzu oluşturma: Hizmet sağlayıcısının bilişim kaynaklarından bir havuz oluşturularak çoklu kiralama mimarisi ile çok sayıda müşteriye sunulur ve bu yapıda farklı fiziksel ve sanal kaynaklar dinamik bir şekilde müşteri ihtiyacına göre kullanılır. Çoklu kiralama mimarisi, aynı altyapının çok sayıda müşteri tarafından kullanılabilmesine imkan tanıyan mimaridir. Müşterinin genel itibarıyla kendisine sağlanan kaynakların tam olarak nerede olduğuna ilişkin bilgisi ve kontrolü olmamakla beraber ülke, bölge veya veri merkezi bazında tercih yapabilmektedir. Bilişim kaynaklarına örnek olarak depolama alanı, işlemci gücü, RAM ve ağ bant genişliği verilebilir.

Anında esneklik: İhtiyaçla orantılı olarak anında genişleme ve daralma sağlanabilmesi için, bazı durumlarda insan müdahalesi gerekmeksizin, kapasite esnek bir şekilde artırılabilir veya artırılan kapasite iade edilebilir.

Ölçülebilir hizmet: Bulut bilişim sistemleri otomatik bir şekilde, hizmetin türüne uygun bir soyutlama katmanında (depolama alanı, işlemci gücü, bant genişliği ve aktif kullanıcı hesabı sayısı gibi) bir ölçümlene mekanizması yardımıyla kaynak kullanımını kontrol altında tutarak optimize edebilir. Kaynak kullanımı hem hizmet sağlayıcısı, hem de müşteri açısından şeffaflık sağlayacak şekilde gözlenebilir, kontrol edilebilir ve raporlanabilir.

Bulut sözcüğü dosyaların saklandığı konumu işaret etmektedir. Klasik bir algı olarak işleme ve saklama konumlarının aynı aygıtta bulunması durumu klişeleşmiştir. Ancak saklama boyutu bulutlara yani saklama ve altyapı hizmeti barındıran hizmetlere doğru kaymaktadır. Bu gidişin ilk öncü uygulamaları, İnternet sağlayıcıları tarafından, yedekleme amacıyla sunulan bulutlardır. Örneğin, Türkiye'de hizmet veren bir İnternet sağlayıcısı olan TTNET; TTNET Bulutu adlı hizmetle Türkiye piyasasına girmiştir. Google gibi uluslararası bilişim şirketleri ise; Google Docs gibi çevrim içi bilgi işleme özelliği sunan uygulamalar geliştirmiştir. Ayrıca; Microsoft ve Intel gibi büyük teknoloji firmaları da; bu teknolojiyi bilişim tüketicisine sunmuştur (Wikipedia, 2014d).

Bilgisayar kuramcıları tarafından İnternet'in geleceğinin bulut bilişimden geçtiği iddia edilmektedir. Buna göre gelecekte, bilgisayar hard disklerinin yerine çevrim içi bulutların kullanılacağı ön görüşü hakimdir. Bu bilişim aygıtlarında her hangi bir altyapı hazırlamadan, tamamen çevrim içi ağ vasıtasıyla işlevsel uygulamalara ulaşmak anlamına gelmektedir. Bu sektörün gelişmesiyle, özellikle bilişim teknolojisi tüketen toplumlarda birçok bilgi dağıtımını sağlayan firmanın önemli bir konuma geleceği, hatta sektördeki rekabetin hukuksal sorunlara neden olabileceği tartışılmaktadır. Çünkü tüm bilgi-işlem uygulamalarının çevrim içi altyapıya kaydırılmasına giden yol; kişisel bilgilere istenilmeyen erişimleri doğurabilme tehlikesini taşımaktadır (Turan, 2011).

4.2. Bulut Bilişim'in Tarihi

1960 ve 1970'lerde, bilişim ihtiyaçları sadece büyük ölçekli kurum ve kuruluşlar tarafından edinilebilen ve büyük çaplı ve yoğun işlemlerde kullanılan oda büyüklüğündeki ana bilgisayarlar (mainframe) kullanılarak karşılanmaktaydı. Üstelik söz konusu işlemler gerçek zamanlı olmamakla birlikte, kullanıcılar sadece kendileri ile ana bilgisayarlar arasında arayüz görevi gören terminaller aracılığı ile bu ana bilgisayarları kullanmaktaydılar (Mirzaoğlu, 2011, s.8).

1980'lerde, önceden işlevsiz olan terminaller, bellek ve işlemci kapasiteleri ile performanslarının artması ve fiyatlarının düşmesi sonucunda kişisel bilgisayar (PC) olarak kullanılmaya başlanmıştır. Önceleri ana bilgisayarların elinde olan kontrol, kullanıcıların kendi PC'leri üzerinde çeşitli kişisel işlemleri yapabilmeye başlamaları ile kullanıcıların eline geçmiştir. Bunun sonucu olarak, bilişim hizmetlerinin sunum modeli merkezilikten sıyrılıp, dağıtık bir hale gelmiş, PC donanımı, işletim sistemi ve kişisel uygulama yazılımı alanlarında çok büyük sektörler oluşmuştur (BTK, 2013, s.4).

1990'larda, PC'ler kaynakların paylaşımını ve performansların artırımını sağlayan yerel alan ağları (LAN) üzerinden haberleşmeye başlamıştır. Bunun sonucu olarak kurum ve kuruluşlar kendilerine ait sunucu bilgisayarlardan oluşan bir sistem odası buldurmaya ve işletmeye başlamışlardır (BTK, 2013, s.5).

1990'ların sonunda ise, uzaktaki kaynakları ve uygulamaları paylaşmak amacıyla birbirlerine bağlanan LAN'lar İnternet'i oluşturmuşlardır (BTK, 2013,s.5). İnternetin ortaya çıkışıyla beraber paket program halinde satılan yazılımların yerini ihtiyaç duyulduğunda hizmet olarak satın alınan yazılımlar almaya başlamıştır. Eş zamanlı olarak genişbant altyapılarının da gelişmesiyle birlikte daha önceleri tartışma konusu yapılmış olmakla beraber etkin bir çözüm olmadığı düşünülen bulut bilişim kavramı sıklıkla gündeme gelmeye başlamıştır (Özdaş, 2014, s.8).

İnternetin olgunlaşarak bilgi amaçlı internet sitelerinin yerini hizmet amaçlı internet sitelerine bırakmasıyla beraber yazılımlar paket program olarak satın alınmak

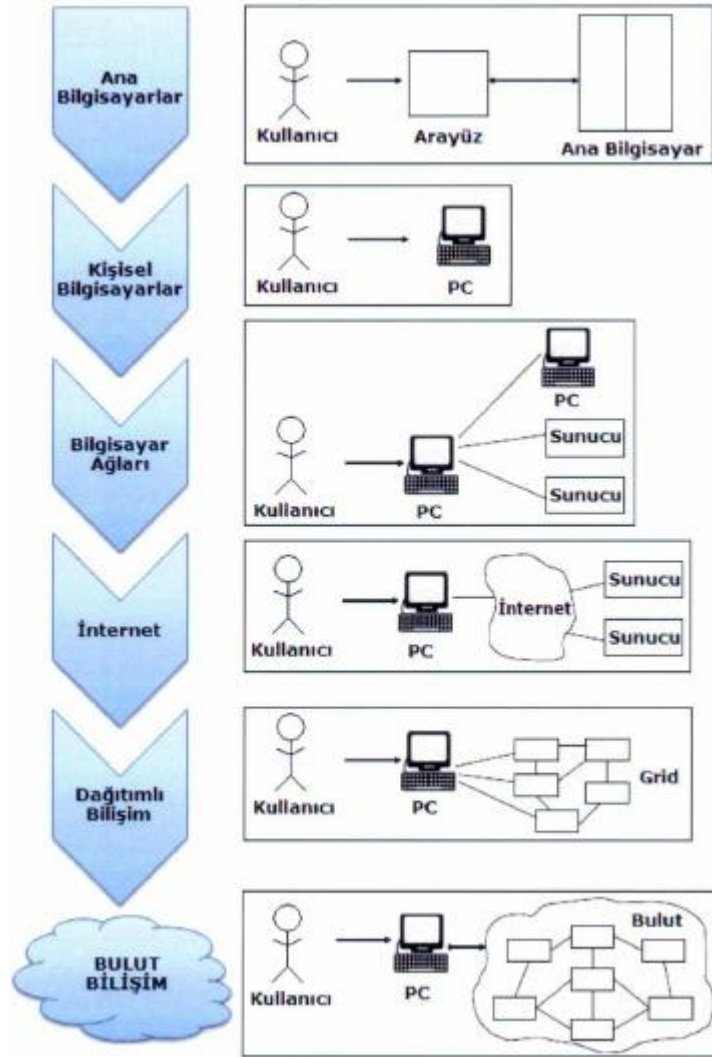
yerine internet üzerinden hizmet olarak sunulması esasına dayanan servis olarak yazılım yaygınlaşmaya başlamıştır. İnternetin kullanım oranının artması ve servis olarak yazılımın avantajlarının firmalarca fark edilmesi ile birlikte hem genişbant altyapıları ortaya çıkarak gelişmiş ve internet ortamı ile yerel ağ ortamı arasındaki performans farkı giderek azalmış, hem de internet tabanlı programlama dilleri ve ara katmanları geliştirilerek internet üzerinden servis olarak sunulan yazılımların daha kolay geliştirilebilmesi mümkün hale gelmiştir. Sanallaştırma teknolojilerinin, 1990'lı yıllardan beri biliniyor olmakla beraber, kullanımının yaygınlaşması ve sanallaştırmaya imkan veren yazılım çözümlerinin yeterince olgunlaşması ise bulut bilişime geçiş sürecindeki diğer önemli bir gelişmedir (Özdaş, 2014, s.8-9).

2000'lerde, bilişim hizmetlerinde satın alma, bakım, işletim, iklimlendirme, enerji, güvenlik, ilgili personel vb. masraflarını azaltmaya yönelik arayışlar, bilişim hizmetlerinin dış kaynak kullanımı (outsourcing) yoluyla alınması fikrini ortaya çıkarmış ve bu bağlamda, dağıtımli bilişim (grid computing), kamu hizmeti bilişimi (utility computing) ve barındırma (hosting) gibi hizmetler gelişmiştir (BTK, 2013, s.5).

Dağıtımli bilişim, homojen olmayan BİT kaynaklarının (sunucular, depolama sistemleri ve ağ elemanları vb.) ortak bir havuzda toplanması (ızgara-grid) ve bu havuzdan oluşan sanal sistemin tek bir bilişim sistemi şeklinde kullanıcılara sunulmasıdır. Bu uygulamaların, "kullandığın kadar öde" mantığıyla, kamuya açık veya bir kuruluşa özel olarak sunulması ise kamu hizmeti bilişimi (utility computing) olarak tarif edilmektedir. Ancak, belli oranda çözüm sağlayabilen dağıtımli bilişim, kamu hizmeti bilişimi, barındırma ve benzeri hizmetler, kendi kendine hizmet (self service) ve ihtiyaca göre kapasite arttırma gibi özellikleri sağlayamamış ve bulut bilişimin doğuşuna zemin hazırlamıştır. Bilgi teknolojilerindeki gelişim sonucu işlemcilerde ve genişbant bilgisayar ağı erişimindeki hızlanma ve fiyatlardaki ucuzlama, sanallaştırma teknolojilerinde, yönetim ve süreç otomasyonunda hızlı gelişme ve veri merkezlerinin endüstriyel ölçekli bilişim hizmeti fabrikalarına dönüşmesi bulut bilişim modelinin doğmasına yol açmıştır. Ana bilgisayarlardan, bulut bilişimin doğuşuna kadar olan gelişim

süreci Şekil 4.1'de gösterilmektedir (Mirzaoğlu, 2011, s.10-11).

Şekil 4.1 Bulut Bilişimin Gelişimi



Kaynak: (Mirzaoğlu, 2011, s.11).

4.3. Bulut Bilişim'in Avantaj ve Dezavantajları

Bulut bilişim, önemli avantajları sebebiyle dünya genelinde artan bir ilginin odağı haline gelmiştir. Özellikle en öne çıkan avantajların esneklik, tasarruf ve performans oluşu, dünya genelinde meydana gelen ve etkileri devam etmekte olan ekonomik krizler sebebiyle, maliyetleri azaltma yoluna giden tüm kuruluşların

bulut bilişime sıcak bakmalarına sebep olmaktadır. Harris ve Alter tarafından bulut bilişimin en çok kullanıldığı sekiz ülkede (ABD, İngiltere, Almanya, Fransa, Singapur, Japonya, Çin ve Brezilya) yapılan bir araştırmaya göre, bulut bilişimin uzun vadede en önemli avantajının yüzde 60 ile esneklik, ikinci önemli avantajının ise yüzde 54 ile tasarruf olduğu ortaya çıkmıştır (Özdaş, 2014, s.29).

Bulut bilişim servisleri bireysel ya da kurumsal olabilen kullanıcılar için aşağıda bazı örnekleri verilen avantajları sunabilmektedir (Microsoft, 2012):

- Düşük donanım maliyeti,
- Gelişmiş performans,
- Düşük yazılım maliyeti,
- Anında güncelleme,
- Sınırsız depolama kapasitesi,
- Artırılmış veri güvenliği,
- İşletim sistemleri arasında geliştirilmiş uyum,
- Artırılmış dosya formatı uyumu,
- Grup çalışması (BTK, 2013, s.10).

Bulut bilişim servisleri bireysel ya da kurumsal olabilen kullanıcılar için aşağıda bazı örnekleri verilen dezavantajlara sahip olabilmektedir (Harris, 2012):

- Sabit internet bağlantısı gerektirmesi,
- Düşük hızlarda düzgün çalışmaması,
- Uygulamanın yavaş çalışması,
- Güvenlik açıkları,
- Sistem güncellemeleri,
- Deneyimsiz bulut operatörü,
- Kullandığınız programın özellikleri (BTK, 2013, s.10).

Bulut Bilişim'in Risklerini ve Faydalarını genel olarak Şekil 4.2'deki gibi gösterebiliriz.

Şekil 4.2 Bulut Bilişim'in Riskleri ve Faydaları



4.4. Bulut Bilişim Hizmet Modelleri

NIST tarafından yapılan bulut bilişim tanımına göre, hizmet sağlayıcılar, hizmet alıcılara üç farklı modele göre bulut bilişim hizmeti sunmaktadır (Mirzaoğlu, 2011, s.19). Bu modeller; Altyapı Hizmeti (IaaS-Infrastructure as a Service), Platform hizmeti (PaaS-Platform as a Service) ve Yazılım hizmeti (SaaS-Software as a Service)'dir.

4.4.1. Alt Yapı Hizmetleri (IaaS)

Bulut bilişimin en fazla esneklik sunan yazılım hizmet modeli olan servis olarak altyapı modelinde, hizmet alıcıya işlemci gücü, depolama alanı, veritabanı gibi en temel bilişim kaynakları geleneksel sunuculara çok benzer şekilde sunulmakta, hizmet alıcının kendisine tahsis edilmiş sunucu üzerinde hemen hemen her türlü yazılımı yükleyip çalıştırabilmesine izin verilmektedir. Sunucu altyapısının sanallaştırma kullanılarak kiralanması, kullanım açısından bir dezavantaj oluşturmamaktadır. Bu altyapıdan kiralanılan sunucu ile satın alınarak yerel sunucu odasına kurulan sunucunun işlevsellik açısından hemen hemen hiçbir farkı yoktur. Hizmet alıcının tek yapması gereken, ihtiyaç duyduğu işlemci gücü, dahili bellek,

depolama alanı ve sunucu üzerinde hangi işletim sisteminin çalışacağını belirlemektir. Bu modelde temel bilişim kaynaklarının bir sanallaştırma ortamı yardımıyla doğrudan sunulması sebebiyle model bazı kaynaklarda servis olarak donanım (hardware as a service, HaaS) veya kaynak bulutu (resource cloud) olarak da tanımlanmaktadır (Özdaş, 2014, s.28).

Ağ üzerinden güvenli erişim imkânı sunan dinamik veri depolama alanı (örneğin; Amazon S3, SQL Azure), işlemci kaynaklarının sanal olarak sunulması (örneğin; Amazon EC2, Zimory, Elastichosts) ve ağ hizmetleri gibi servisler, bulut bilişim alt yapı servisi örnekleridir. Kullanıcının bulut alt yapısında yönetim işlevi bulunmamaktadır. Fakat işletim sistemi, veri depolama alanı ve sınırlı olarak ağ bileşenleri (güvenlik duvarı gibi) üzerinde kontrol sağlayabilmektedir (Henkoğlu ve Külcü, 2013 ,s.66).

4.4.2. Platform Hizmeti (PaaS)

Platform Hizmeti modelinde, hizmet sağlayıcı tarafından sunulan programlama dilleri, yazılım kütüphaneleri, servisler ve araçlar kullanılarak, yazılımın bulut altyapısına uygun şekilde geliştirilerek bu altyapı üzerinde çalıştırılması söz konusudur (Özdaş, 2014, s.27).

Geliştirilen uygulama ile ilgili alt yapı, ortam ve diğer servisler bulut hizmet sağlayıcı tarafından sağlanır. Kullanıcının sunucu, işletim sistemi, veri depolama alanı üzerinde yönetim işlevi bulunmamaktadır. Sadece geliştirilen uygulamalar üzerinde kontrol sağlayabilmektedir. Bir bulut hizmet sağlayıcısı üzerinde geliştirilen uygulama, standartların bulunmaması nedeniyle sadece geliştirilen platform üzerinde kullanılabilir (Henkoğlu ve Külcü, 2013 ,s.65-66). Bu servislere örnek olarak; Google Apps Engine, Microsoft, Force.com, Windows Azure ve Salesforce.com verilebilir.

4.4.3. Yazılım Hizmeti (SaaS)

Yazılım hizmeti, bulut altyapısı üzerinden uygulamaların hizmet olarak sunulduğu modeldir. Servis olarak yazılımda e-posta, doküman işleme yazılımı ve benzeri yazılımlar internet üzerinden birer hizmet olarak sunulur ve hizmet kullanım bazlı olarak ücretlendirilir. Yazılım hizmetinde alıcının, hizmetin sunumu için gerekli olan sunucular, veri tabanları, işletim sistemleri, depolama alanları gibi bileşenlerden hiçbirini kontrol etme yetki ve sorumluluğu yoktur. Hizmet alıcısına sadece hizmet olarak aldığı uygulamaya has konfigürasyon ayarlarını yapabilme yetkisi verilir. Bu modelde sistem yöneticilerinin rolleri tümüyle değişmektedir. Örneğin yerel sunucularda sunucuların bakımı, onarımı, güvenliği, uygulamaların bakımı ve güncellenmesi, gerektiğinde altyapının uygulama ihtiyaçlarına uygun şekilde yeniden tasarlanması, hizmet devamlılığının temini, hizmet kalitesi gibi sistem yöneticisinin sorumluluğunda olan pek çok iş yükü, üçüncü bir tarafın sorumluluğuna geçmektedir (Özdaş, 2014, s.26).

Sunulan hizmetlerden bazıları; doküman paylaşımı (Google, Microsoft, Adobe), e-posta (Google, Yahoo), ofis yazılımları (Thinkfree, Zoho, Google), satış otomasyonu ve müşteri yönetimidir (Oracle, Salesforce.com) (Yıldız, 2009, s.8).

4.4.4. Bazı Bulut Depolama Hizmetleri

Bulut depolama hizmetlerine örnek olarak; Dropbox, Google Drive, SkyDrive, iCloud, Ubuntu One, Google Picasa Web Albums, Yandex.Disk, Mobile Me, iOmegaCloud, Box.net, Tnet Netdisk ve Slax Drive verilebilir (Wikipedia, 2014d).

4.5. Bulut Bilişim Yerleştirme Modelleri

Bulut Bilişim yerleştirme modelleri 4 farklı yapıya sahiptir. Genel Bulut, Topluluk Bulutu, Hibrit Bulutu ve Özel Buluttur.

4.5.1. Genel Bulut

Genel bulut uygulamaları, depolama ve diğer kaynaklar bir hizmet sağlayıcı tarafından genel kullanıcılara sunulmaktadır. Bu hizmetler ücretsiz erişimlidir veya kullanım başına ödeme modeliyle ücretlendirilmektedir. Genel olarak, Amazon AWS, Microsoft ve Google gibi genel bulut sağlayıcıları kendi altyapılarını işletmekte ve sadece internet aracılığıyla erişim sunmaktadırlar (IDC, 2008).

4.5.2. Topluluk Bulutu

Topluluk bulutu, bulut bilişimin hedef, güvenlik gereksinimi, politika ve uyumluluk gereksinimleri gibi ortak ihtiyaçlara sahip belli bir müşteri veya organizasyon topluluğunun özel kullanımına sunulan mimari çeşididir. Bulut bilişim altyapısı toplulukta bulunan bir veya daha fazla organizasyon tarafından sahip olunarak yönetilebileceği gibi bu topluluk için üçüncü bir tarafça da yönetilebilir (Özdaş, 2014, s.22).

4.5.3. Hibrit (Karma) Bulut

Hibrit bulut, iki veya daha fazla özel bulut, topluluk bulutu veya kamuya açık bulut, kendi aralarında veri ve uygulama transferine imkan veren standart veya buluta özgü teknolojiler aracılığıyla bir araya gelerek yeni bir bulut altyapısı oluşturmaktadır (Mirzaoğlu, 2013, s.23).

Karma bulut mimarisi çoğunlukla hassas verilerin kontrol altında tutulması ve aynı zamanda dış kaynakların da kullanımıyla daha yüksek bir esneklik sağlanması amacıyla verinin sadece bir kısmının üçüncü tarafa açılmasının uygun olduğu durumlarda tercih edilmektedir (Özdaş, 2014, s.23).

Hibrit bulut mimarisi, şirketlerin ve bireylerin internet bağlantısına gerek olmadan yerel olarak acil kullanılabilme kabiliyeti ile hata tolerans derecesini yükseltmeyi

başarmaktadır. Hibrit bulut mimarisi hem şirket içi kaynaklara hem de dışarıdan (uzak) sunucu tabanlı bulut altyapısına gereksinim duymaktadır (Stevens, 2011).

4.5.4. Özel Bulut

Özel bulut, bulut bilişim altyapısının sadece bir kuruluşun erişimine açık olan türüdür. Bu bulut mimarisinde altyapı kuruluşun yerel veri merkezinde tutulabileceği gibi, bu kuruluş adına üçüncü bir tarafça da barındırılabilir. Tek bir kuruluşa hizmet verilmesi esas olmakla birlikte, kuruluş bünyesindeki çok sayıda birim bu hizmetten ayrı bir müşteri gibi faydalanabilmektedir. Özel bulutta da açık bulutta olduğu gibi bulut bilişimin performans ve mimari altyapıya ilişkin tüm karakteristik özellikleri korunmaktadır. Özel bulut ile işlemci ve depolama alanından tasarruf sağlanmakta, yönetim tek merkezden kolaylıkla yürütülebilmekte, verilere izin verilen her noktadan kontrollü erişim mümkün olmakta, ihtiyaca göre kaynak artırımı/azaltımı kolaylıkla gerçekleştirilebilmekte ve uygulamaların daha az sayıda sunucu ile çalışabilmeleri sonucu yüksek oranda maliyet ve enerji tasarrufu sağlanmaktadır (Özdaş, 2014, s.21).

4.6. Bulut Bilişim Mimarisi

Bir bulut bilişim sisteminden bahsederken ön taraf ve arka taraf olmak üzere iki kategoride değerlendirmek gerekmektedir. Bu iki kısım birbirlerine bir ağ, genellikle internet ile bağlıdır. Ön taraf bilgisayar kullanıcısı veya müşteri tarafıdır. Arka taraf ise sistemin bulut kısmıdır.

Ön taraf, istemcinin bilgisayarını (veya bilgisayar ağını) ve bulut bilişim sistemine erişim için gerekli olan uygulamayı içermektedir. Bütün bilişim sistemleri aynı kullanıcı ara yüzüne sahip değildir. Web tabanlı e-posta programları gibi hizmetler herhangi bir web tarayıcısı kullanarak çalışabilir. Diğer sistemler istemcilere ağ erişimi sağlayan birbirinden farklı uygulamalar sağlamaktadırlar.

Sistemin arka tarafında bilişim hizmetlerinin bulutunu oluşturan çeşitli bilgisayarlar, sunucular, veri depolama sistemleri vardır. Teoride, bir bulut bilişim sistemi pratik olarak veri işlemeden video oyunlarına kadar bütün bilgisayar programlarını içerebilmektedir. Genellikle her bir uygulamanın kendine ait bir sunucusu vardır.

Bir merkez sunucusu, sistemi yönetmekte, trafiği ve istemci taleplerini her şeyin yolunda gittiğinden emin olmak için monitörlmektedir. Protokoller denilen bir takım kuralları izlemekte ve middleware denilen özel bir yazılım kullanmaktadır. Middleware, ağ bağlantılı bilgisayarların birbiriyle iletişim kurmasını sağlamaktadır. Çoğu durumda sunucular tam kapasite çalışmazlar. Bu kullanılmayan işleme gücünün boşa gitmesi manasına gelmektedir.

Eğer bir bulut bilişim şirketi birçok istemciye sahip ise, depolama alanı için yüksek bir talep olması muhtemeldir. Bazı şirketler yüzlerce dijital depolama cihazı gereksinimi duymaktadır. Bulut bilişim sistemleri bütün istemcilerinin bilgilerini koruyabilmek için asgari çiftli depolama cihazları bulundurmalıdır. Bunun sebebi bu cihazlar aynı bilgisayarlar gibi kimi durumlarda arızalanmaktadır. Bir bulut bilişim sistemi bütün istemcilerinin bilgilerinin kopyasını oluşturmalı ve diğer depolama cihazları üzerinde depolamalıdır. Bu kopyalar merkez sunucunun yedek makinelerine erişmesine ve verileri geri getirmesine izin verir aksi takdirde verilerde kayıplar yaşanabilmektedir (Strickland).

4.7. Bulut Bilişimin Güvenliği

Bulut bilişim popülerliğini artırdıkça, bu yeni modelle ortaya çıkan güvenlik sorunları endişeleri artırmıştır. Geleneksel koruma mekanizmalarının etkinliği ve verimliliği yeniden değerlendirilmektedir, çünkü bu yeni yerleştirme modelinin özellikleri büyük ölçüde geleneksel mimarilerden farklılık arz etmektedir.

Dağıtık mimarilerde güvenlik, geleneksel mimarilerden daha kapsamlı bir bakış açısıyla ele alınması gereken bir konudur. Sistem bileşenlerinin birbirlerine daha gevşek bir yapıda bağlı olduğu bu mimarilerde güvenlik açısından risk oluşturan bileşenler incelenir ve hizmet kalitesi ve sürekliliğini etkileme durumuna göre çoktan aza doğru sıralanarak bu bileşenlerin taşıdıkları riskler azaltılmaya çalışılır. Bulut bilişim ve geleneksel bilişim sistemleri güvenlik açısından karşılaştırıldığında, bulut bilişimin olumlu etkilerinden de bahsetmek mümkündür. Yüksek düzeyli güvenlik önlemlerinin merkezi olarak alınabilmesi ve ölçek ekonomisi ile yüksek nitelikli güvenlik uzmanlarının istihdam edilebilmesi maliyet etkin bir şekilde mümkün olmakta, bu sebeple bulut bilişimin daha güvenli bir ortam sağlama potansiyeli bulunmaktadır (Özdaş, 2014, s.45).

Bulut bilişimin hizmet sağlayıcısına güvenilebilirlik açısından da bazı riskleri bulunmaktadır. Bulut bilişim hizmet sağlayıcılarının hizmetlerinde kesintiler yaşanabilmektedir. Yerel sunuculara sahip bir kuruluştaki yönetim ve yetki kuruluşu kendisinde iken, bulut bilişimde yönetim ve yetki paylaşılmaktadır. Bulut bilişim hizmetlerinde hizmet sağlayıcısına güven söz konusu olup kritik düzeydeki uygulamalar için alınabilecek tek önlem, bulut bilişim hizmet sağlayıcısının doğru seçilmesi, gerekirse iki alternatifli çözümlerin tercih edilmesidir (Özdaş, 2014, s.45).

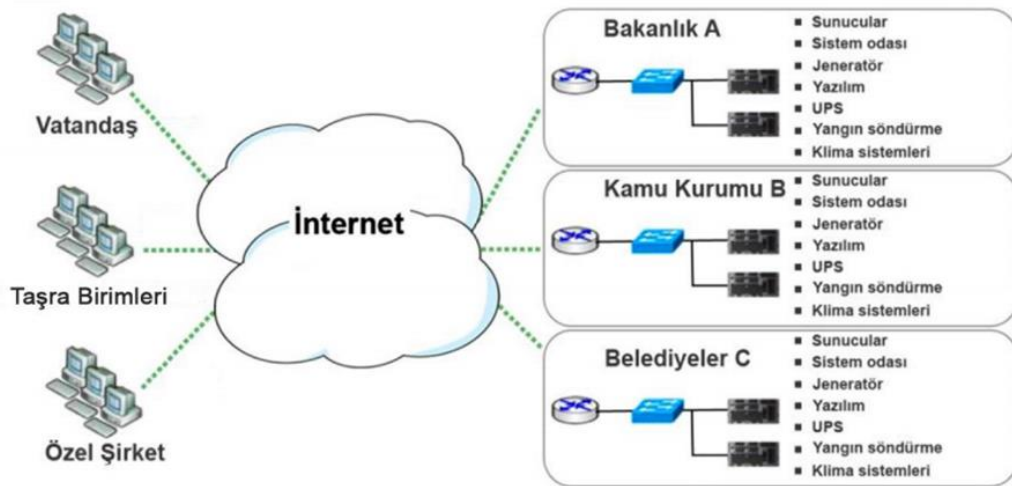
5. KAMU ENTEGRE VERİ MERKEZİ

5.1. Kamu Entegre Veri Merkezi için Bilişim Yapısı

5.1.1. Mevcut Kamu Bilişim Yapısı

Mevcut kamu bilişim yapısında, her bir bakanlık, kamu kurumu ve belediyelere ait sunucu, sistem odası, jeneratör, yazılım, UPS, yangın söndürme ve klima sistemleri bulunmaktadır.

Şekil 5.1 Mevcut Kamu Bilişim Yapısı



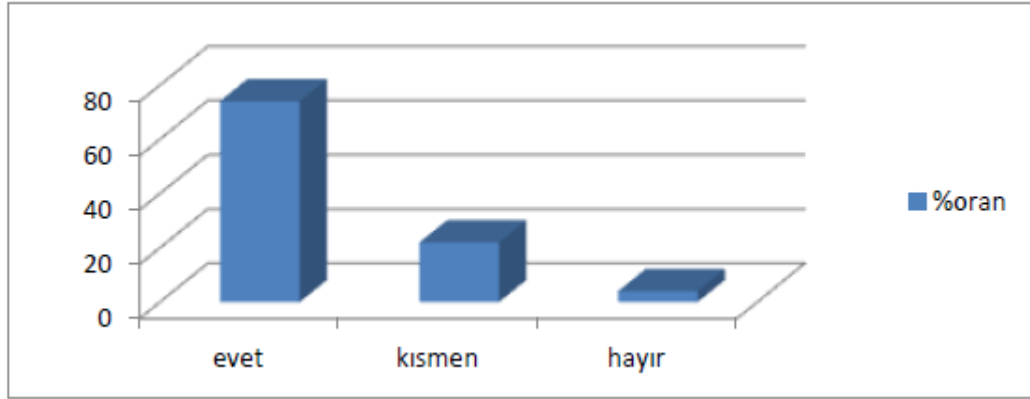
Kaynak: (UDHB, 2013, s.12)

Her kamu kurum ve kuruluş kendi bünyesinde bulunan veri merkezlerini kullanmaktadır. Bilgi paylaşımları da kurumlar arasında yapılan anlaşma ve protokollere göre yapılmaktadır. Kamu bilişim merkezlerinin kullanabileceği ortak veri merkezleri henüz ülkemizde bulunmamaktadır.

Kamuda hemen hemen tüm kurumlarda tam donanımlı bir veri merkezi bulunmaktadır. (Şekil 5.2) Bu merkezlerin sağlıklı çalışabilmesi için hem yüksek nitelikte insan gücüne ihtiyaç duyulmakta hem de eskiyen ve teknolojinin gerisinde

kalan yatırımlar her kurum tarafından ayrı ayrı satın almalar yoluyla yenilenmektedir (TBD, 2013, s.33).

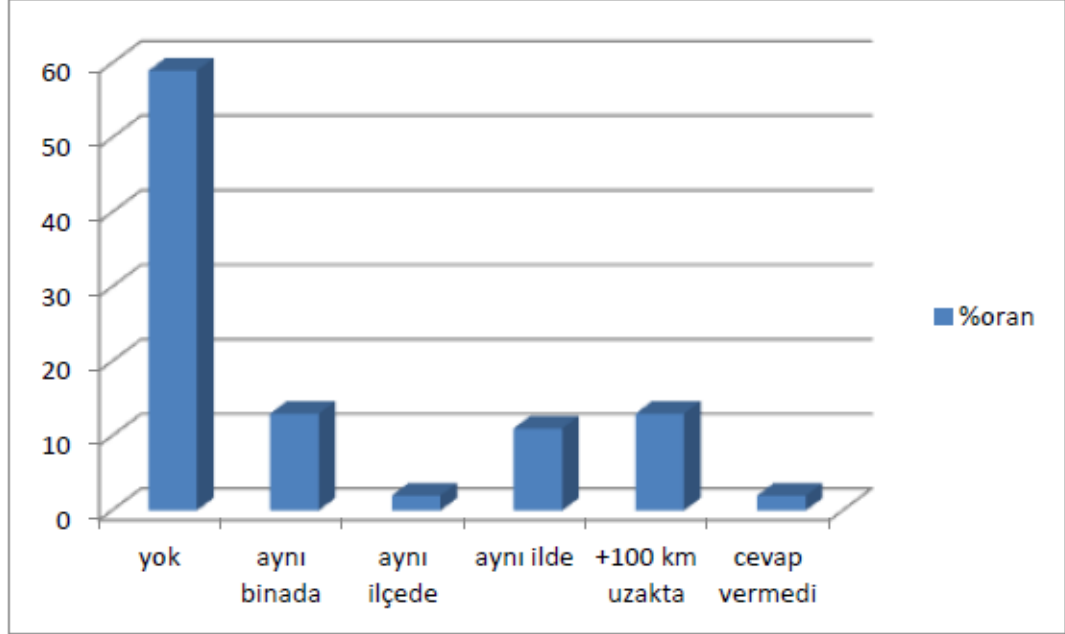
Şekil 5.2 Tam Donanımlı Veri Merkezi Bulunan Kamu Kurumları



Kaynak: (TBD, 2013, s.33)

Kamu kurumlarının büyük çoğunluğunda bilişim sistemlerinde felaket kurtarma merkezi bulunmamaktadır. Kamu kurumlarının %40'ına yakın bir bölümünde, felaket durumlarında veri kaybını önlemek ve bilişim sistemlerinin sürekliliğini sağlamak üzere, ayrıca donanım yatırımları yapılmakta ancak bu yatırımların çoğu (%66) mekan ve altyapı sıkıntısından dolayı olması gereken yerleşelerde tutulamayarak büyük risk alınmaktadır. Felaket kurtarma merkezlerinin sadece üçte biri, olması gereken şekilde en az 100 km. uzakta kurulabilmiştir (TBD, 2013, s.33)

Şekil 5.3 Felaket Kurtarma Merkezi Bulunan Kamu Kurumları



Kaynak: (TBD, 2013, s.34)

Türkiye Kamu Sektöründe Bulut Bilişim Yapısı'nı gösteren IDC'nin yayınlanmış olduğu raporda kurumların %25'nin bulut servisleri kullandığını, %17'sinin ise bulut servisleri kullanacağı belirtilmektedir. (Şekil 5.4)

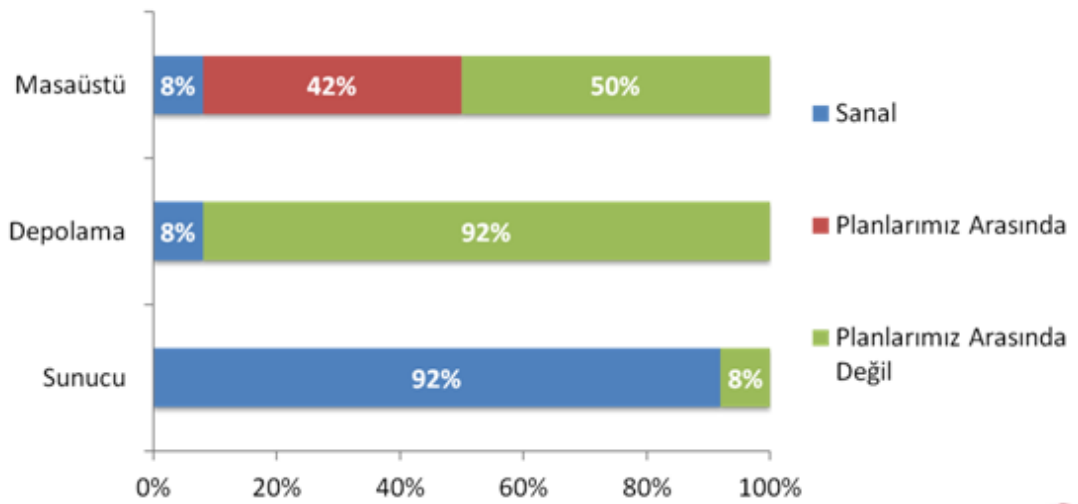
Şekil 5.4 Kamuda Bulut Servislerinin Kullanımı



Kaynak: (IDC)

IDC raporuna göre, BT altyapılarında sanallaştırma kullanım oranı aşağıdaki gibidir:

Şekil 5.5 BT Altyapılarında Sanallaştırma Kullanım Oranı



Kaynak: (IDC)

Türkiye'deki kamu kurumlarındaki bilişim alt yapısının sanallaştırılmasına örnek olarak Aile ve Sosyal Politikalar Bakanlığı, Ulusal Yargı Ağı Projesi (UYAP), E-Sağlık uygulamaları altyapısı verilebilir.

Aile ve Sosyal Politikalar Bakanlığı, Sosyal Yardımlaşma ve Dayanışma Genel Müdürlüğü'nün sunduğu bilişim hizmetlerinin genişlemesine paralel olarak, bilgi sistemleri altyapısının yeniden gözden geçirilmesi ve düzenlenmesi ihtiyacı doğmuştur. Bu ihtiyaç kapsamında; sunucu/istemci altyapısı içinde sorun çözüm sürecinin standardize edilmesi ve kısaltılması, daha güvenli bir sunucu/istemci altyapısı oluşturulması, sistemlerin yönetimini sağlayarak oluşacak arızalarda proaktif müdahale oluşturulması amaçlarına yönelik çalışmalar yapılmıştır (SYDGM, 2009).

Bilgi sistemleri altyapısının en yeni teknolojilerle yeniden yapılandırılması, sunucu/istemci altyapısı içinde sorun çözüm sürecinin kısaltılması ve daha güvenli bir sunucu/istemci altyapısı oluşturulması hedeflenmiştir.

Sanallaştırma sayesinde SYDGM olarak elde edilen kurumsal katma değerler aşağıdaki gibidir (Yeşilirmak, 2010, s.50-51):

- Kurumun tüm servisleri sanal ortama taşınmıştır.
- RAM, CPU kullanımlarında artış; altyapı ve bakım maliyetlerinde azalma sağlanmıştır.
- 10 tane tam dolu kabin sanallaştırma projesi sonrasında devre dışı bırakılmış ve tek kabin içinde yeni blade sunuculara aktarılarak daha yönetilebilir bir yapı oluşturulmuştur.
- Boşa çıkarılan sunucular geliştirilen yeni projelerde ihtiyaç duyulan veri paylaşımlarının sağlanabilmesi adına talepte bulunan kamu kurumlarına hibe edilerek kamu kaynaklarının atıl kalması engellenmiştir.

- Sunucu/istemci altyapısı içinde sorun çözüm süreci standardize edilmiş ve kısaltılmıştır.
- Daha güvenli bir sunucu/istemci altyapısı oluşturulmuş, güvenlik altyapısı yeniden tasarlanmış, altyapı da yedekli bir şekilde donatılmış, yedekli yapı ile iş sürekliliği sağlanmıştır.
- 5 binden fazla kullanıcıya hizmet veren kurumda performans artışı sağlanmıştır.

SYDGM'nin sanallaştırma öncesi ve sonrası durumu Tablo 5.1 'deki gibidir.

Tablo 5.1 Aile ve Sosyal Politikalar Bakanlığı Sanallaştırma Öncesi ve Sonrası Genel Durum

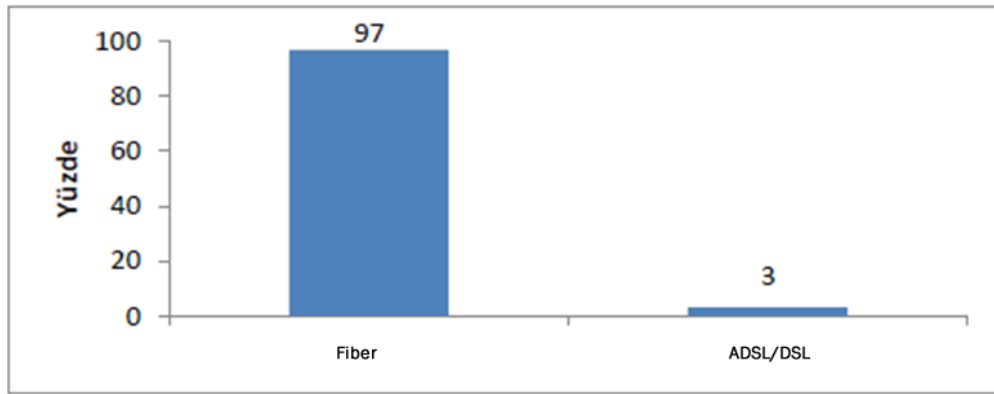
	Sanallaştırma Öncesi	Sanallaştırma sonrası
Kabin Sayısı	10	2
Fiziksel Sunucu Sayısı	40	8
Toplam Network Kablo Sayısı	120	8
Toplam Enerji Kablo Sayısı	20	4
Toplam Enerji Kullanımı	43 KW	13 KW
İşletim Sistemi Kurma Süresi	1-2 Saat	10-15 Dakika

Kaynak: (SYDGM, 2009)

Kalkınma Bakanlığı tarafından, Kamu kurumlarının bulut bilişim açısından mevcut durumunun sayısal verilerle desteklenerek ortaya konması ve kamu bilgi işlem birimlerinin bulut bilişime bakış açılarının kısmi ölçüde de olsa gözlenmesi amacıyla 2012 yılında, 43 merkezi kamu kurumu ve 34 üniversitenin cevap verdiği bir anket çalışması yapılmıştır. Anket çalışmasından elde edilen önemli bulgular aşağıdadır:

Anket soruları ile ağırlıklı olarak kurumun mevcut bilişim altyapısı bulut bilişim bağlamında ortaya konmuştur. Bulut bilişim, yüksek veri aktarım hızına sahip bir ağ altyapısı gerektirmektedir. Günümüzde kullanılan internet bağlantı türlerine bakıldığında, fiber kablolar ile gerçekleştirilen bağlantıların bulut bilişim için yeterli olduğu söylenebilir. Kurumların yüzde 97'sinde fiber ağ altyapısı kullanılmaktadır (Şekil 5.6) (ÖZDAŞ, 2013).

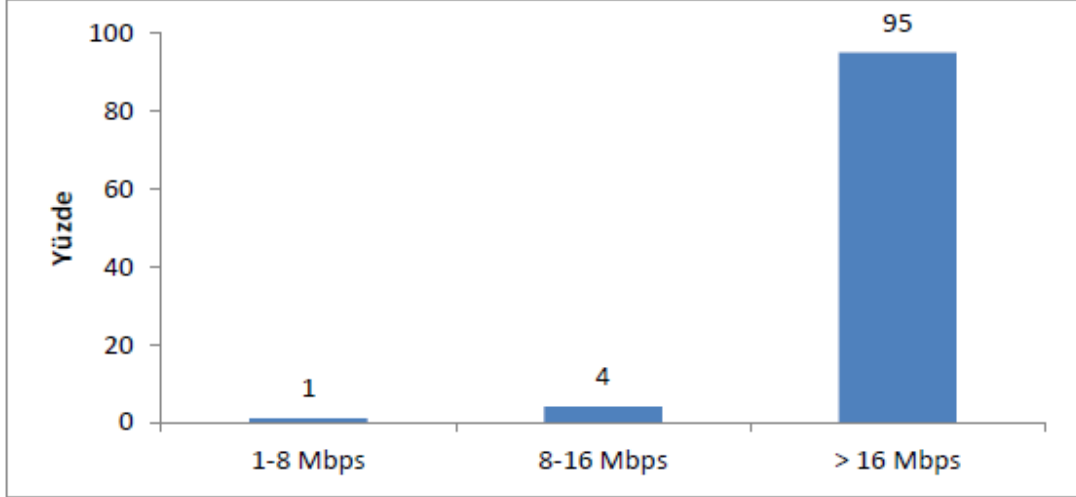
Şekil 5.6 Kurumlarda İnternet Türü Dağılımı



Kaynak: (ÖZDAŞ, 2013)

ADSL/DSL altyapısına göre çok daha hızlı bir altyapı olan fiber altyapısının varlığı, bulut bilişimin uygulanabilmesinin en önemli ön şartlarından biridir. İnternet bağlantı hızlarına bakıldığında, bağlantı türü ile paralel şekilde, kurumların yüzde 95'inin 16 Mbps'den daha hızlı internet bağlantı hızına sahip olduğu görülmektedir (Şekil 5.7) (ÖZDAŞ, 2013).

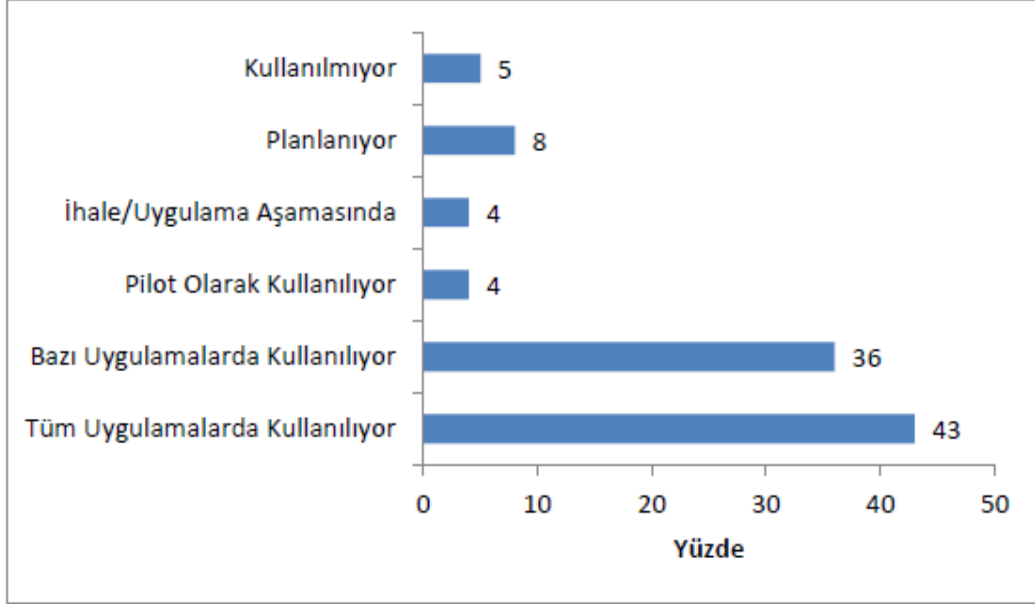
Şekil 5.7 Kurumlarda İnternet Hızı Dağılımı



Kaynak: (ÖZDAŞ, 2013)

Kurumların yüzde 43'ü tüm uygulamalarında, yüzde 36'sı ise bazı uygulamalarında sanallaştırma kullanmakta olup kurumların yalnızca yüzde 5'inde sanallaştırmaya ilişkin hiçbir çalışma yoktur (Şekil 5.8). Bulut bilişim altyapılarında sanallaştırma teknolojisinin kullanılması sebebiyle, sanallaştırma bulut bilişimin bir önceki adımı olarak görülebilir. Bu nedenle, kurumsal bilgi birikimi ve kullanım alışkanlıkları açısından bulut bilişime geçişte kayda değer bir zorluk yaşanmayacağı değerlendirilmektedir (ÖZDAŞ, 2013).

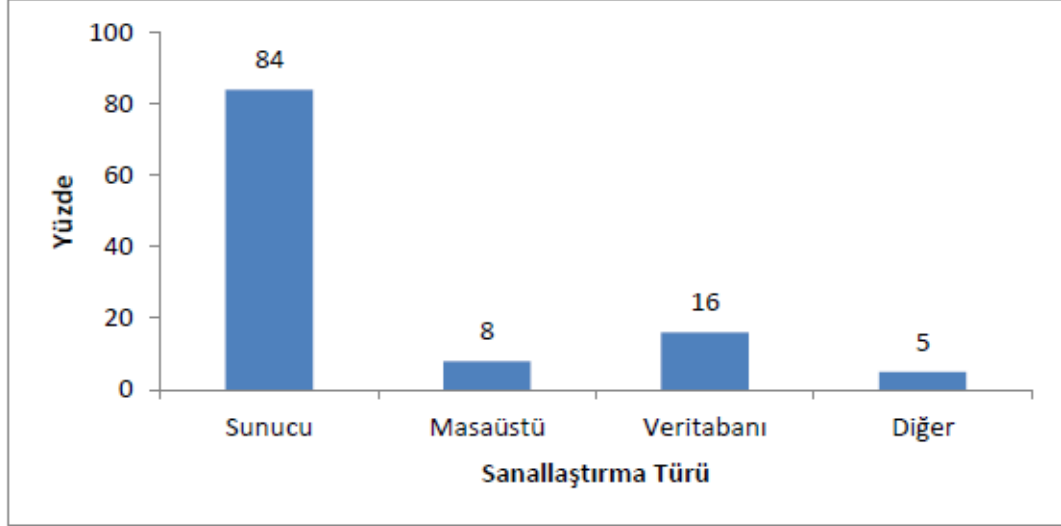
Şekil 5.8 Kurumlarda Sanallaştırma Kullanımına İlişkin Mevcut Durum



Kaynak: (ÖZDAŞ, 2013)

Kurumlarda kullanılan sanallaştırma türlerine bakıldığında, yüzde 84'lük bir oranla sunucu sanallaştırmasının kullanıldığı ve diğer sanallaştırma türlerinden etkin bir şekilde faydalanılmadığı görülmektedir (Şekil 5.9) (ÖZDAŞ, 2013).

Şekil 5.9 Kurumlarda Kullanılan Sanallaştırma Türleri



Kaynak: (ÖZDAŞ, 2013)

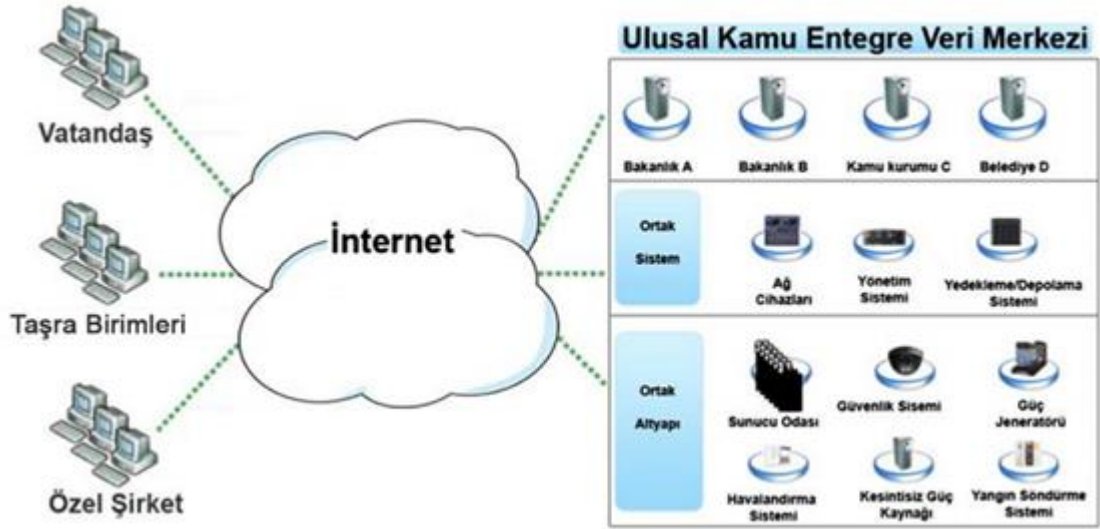
5.1.2. Hedeflenen Kamu Bilişim Yapısı

2006-2010 BTSE Planı kapsamında kamu hizmetlerinin elektronik ortamda sunumu noktasında önemli adımlar atılmış olup, e-Devlet hizmetleri arasında; MERNİS, AKS, TAKBİS, MERSİS, elektronik yazışma, kimlik kartı gibi ortak altyapı ve hizmetlerin yanı sıra, eğitim, sağlık, vergi, adalet, emniyet, sosyal güvenlik, gümrük ve bazı yerel yönetim hizmetleri gibi vatandaşlar ve girişimciler tarafından yaygın şekilde talep gören temel uygulamalar bulunmaktadır.

Ancak, kurum düzeyinde hayata geçirilen uygulamalara rağmen hem kamu hem de kullanıcılar açısından idari yükleri azaltarak maliyet ve zaman tasarrufu yaratmaya, vatandaş memnuniyeti ve yaşam kalitesini arttırmaya yönelik kurumlar arası entegrasyon ve ortak hizmet sunumu konusunda ilerleme sağlanamamıştır. Bu nedenle KEVM'ne ihtiyaç duyulmaktadır.

Türkiye'de kamu kurumlarına ilişkin veri merkezleri tek bir çatı altında toplanarak, KEVM'nin kurulması hedeflenmektedir. Hedeflenen kamu bilişim yapısı Şekil 5.20'de gösterilmektedir.

Şekil 5.10 Hedeflenen Kamu Bilişim Yapısı



Kaynak: (UDHB,2013)

5.2. Ortak Veri Merkezi Stratejisi

Kamu bilişim merkezlerinin kurumsal hedef ve stratejiler doğrultusunda 2023 Vizyonuna uygun şekilde hızla ilerlemesi için doğru yönetim modeli ve insan kaynağı kapasitesi oluşturmasının yanında oluşturulan kapasitenin etkin kullanımı için doğru teknolojik tercihlere yönelmesi gerekmektedir. Bu nedenle hızla gelişen bilişim teknolojilerinin öne çıkardığı unsurları doğru değerlendirmek ve ülke yapısına uygun çözümler üretmek gerekmektedir (TBD, 2013, s.65).

Bu amaca uygun olarak; kamu bilişim merkezlerinin bulut bilişimden faydalanmaları ve insan kaynaklarını daha etkin kullanabilmeleri için oluşturulacak bir devlet politikası çerçevesinde kamu kurumları tarafından organize edilecek ulusal veri merkezleri ivedilikle kurulmalıdır. Bu merkezlerin sorunsuz hizmet vermesini sağlamak üzere bulut bilişimin hukuki alt yapısı oluşturularak; verilerin korunması, gizlilik, fikri mülkiyet, mesleki sorumluluk, dış kaynak kullanımı, bilgi güvenliği gibi mevzuat gözden geçirilerek gerekli değişiklikler yapılmalıdır (TBD, 2013, s.65).

Kurulacak ulusal veri merkezlerinin yedekli olarak tasarlanacağı da değerlendirildiğinde her kamu kurumu tarafından kendi imkanları ile oluşturulan ve güncelliği ve ihtiyaçları karşılamak üzere her yıl ciddi yatırımlar, bakım, lisans, bilgi güvenliği, personel ve fiziki güvenlik için tüketilen kaynaklarda tasarruf sağlanacaktır. Ayrıca kurulan yapı ile hem altyapı daha yetkin personel eliyle yönetilecek hem de sürdürülebilirlik ve hizmet sürekliliği daha yüksek seviyede sağlanmış olacaktır (TBD, 2013, s.65).

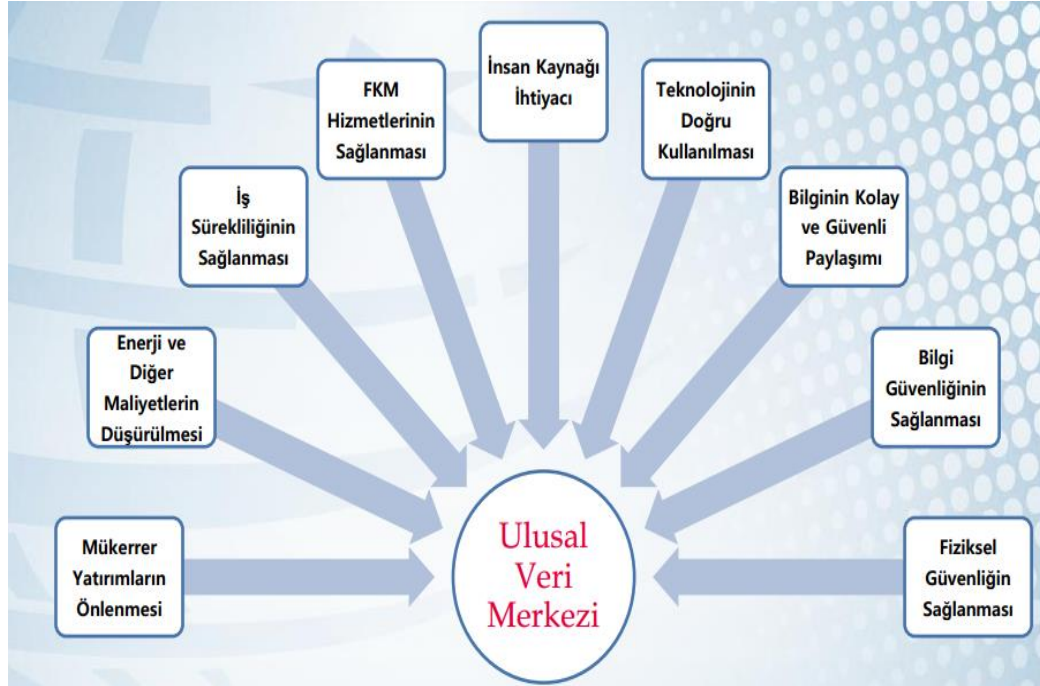
Bilim ve Teknoloji Yüksek Kurulu (BTYK) 25. Toplantısında gündeme gelen ve tüm kamu kurum ve kuruluşlarının verilerinin tek bir merkezde toplanmasını hedefleyen Kamu Entegre Veri Merkezi projesinin ihalesinin 2013 yılı sonuna kadar yapılması öngörülmektedir. Kamu ortak veri merkezi projesiyle tüm kamu kurum ve kuruluşlarının verilerinin bir merkeze aktarılması, yedeklenmesi ve olası felaket durumlarına karşı önlem alınması hedeflenmektedir. Karar alıcıların bu adımı atmasındaki önemli etkenlerden birisi de mükerrer yatırımların önüne geçilmesi ve tasarruf sağlanmasıdır.

5.3. Ortak Veri Merkezleri'nin Avantajları, Dezavantajları ve Riskleri

5.3.1. Ortak Veri Merkezleri'nin Avantajları

Kamu Entegre Veri Merkezi'nin avantajları şekilde olduğu gibidir.

Şekil 5.11 Kamu Entegre Veri Merkezi'nin Avantajları



Kaynak: (UDHB, 2013, s.14)

Kamu ortak veri merkezlerinin büyük yapılar ve organizasyonlarda sağlayacağı faydalara bakarsak, mükerrer yatırımların önüne geçilmesi, standartların belirlenmesi, yedeklilik, felaket kurtarma, bilgi güvenliği, iş sürekliliği ve birlikte çalışabilirlik konularının ön plana çıkacağını söylenebilir (Sezgin ve Akdemir, 2014, s.17)

Teknolojideki gelişmeler; farklı kurumlarda ve/veya kurumlara bağlı birimlerde ayrı ayrı bulunan ve işletilen sunucuların, ana bilgisayarların, ağların, portalların, haberleşme hizmetlerinin, bilgi teknolojileri destek personelinin, kısaca tüm bilgi teknolojileri altyapı ve harcamalarının, birleştirilmesine olanak sağlamaktadır. Bu sayede sistemler daha verimli kullanılmakta, personel, yazılım, donanım, altyapı, işletme giderleri azalmakta ve birim maliyetler düşmektedir (Sezgin ve Akdemir, 2014, s.18).

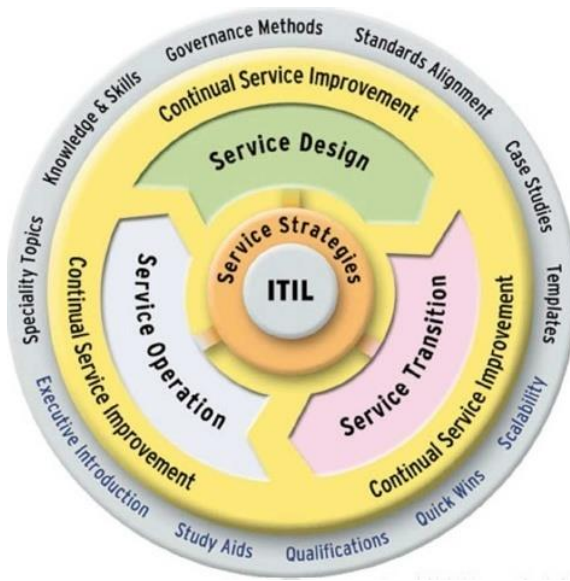
Birleştirme (consolidation) stratejisinden sağlanabilecek kazançlar şunlardır:

- Maliyetlerde azalma (personel, donanım, lisans, yer)

- BT varlıklarının daha iyi değerlendirilmesi
- Daha düşük depolama gereksinimi
- Daha düşük donanım ve yazılım fiyatları
- Daha iyi 7/24 hizmet olanakları (Sezgin ve Akdemir, 2014, s.19).

Kamu Veri Merkezi ile daha fazla uyumluluk, yasal denetimler, SOX (Sarbanes Oxley) ve ITIL gibi denetim mekanizmalarına uyumlu raporları her an üretebilme imkanı bulunabilmektedir (Sezgin ve Akdemir, 2014, s.21).

Şekil 5.12 ITIL Hizmet Stratejileri



Kaynak: (Sezgin ve Akdemir, 2014, s.21)

Kamu Veri Merkezi;

- Felaket sonrasında her bir yazılımın konfigürasyonundan, veri merkezinin genel yapısına kadar tüm altyapının güncel modelinin her an erişilebilir olması, bu sayede ihtiyaç anında veri merkezi hızlıca yeniden yapılandırılabilen,

- En iyi uygulama örnekleri sayesinde ağ, sunucu ve uygulamaların kullanılabilirlik oranının yükselmesi ve karmaşık ortamın çok daha kolay yönetilebilmesi sağlanmakta,
- Ortak kaynak kullanımı ve gereksinimlere göre kaynak ataması ile verimlilik sağlanmakta,
- Uzaktan yönetim sayesinde sisteme erişebilme, sistemi izleme ve sistemi yönetebilme,
- Uzman personel ile hizmet kalitesi ve sürekliliği sağlanmakta,
- Hizmetin istenildiği zaman kullanılabilmesi,
- İştaki artma ve azalmalara anında cevap verebilme,
- Ortak kullanım enerji verimliliğini artırmakta,
- Daha düşük karbon salınımı ile küresel ısınmanın önlenmesine katkı sağlamaktadır (Sezgin ve Akdemir, 2014, s.22-27).

5.3.2. Ortak Veri Merkezileri'nin Dezavantajları

Kamu ortak veri merkezi büyük bir organizasyon ve orkestrasyon ihtiyacını da beraberinde getirmektedir (Yazıcı, 2013).

Kamu Ortak Veri Merkezi'nin dezavantajları aşağıdaki gibidir:

- Ortak kullanılan kaynaklar ve veriler,
- Veri güvenliği ve gizliliği,
- Hizmet sağlayıcılar ile paylaşılan bilgiler,
- Dinamik kaynak yönetimi sırasında işletim sistemi tarafından silinen veriler,
- Alınmayan Önlemler;
 - Şifreli veri saklama,
 - Sanal yerel ağlar kullanımı,
- Ağ içi güvenlik duvarı kullanımınıdır (Sezgin ve Akdemir, 2014, s.28).

5.3.3. Ortak Veri Merkezileri'nin Riskleri

Ortak Veri Merkezleri'nin riskleri;

- Tüm kamu verisinin tek bir merkezde toplanıyor olması risklerin de tek merkeze odaklanmasına neden olacaktır.
- Bilgi güvenliği ve siber riskler konusunda daha yüksek standartların hedeflenmesi gerekecektir.
- Her kurumun güvenlik standartlarının yeniden gözden geçirilmesi ihtiyacını gözden kaçırmamak gerekmektedir. Kurumlardan gelecek verilerin ve veri merkezine bağlanan uç kullanıcıların aynı standartlarda ve güvenlik kriterlerinde sisteme erişiyor olması bir zorunluluk olacaktır (Sezgin ve Akdemir, 2014, s.30).

5.3.4. Ortak Veri Merkezi Planlaması

Veri merkezinin planlanmasında önemli hususlar aşağıdaki gibidir:

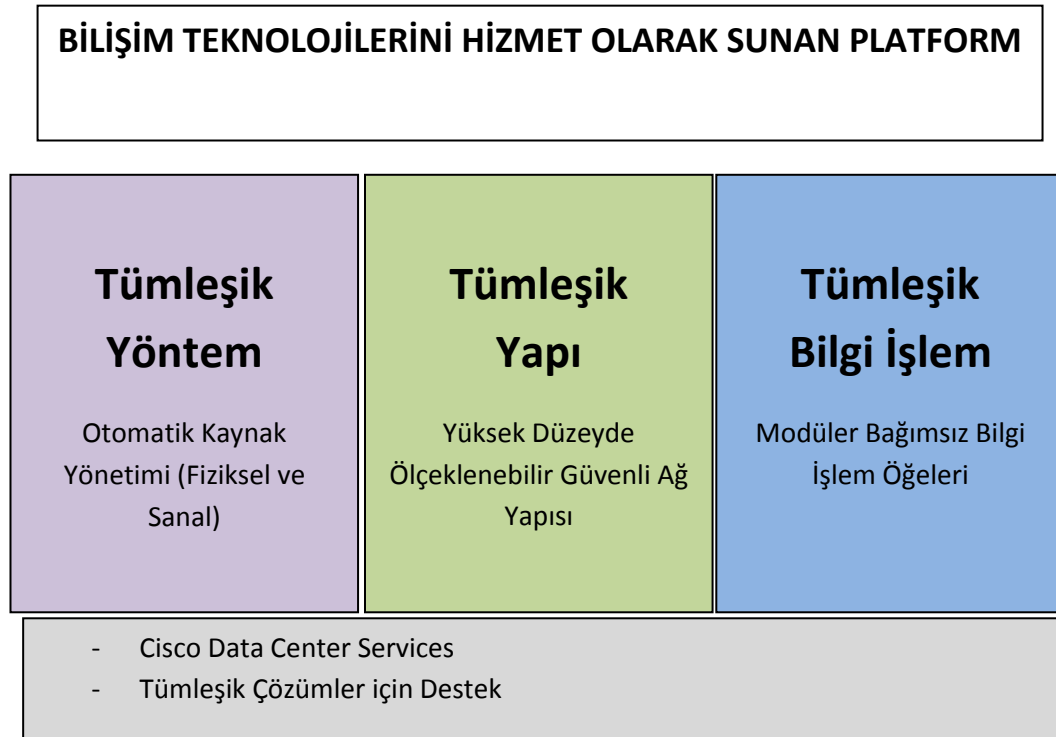
- Yer tespiti (Deprem, Sel, Doğal Afet Riskleri),
- Ulaşım kolaylığı,
- İnsan kaynağı,
- Enerji (Yenilenebilir enerji ve yeşil bilişim),
- İletişim alt yapısı,
- Yazılım lisanslarının tedariki,
- Donanım tedariki,
- Uygulamaların analizi,
- Veri merkezi standartlarıdır (UDHB, 2013, s.17).

6. KAMU ENTEGRE VERİ MERKEZİ'NE GEÇİŞ SÜRECİ

6.1. Veri Merkezi Mimarisi

Günümüz veri merkezi mimarisi yüksek düzeyde iş gücünü, cihaz yaygınlaşmasını, veri temelli iş modellerini desteklemeli ve bulut uygulamalarıyla servislerin sorunsuzca birlikte çalışmasını sağlayabilmelidir. Farklı gereksinimleri karşılayabilmek için bilgi işleme, depolama, ağ ve yönetimini sağlama, BT'ni fiziksel ve sanal ortamlarda hizmet olarak otomatikleştirmek üzere tasarlanmış bir platformla birleştiren tümleşik veri merkezi mimarisi artan bütçe verimliliği, daha çevik bir kurumsal yanıtlama yeteneği ve basitleştirilmiş BT işlemleri sağlayan mimari ideal mimari yapısıdır (Cisco).

Şekil 6.1 Bilişim Teknolojilerini Hizmet Olarak Sunan Platform



Kaynak: (Cisco)

6.2. Veri Merkezi Fiziksel Ağ Yapısı

Günümüzün veri merkezlerinde iletişim en çok IP protokolünü kullanan ağlara dayanmaktadır. Veri merkezleri sunucular ve dış dünya arasındaki trafiği taşıyan bir dizi yönlendiriciler ve anahtarları içerir. İnternet bağlantısının fazla olması çoğunlukla iki veya daha fazla servis sağlayıcıları tarafından sağlanmaktadır.

Veri merkezinde sunucuların bazıları temel internet ve intranet hizmetleri çalıştırmak için kullanılır. Ağ güvenlik elemanları genellikle güvenlik duvarları, VPN ağ geçitleri, saldırı tespit sistemleri (IPS)'ne konuşlandırılır. Bunların geneli ağ sistemlerini ve uygulamaların bazılarını da izlemektedir. Veri merkezi içindeki iletişimde bir arıza durumuna karşın ilave kapalı alanları izleme sistemleri de olağandır. Veri merkezi binasında bulunan temel altyapı olanaklarının üzerinde ağ altyapısı hizmetleri yer almaktadır. Bu ağ altyapı hizmetleri; ulusal ve uluslararası ağa yedekli bağlantı, ağ güvenliği, LAN bağlantısı (10/100/1000 Mbps), kullanıcıların talebine göre ölçeklenebilir bant genişliği ve kablolamadır (Wikipedia, 2014a).

6.3. Veri Merkezi Güvenliği

Veri Merkezi güvenliği Fiziksel ve Yazılımsal Güvenlik olmak üzere iki başlıkta incelenmiştir.

6.3.1. Fiziksel Güvenlik

Fiziksel güvenlik büyük önem arz etmektedir. Veri merkezinde seçilmiş ehil personeller harici girişler bazı bölümlerde kısıtlanmalıdır. Bu kısıtlamalar yazılım ile desteklenmelidir. Bu yazılımın bulunduğu Diskin özelliği ISE (Anında Güvenli Silme - Kriptografi) ile donatılmalıdır.

6.3.2. Yazılımsal Güvenlik

Yazılımsal güvenlikte en önemli unsur HDD'lerdir. Günümüzde ISE özelliği ile diskler 4 saniyeden kısa sürede kriptografik olarak silinebilir. Dolayısıyla Veri Merkezlerinde bulunacak Disklerin (HDD ve SSD) ISE özelliği ile donatılmış olması oldukça önemlidir.

6.4. Veri Merkezi Loglama

Veri merkezlerinin, 04/05/2007 tarihli ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele edilmesi Hakkında Kanun" gereği logların tutulması gerekmektedir.

5651 sayılı kanun:

- Yer Sağlayıcılar: Sisteminde En Az Bir Web Sitesi Olan Kurumlar
- İnternet Toplu Kullanım Sağlayıcılar: İnternet Erişimi Sağlayan Kurumlar
- Ticari Amaçla İnternet Toplu Kullanım Sağlayıcılar, Erişim Sağlayıcılar
- Telekomünikasyon Hizmeti Veren Kurumlar
- İçerik Sağlayıcılar: İnternet Ortamında İçerik Üreten Kurumları kapsamaktadır.

Telekomünikasyon Hizmeti Veren Kurumlar başlığı altında olacak olan veri merkezleri de kendi sunucularında bu logların tutulmasını sağlamalıdır.

6.5. Veri Merkezi Enerji Kullanımı

Son zamanlarda, yapılan çalışmalar enerji kullanımının BT operasyonlarının önemli bir maliyet kalemi olduğunu ve bazı durumlarda BT donanımının kendisinin maliyetlerini aştığını göstermiştir. Bu maliyet baskısı, veri merkezlerinin enerji kullanımlarında çok daha etkin olabileceklerinin farkına varılmasıyla birleştirildiğinde, pek çok veri merkezi operatörünün enerji yönetimini bir öncelik haline getirmelerine neden olmuştur.

Veri Merkezinde yedekliliği ve sürekliliği en önemli olan sistemler enerji sistemleridir. Sistem odalarında kesintisiz hizmet verebilmenin ilk adımı güç kaynaklarını yedeklemekle baslar. Her ne kadar donanım maliyetlerini ikiye katlıyor olsa da en az iki farklı kaynaktan enerji ihtiyacının karşılanması zorunluluk halini almıştır (Gökmen ve Küçüksille, s.2-3).

6.5.1. Sera Gazı Etkisi

2007 yılında iletişim ve Telekomünikasyon Teknolojileri sektörü tüm dünyada %2' lik bir karbon salınımından, veri merkezleri de sektör içerisinde %14'lük bir salınımdan sorumludurlar (Wikipedia, 2014a).

6.5.2. Enerji Verimliliği

Enerji verimliliğini ölçmede en genel kıstas güç kullanım verimliliği (PUE)'dir. Bu basit oran aslında veri merkezine giren toplam gücün BT ekipman tarafından tüketilen güce bölümüdür.

Destek ekipmanları tarafından kullanılan güç çoğunlukla genel gider olarak adlandırılır, soğutma sistemleri, elektrik tesisat ve aydınlatma gibi tesis altyapılarının sebep olduğu tüketimdir.

Amerika Birleşik Devletlerindeki ortalama bir veri merkezi 2.0 değerinde bir PUE değerine sahiptir, bu değer tesiste BT ekipmanlara harcanılan enerji kadar destek ekipmanlarına da aynı miktar harcandığını gösterir. PUE değeri ne kadar düşükse işletme için o kadar iyi olmaktadır (Wikipedia, 2014a).

6.6. Soğutma Sistemleri

Veri merkezinde bulunan cihazların büyük bir bölümü çabuk ve yüksek ısı üretmektedir. Elektronik cihazların tamamı fazla ısıda performans kaybı ve daha sonra arıza yaşamaktadır. Dolayısı ile soğutma sistemleri, devamlılığının sağlanması konusunda en önemli ünedir.

Soğutma sistemleri enerji sarfiyatının büyük bölümünü üstlenir. Bu yüzden minimum maliyetle maksimum fayda alınmalıdır. Günümüzde en çok kullanılan alan soğutmalı çözümlerdir. ANSI/TIA/EIA-942 standardı, soğutmada en öncelikli yapılması gereken çalışmayı, kabinlerin yerleşimlerinin düzenlenmesi olarak ortaya koymaktadır. Bu çözümde dikkat edilmesi gereken sıcak ve soğuk hava koridorları oluşturmaktır. Kabin ve Klima yerleşimlerinde cihazların soğuk havayı çektiği ve sıcak havayı boşalttığı alanlar bir koridor gibi oluşturulmalıdır. Sıcak hava özkütleden dolayı yükseleceği için klimaların bu havayı çekebilecek konumda olmalıdır. Soğuk hava ise yükseltilmiş zeminin altından kabin özlerindeki menfezlerden cihazlara ulaşmalıdır. Günümüzde en yaygın soğutma yöntemi soğuk hava (Klima) ile yapılmaktadır. Su ile soğutma (Green Data Center) yeni bir çözüm olarak karşımıza çıkmaktadır. Devamlılığın öneminden dolayı klimaların yedekliliği de son derece önemlidir. Klimalar sık arızalanan bir yapıya sahiptir bu yüzden yedeklilik son derece önemlidir (Gökmen ve Küçüksille, s.3).

7. PROJELENDİRME

Kamu Entegre Veri Merkezi'nin kurulması Analiz ve Hazırlık süreçleri ele alınarak değerlendirilmiştir.

7.1. Analiz

Kamu Entegre Veri Merkezi kurulumu için İhtiyaç analizi, Swot analiz, Alt Yapı analizi, Risk Analizi ve Maliyet Analizi başlıklarında incelemeler yapılmıştır.

7.1.1. İhtiyaç Analizi

Veri Merkezi kurulumu için en önemli analiz ihtiyaç analizidir. Veri Merkezi için gerekli olan donanımsal, yazılımsal ve insan ihtiyacının belirlenmesi doğru bir yolda ilerlemek için oldukça önemlidir. Bu aşamada veri merkezi için gerekli olan ihtiyaçların analizinin yapılabilmesi için çeşitli örneklerden faydalanılmıştır. Bu örnekler içerisinde ilk veri merkezini kuran G. Kore, Amerika Birleşik Devletleri, İngiltere ve Japonya örnekleri ile teknolojik gelişmeler göz önünde bulundurulmuştur.

Veri Merkezi için öncelikle donanımsal ihtiyaçların belirlenmesi ve bu donanıma uygun yazılımların belirlenmesi gerekmektedir.

7.1.1.1. Fiziksel Mekan İhtiyacı

KEVM'nin kurulmasında fiziksel mekanın seçimi oldukça önemlidir. Fiziksel mekanın seçiminde dikkat edilmesi gereken hususlar:

- Ankara ilinden yeterli uzaklıkta olması,
- Deprem riskinin düşük olması,
- Sıcaklık ve nem oranlarının düşük olması,
- Uydu iletişimde açık iletişim hattının bulunması,
- Uzman personelinin çalışmasının uygunluğu,

- Çevresel etkenlerden yeterli mesafede uzak olması,
- Genişleyebilmeye uygun olması söylenebilir.

7.1.1.2. Donanımsal İhtiyaçlar

Veri merkezi kurulumu için en önemli donanımsal ihtiyaçların başında sunucular gelmektedir. Tüm donanım özellikleri Tier IV Standartları gereğince hazırlanmalıdır. Tier IV bütün Tier III kriterlerini karşılamakla birlikte, ek olarak 96 saatlik kesintiye dayanabilmektedir. 7/24 çalışan bir personel ekibi mevcuttur. Yer seçiminde çok sıkı davranılmalı, yüksek güvenlik önlemleri alınmalıdır.

Tier IV Standartlarının donanım seçiminde dikkate alınmasıyla; Jeneratör, UPS ve klima'da her bileşen yedekli olmaktadır. %99,995 kullanılabilirlik sağlamaktadır.

7.1.1.3. Yazılımsal İhtiyaçlar

Kullanılacak veri merkezi yazılımlarının en önemli iki özelliği olmalıdır. Birincisi güvenlik, ikincisi hız. Hız faktörü seçilen donanım özelliklerine göre değişmekle birlikte yazılım seçimi de hızı önemli ölçüde etkileyebilmektedir. Kullanılacak işletim sisteminin çalışma prensibi öncelikle 7/24 kesintisiz olmalıdır. Bu anlamda Windows ya da Linux işletim sistemleri arasında tercih yapılması gerekmektedir.

Ulusal güvenlik ve dışa bağımlığı ortadan kaldırmak açısından Türkiye'nin kendi işletim sistemini Linux çekirdeği üzerinden tasarlaması gerekmektedir. Daha önce TÜBİTAK tarafından geliştirilen Linux İşletim sistemi olan Pardus daha çok masaüstü uygulamaları için kullanılabilir durumdaydı, Pardus kurumsal ismiyle çıkarılan işletim sisteminde ise bazı hatalar mevcuttu. Bu bakımdan Türkiye'nin bu konuda daha kapsamlı bir çalışma yapması, bu çalışmayı TÜBİTAK kurumu ile birlikte Ulaştırma bakanlığının üstlenmesi veri merkezi için oldukça önemlidir.

Bir diğer yazılımsal unsur ise güvenlik duvarı yazılımı, her ne kadar güvenliği donanımsal olarak düşünsük de yazılımsal olarak da ek güvenlik önlemleri alınması

gerekmektedir. Bu anlamda yine Türkiye'nin kendisinin geliştirebileceği açık kaynak kodlu bir yazılım kullanabilir, örneğin PfSense Güvenlik duvarı gibi.

Uygulama yazılımları açısından düşünüldüğünde Tier standartları gereği personel yetki kısıtlanmalarının, giriş çıkışların takip edildiği bir uygulama yazılımının yine Türkiye'nin kendisinin geliştirmesi gerekmektedir. Bu yazılım tüm güvenlik önlemleri alınarak internetten de bazı bölümlere erişilebilecek web tabanlı bir uygulama yazılımı olabilir.

7.1.1.4. Kalifiye İnsan Gücü İhtiyacı

Veri Merkezi'nde her ne kadar standartlara uygun sistem kurulmuş olursa olsun personelin alanında uzman kişilerden oluşması oldukça önemlidir. Bilgisayar, Elektrik Elektronik, Endüstri Mühendislerinin yanı sıra konusunda uzman eğitmenlerin, rehberlik uzmanlarının 7/24 çalışan bir ekibin veri merkezi bünyesinde bulundurulması oldukça önemlidir.

7.1.2. SWOT Analizi

SWOT Analizi, bir projede ya da bir herhangi bir ticari girişimde kurumun, tekniğin, sürecin, durumun veya kişinin güçlü (Strengths) ve zayıf (Weaknesses) yönlerini belirlemekte, iç ve dış çevreden kaynaklanan fırsat (Opportunities) ve tehditleri (Threats) saptamak için kullanılan stratejik bir tekniktir. Bu teknik projenin ya da girişimin hedeflerini belirlemeyi ve amaca ulaşmak için olumlu ya da olumsuz olan iç ve dış faktörleri tanımlamayı gerektirir.

Swot Analiz yukarıda da belirtildiği gibi 4 aşamadan oluşmaktadır. Bu aşamalar aşağıdaki Tablo 7.1'de belirtilmiştir.

7.1.2.1. Tespit

4 aşamadan oluşan Swot Analizi, Kamu Entegre Veri Merkezi'nin kurulması için yapılmıştır. Buna göre oluşan tablo aşağıdaki gibidir.

Tablo 7.1 Kamu Entegre Veri Merkezi Swot Analizi

GÜÇLÜ YÖNLER	ZAYIF YÖNLER
<ol style="list-style-type: none"> 1. Devletin maddi desteği 2. Bu yönde bir ihtiyaç olduğunun biliniyor olması, 3. Ülke olarak TIER standartlarına uygun Veri Merkezi kurabilme kapasitesine sahip bilgi birikimine sahip olunması, 4. Ulusal bir işletim sistemi yazmış olmak, 5. Nitelikli insan kaynağının bulunması, 6. Kaynak verimliliğinin sağlanması, 7. Özel şirketlerin deneyimleri. 	<ol style="list-style-type: none"> 1. Bürokratik işlemlerin çokluğu, 2. Hızlı karar alamama, 3. Bu yönde yapılmış bir çalışmanın Türkiye'de bulunmaması, 4. Fiziki güvenliğin sağlanamaması, 5. Birlikte çalışabilme sorunları, 6. Yönetilebilirlik sorunları, 7. Altyapı yatırımları yetersizliği, 8. Teknik entegrasyonda yaşanabilecek sorunlar, 9. Sürdürülebilirliğin sağlanamaması, 10. İşletme maliyeti.
FIRSATLAR	TEHDİTLER
<ol style="list-style-type: none"> 1. Türkiye'nin istikrarlı büyüme hızı, 2. Genç nüfus oranının yüksek olması, 3. Türkiye'nin teknolojiye duyduğu ilginin büyüklüğü, 4. Çevresel olarak iklim koşullarının uygun olduğu ortamı seçebilme özgürlüğü. 	<ol style="list-style-type: none"> 1. Ekonomide gerileme, 2. Çevre ülkelerdeki siyasi, askeri ve etnik sorunların varlığı, 3. Siber saldırı ihtimali, 4. Kullanılacak cihazların yurt dışından temin edilmesiyle birlikte karşımıza çıkabilecek güvenlik sakıncaları.

7.1.2.2. Analiz

Güçlü Yönlerden Daha Fazla Yararlanmak için; Devletin veri merkezine ayırdığı bütçenin artırılması gerekmektedir. Türkiye'nin Ulusal bir veri merkezine duyduğu ihtiyacı belirginleştirmek için bu konuyla ilgili çalıştayların düzenlenmesi oldukça önemlidir. Türkiye'nin kendi işletim sistemini dünya standartlarında bir işletim sistemi haline getirmesi gerekmektedir. Genç nüfusun yoğun olmasından kaynaklanan nitelikli insan gücünün etkin kullanılması önem arz etmektedir. Kamu kurumlarına ayrılan kaynakların etkili bir şekilde kullanılması ile verimlilik sağlanacaktır. Türkiye'deki özel şirketlerin bu alandaki tecrübelerinden faydalanılması gerekmektedir.

Zayıf Yönlerin Giderilmesi için; Bürokratik işlemlerin çokluğundan dolayı işlerin yavaşlamasına karşın alınacak önemlerin başında yasal bir takım düzenlemeler yapılmalıdır. Bu hızlı karar almayı da sağlayacaktır. Türkiye'nin veri merkezi tecrübesinin olmamasından dolayı yurt dışındaki örneklere daha fazla önem verilmelidir. Fiziki güvenlik ile ilgili zayıf noktayı güçlendirmek için veri merkezinin kurulacağı lokalizasyonu çok iyi belirlemek gerekmektedir. Birlikte çalışabilirliği artırmak için yazılımsal teknoloji en üst düzeyde etkin bir şekilde kullanılmalıdır. Yönetilebilirlik ile ilgili sorunların azaltılması için yetkilendirmelerin hassasiyetle yapılması gerekmektedir. Teknik kısımda yaşanabilecek sorunların önceden tespit edilmesi için uygulamada sanallaştırmanın önemi göz önüne alınmalıdır. Sürdürülebilirliğin sağlanması için kurumlar arasında koordinasyonun sağlanması önemlidir. İşletme maliyetlerine ilişkin sorunların giderilmesi için sadece zorunlu harcamaların yapılması gerekmektedir.

Fırsatlardan daha fazla yararlanmak için; Türkiye'nin mevcut dönemdeki istikrarlı büyümesi göz önüne alınarak projeye hızlı bir şekilde başlanması ve bitirilmesi gerekmektedir. Veri Merkezinin teknolojik gelişmeleri genç ve nitelikli insan gücü ile yapılmalıdır. Türkiye'nin coğrafi konumundan dolayı veri merkezlerine uygun bölgenin kolaylıkla seçilebilir olması bir fırsattır.

Tehditleri Fırsata Dönüştürmek için; Ekonomide gerilemenin yaşanması ihtimaline karşın veri merkezine ait bütçenin oluşturulması gerekmektedir. Çevre ülkelerdeki olası bir takım sorunların Türkiye'ye sıçraması durumunda askeri önlemlerin üst düzeyde alınması gerekmektedir. Siber saldırı ihtimaline karşı Kriptolu Disklerin kullanılması oldukça önemlidir. Siber saldırılara karşı uzman personelin çalıştırılması gerekmektedir. Kullanılacak cihazların yurt dışından alınması sonucu yaşanacak donanımsal ve yazılımsal dışa bağımlılığı azaltmak için Türkiye'nin kendi donanımlarını ve yazılımlarını geliştirmesi gerekmektedir.

7.1.3. Alt Yapı Analizi

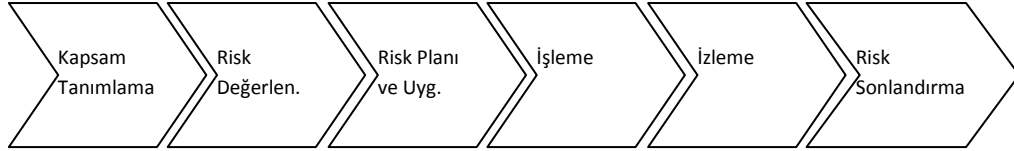
Veri Merkezi olacak binanın fiziksel özellikleri oldukça önemlidir. Mimari açıdan doğal soğutma özellikleri göz önünde bulundurulması oldukça önemlidir. Güneş ışığının doğrudan binaya çarpmasını engellemek için özel mimari çalışmanın yapılması gerekmektedir. Veri Merkezi'nin kayalık bir bölüme yapılması olası deprem risklerini en aza indirecektir.

7.1.4. Risk Analizi ve Yönetimi

Türk standartları Enstitüsü'nde, Risk yönetim süreci; Bir kuruluşun riski kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler bütününe bilgi sistemlerini etkileyebilecek olan güvenlik risklerinin, uygun bir maliyette tanımlanması, kontrol edilmesi ve en aza düşürülmesi veya ortadan kaldırılması süreci” olarak tanımlanmıştır (Şahinaslan, 2011, s.568).

Bilgi ve bilgi teknolojileri üzerinde yer alan risklerin yönetilmesinde gerçekleştirilen bir dizi faaliyetleri; risk tanımının yapılması, değerlendirmesi, planlama, işleme, izleme ve risk sonlandırma süreç adımları olarak tanımlanabilir, temel bir risk yönetim süreci Şekil 7.1'de gösterilmektedir.

Şekil 7.1 Risk Yönetimi



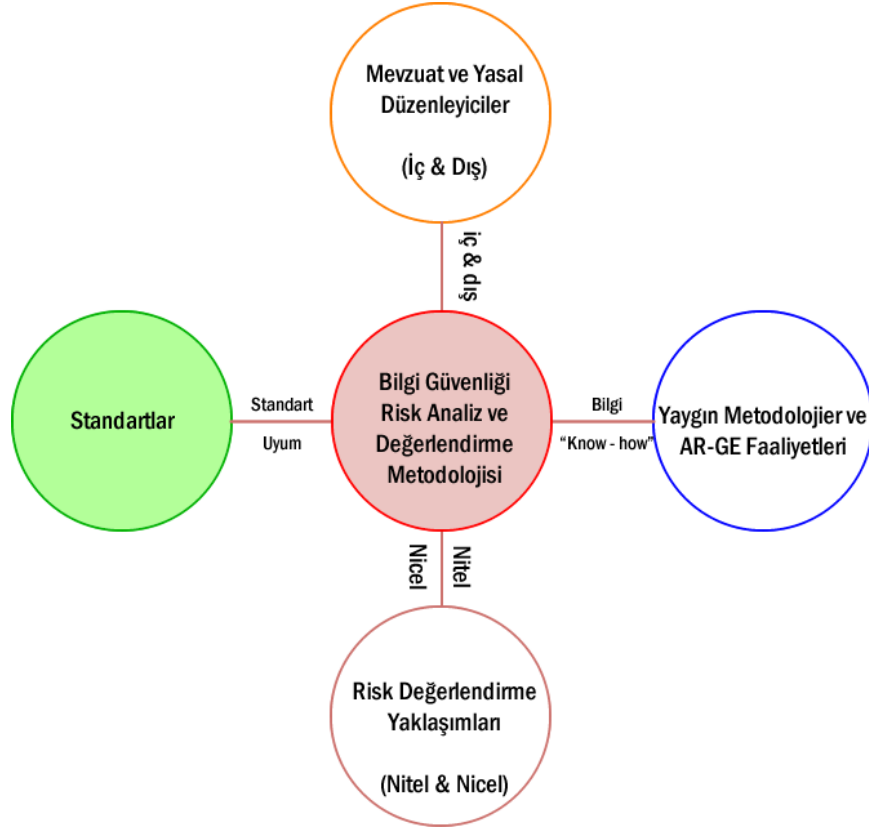
Kaynak: (Şahinaslan, 2011, s.568)

Sağlıklı bir risk yönetimi yapmak için kurum, risk yönetimine ait bu süreç aşamalarını işleterek riski doğuran tehditlere karşı kontrol ve önlemleri almak ve riskin mümkün olan kabul edilebilir seviyeye çekilmesi ya da tamamen yok edilmesi gerekmektedir.

Risk yönetim süreci işletmede; kurum beklentileri, yasal ve standart yaklaşımlara uyum gibi unsurları dikkate alan bir risk değerlendirme yönteminin seçimi, risk yönetiminin yapılacağı platform-uygulama seçimlerinin karar verilmesi gereken ana unsurların arasında yer almaktadır.

Genel bir risk yönetiminde özelde ise bilgi ve bilgi teknolojileri alanında yapılacak bir risk yönetimi için kurumsal bir firmanın karar vermesi gereken ilk unsur risk değerlendirme yöntemine karar verilmesidir. Bu yönde yapılacak bir arayış için çıkılan yolculuk da düşünülmesi gereken belli başlı alanlar Şekil 7.2’de gösterilmektedir (Şahinaslan ve Kandemir, 2010).

Şekil 7.2 Risk Değerlendirme Yöntem Bileşenleri



Kaynak: (Şahinaslan ve Kandemir, 2010)

Risk değerlendirme yönteminde yer alması gereken temel unsurlar aşağıda belirtilmiştir.

Standartlar (ISO/IEC 27005, ISO/IEC 31000, RISK IT, COBIT vb)

- İlgili kurum mevzuatlarına uyum gereklilikleri (İç ve dış),
- Risk değerlendirme yaklaşımı; Nitel-nicel karma model,
- Yaygın kullanılan metodolojiler ve bu alanda bilinen en iyi uygulama örneklerinin incelenmesi kurum için önemli avantaj doğurmaktadır (Şahinaslan, 2011, s.568).

Kurumsal bir kimliğe sahip olmak isteyen bir kurum, faaliyet kollarına ilişkin alanlarda, uluslararası standartların belirlemiş olduğu kurallara asgari seviyede uyumlu olması gerekmektedir. Kurumun standartlara uyumluluğu önemli bir gösterge olarak kabul edilmektedir. Aynı zamanda bu uyumluluk artık gittikçe globalleşen bu çağda daha da önemli kılmaktadır (Şahinaslan, 2011, s.569).

Uluslararası standartlar incelendiğinde ISO/ IEC 9001, ISO/IEC 27001, ISO/IEC 27005, RISK IT, ISO/IEC 31000, AS/NZS 4360:2004, FISMA, NIST SP 800–53, PCI, PMI, CMMI, SPICE, ITIL, COBIT gibi standartlar mevcuttur. Bunların bir kısmı doğrudan bir risk yönetim standardı iken ISO/IEC 9001, PCI, CMMI, SPICE, PMI, ITIL, COBIT, HIPAA gibi bir takım standartlar ise kendisi bir risk yönetim standardı olmamakla birlikte risk yönetimi ile de ilintilidir. Bilgi ve Bilgi Teknolojilerine yönelik risk yönetim standartları;

- a. ISO/IEC 27005: Bilgi Güvenliği Risk Yönetim Standardı
- b. RISK IT: Bilgi teknolojileri risklerinin etkin yönetimine yönelik bir dizi ilkelerden oluşan ana çerçeve niteliğindedir.
- c. NIST SP 800–30: Bilgi Teknoloji için Risk Yönetim Rehberi (Şahinaslan, 2011, s.569).

Bilgi ve bilgi teknolojilerine ait risk yönetimi süreci içerisinde risklerin analiz ve değerlendirme aşamasında nitel ya da nicel risk analiz yöntemlerinden biri ya da bu iki yöntemi birlikte kullanabilen karma yöntemden biri seçilerek gerçekleştirilir (Şahinaslan, 2011, s.569).

‘Yüksek, orta, düşük, imkansız’ gibi sözel ifadelerin kullanılarak gerçekleştirilmesine nitel (sözel) analiz, ‘3, 2, 1, 0’ gibi sayısal ifadelerin kullanılmasıyla gerçekleştirilen analiz yöntemine ise nicel (sayısal) analiz yöntemi denir. Bir tehdit’in vuku bulma ihtimaline karar vermede kullanılan karar tablosu örneği Tablo 7.2’de verilmiştir.

Tablo 7.2 Tehdit Etki-Olasılık Karar Çizelgesi

Nicel	Nitel	Olasılık	Açıklama
0	İmkansız	% 0	İmkansız veya 10 yıl üzeri oluşabilir
1	Düşük	% 1-34	1 - 10 yılda bir kez oluşabilir
2	Orta	% 35 - 74	1 - 5 yıl içinde en az bir kez oluşabilir
3	Yüksek	% 75 - 100	0 - 12 ay içinde bir veya üzeri oluşabilir

Kaynak: (Şahinaslan, 2011, s.569)

7.1.5. Maliyet Analizi

Bir kurum internet üzerinden bilgi paylaşımına karar verdiğinde yapması gereken işler ve tahmini maliyet kalemleri Tablo 7.3'de sıralanmıştır. Kurumun, yapılacak ilk yatırım maliyetini ve bir sonraki yılda yapacağı güncellemeleri göz önünde bulundurması gerekmektedir. Orta büyüklükte bir kamu kuruluşun ülke geneline yayılmış bölge ve il müdürlükleri ile internet üzerinden veri alış verişi yapmak ve vatandaşlara hizmet götürmek istediğinde, erişim, donanım, yazılım ve kablolama maliyetlerini göz önünde bulundurmak zorundadır. Aşağıdaki Tablo 7.3'de ülkemizde bir bakanlığa bağlı genel müdürlüğün taşra teşkilatı ile kendisi arasında kurulacak iletişim, veri saklama ve işleme merkezinin kurulma maliyetini göstermektedir. Bu maliyetlere binanın yapım maliyeti eklenmemiştir (Tanrıku, 2002, s.3).

Tablo 7.3 Tahmini Maliyet Kalemleri

BT Giderleri	Miktarı (\$)
Web, Database, Lan sunucu ve ilgili donanımları	200.000 \$
İnternet bağlantıları ve RAS	175.000 \$
Desktop PC, LapTop PC, Lan kartları (Lan yönetmek için kullanılan cihazlar)	20.000 \$
Destek elemanları (Hub, switch.) ve kablolama	20.000 \$
Sunucu OS, Website tools ve Database yazılım lisansları	60.000 \$
LAN ve Desktop Yazılım Lisansları	30.000 \$
Müşteri Destek Yazılımları, Güvenlik sistemleri yazılımları	50.000 \$
İçerik, script ve uygulama geliştirme yazılımlarının yapılması	350.000 \$
Taşıma hizmetleri (Devre Kirası)	50.000 \$
Sistemlerin fiziksel kurulumu ve çalışır hale getirilmesi	30.000 \$
Planlama ve Danışma ücreti	150.000\$
Personel Gideri	225.000\$
Personel Eğitimi	40.000\$
Elektrojen Grubu + UPS	10.000\$
Klima	20.000\$
Toplam	1.430.000\$
Ek Maliyetler	Miktarı (\$)
Sistem Donanım Güncellenmesi	60.000 \$
Sistem Yazılım Güncellenmesi	50.000 \$
Site Yazılımı Güncellenmesi (Yönetim Araçları Dahil)	80.000 \$
Danışmanlık	100.000 \$
Değişen Uygulama Yazılımlarının Güncellenmesi	175.000 \$
Eğitim	40.000 \$
Ek sarf Malzemeler	100.000 \$
Toplam (Güncelleme Maliyeti)	605.000 \$

Kaynak: (Tanrıku, 2002, s.3-4)

Toplam İlk yatırım maliyeti analizi: 1.430.000 \$

Bir kurumun, internet üzerinden kendi ofisleri ve vatandaş ile veri alış verişine girmesi, iş yükünü internete aktarması, hizmetlerini internet üzerinden yapmasının maliyeti yaklaşık 2.000.000 \$'dır. Bir yıl sonra bu yatırım %50 değer kaybettiğinden, her yıl yeniden güncellenmesi için yatırım yapılması gerekmektedir. Bu nedenle Kamu Entegre Veri Merkezi kurularak kaynakların verimliliği sağlanmalıdır.

7.2. Hazırlık

7.2.1. Fiziksel Alt Yapı Hazırlığı

Veri merkezindeki donanımların kabinetlere sabitlenmesi, kabinetlerin duvarlara sabitlenmesi gerekmektedir. Kablolamaların bina yapımından önce hesaplanıp gerekli düzenlemelerin yapılması gerekmektedir. Binada Server Odaları özel olarak tasarlanıp, kabinetlerin özenle yerleştirilmesi gerekmektedir. Bu odaların en az 4 IP kamera ile izlenebilir durumda olması gerekmektedir. Bu odalara giriş çıkışlar özel yazılımlar ile yetki bazlı kısıtlanmalıdır. Bu çalışma için veri merkezi çalışanlarına yönelik parmak okuyucu bulundurulmalı, özel yetkilendirme ile hem parmak izine göre, hem de göz okumaya dayalı yetkiler verilmelidir.

7.2.2. Donanım ve Yazılım Tedariki

Donanım ve Yazılım tedariki noktasında ANSI TIA 942 'ye göre belirlenmiş yazılımların ve donanımların tercih edilmesi son derece önemlidir. Yazılım ile ilgili Veri Merkezi'nin kendi yazılımlarının kullanılma oranı ne kadar yüksek olursa o derece güvenlik sağlanmış olacaktır.

7.3. Uygulama

KEVM içinde veri paylaşımı; geliştirilecek uygulama yazılımları ile tek noktadan erişim sağlanarak, KEVM içindeki kurumların sistemleri arasında bilgi paylaşımı

yapılarak, tek noktadan, çok noktaya erişim yapılarak, geri besleme ile tek noktaya hizmet sunumu sağlanacaktır.

BTYK'nın 2003/105 nolu kararının KEVM kurulmasıyla uygulama bulacaktır.

SONUÇ ve ÖNERİLER

Bilgi iletişim altyapısının kamu kurum ve kuruluşları, özel sektör ve vatandaşlar tarafından kullanımının artmasına bağlı olarak kamu kurumları tarafından verilen hizmetlerin elektronik ortama aktarılması ve bu iş ve işlemlere ilişkin verilerin elektronik ortamda saklanması zorunluluk haline gelmiştir. Bu nedenle her kurum kendi bünyesinde bu verilerin tutulduğu bir veri sistemi kurmakta ve bu sistem üzerinden verilere erişerek hizmet sağlamaktadır.

Her kamu kurumu kendi verilerini saklaması, fiziki ve siber güvenliğini sağlaması, nitelikli insan kaynağı oluşturması, kendi ihtiyaçlarına yönelik verilerinin kullanımını sağlamak için yangın koruma, soğutma, enerji, iletişim vb. altyapıların oluşturulması, donanım ve yazılım tedariki ile bu yazılım ve donanım eğitimlerinin personellere verilmesi gibi pek çok kalemde harcama yapmaktadır. Aynı zamanda mevcut sistemin idamesinin sağlanmasıyla iş geliştirme süreçleri gerçekleştirilememekte ve bilgi işlem personelleri proje geliştirememektedir.

Yatırım ve operasyonel maliyetlerin düşürülmesi, hizmet kalitesinin artırılması, idari ihtiyaçlar, tasarruf imkanı ve siber güvenlik gereksinimleri doğrultusunda halen her kurumda müstakil olarak işletilmekte olan kamu kurumlarının veri merkezleri tek bir merkezde toplanacak şekilde birleştirilerek Kamu Entegre Veri Merkezi'nin kurulması önem arz etmektedir.

Güvenliği yeterince sağlanmış, merkezi olarak kurulacak sistemsel bir yapıyla birlikte kamusal alanda bilgi teknolojileri yatırımları daha efektif ve kontrol edilebilir olacaktır.

Kamu Entegre Veri Merkezi'nin kurulması çalışmalarında, bu konuda başarılı olan ülkelerin oldukça uzun süreçler neticesinde, önemli analizler ve aşamalı geçişler ile tamamladığı çalışmaları incelenerek, ülkemizde en verimli olabilecek şekilde hayata geçirilmesinde; kamu kurumları, özel sektör, üniversiteler ve sivil toplum kuruluşlarının etkin katılımıyla çözülmesi önem arz etmektedir. Bu konuda, mevcut

kamu veri merkezi örneklerinin, dünyada ve Türkiye'deki uygulamalarının analizi bu konuda uzman kişilerin danışmanlığında yapılmalıdır.

Kamu Entegre Veri Merkezi'ne güvenlik boyutunda öncelikli olarak hangi kurumların kapsama dahil edilmesi gerektiğine karar verilmelidir. Entegre edilecek kurumların seçiminde dikkat edilmesi gereken hususlar; dışarıdan hosting hizmeti alan kurumlar, veri merkezleri başka bir kurum üzerinde olan kurumlar ve merkez teşkilatındaki kurumlar öncelikli olarak belirlenmelidir.

Güvenliği hassas olan kurumlarla, hassasiyeti az olan kurumlara karşı farklı tedbirler uygulanmalı, güvenlik ve gizlilik farklı açıdan değerlendirilmelidir. Hassas sistemlerin verilerinin tutulmasında dışarıdan hizmet alımı yapılmamalı, kamu bulutu veri depolama altyapısında tutulmalı ve dışarıya açılmamalıdır. Kamu Entegre Veri Merkezi'nde veri gizliliği için bulut bilişimde verilerin şifreli saklanması, sanal yerel ağların kullanılması ve ağ için güvenlik duvarı vb. yöntemler ile sağlanmalıdır. Güvenlik hassasiyeti az olan ve verimlilik açısından dışarıdan bulut hizmeti ile yönetilecek veriler ise güvenlik ve gizlilik açısından farklı açılardan değerlendirilmelidir.

Kamu Entegre Veri Merkezi ile standartlaştırılmış, iş yüküne göre ayrılabilen, birleşik ve sanal sunucuların kullanıldığı bir yapıya geçilmesi gerekmektedir. Bu yapıya geçilmesi için öncelikle veritabanı ve uygulama katmanı, uygulamadan diske kadar tümüyle entegre edilerek sanallaştırma yapılmalıdır.

Sanallaştırma yapıldıktan sonra kamu da bulut bilişim modeli oluşturulmalı, kamu bulutu hayata geçirilmelidir. Kamu bulutu ile birlikte, kamu da ortak ihtiyaçlar için ortak kullanım alanları yaratılarak verimsizlik ortadan kaldırılabilecektir. Bulut bilişimle, kurumlar daha az enerji tüketip daha az donanım ve daha düşük maliyetlerle ihtiyaçlarını karşılayabilecek, yönetim kolaylığı ve esneklik sağlanacaktır. Bu kapsamda, öncelikli olarak kamu veri merkezlerinin bütünleştirilmesi çalışmaları tamamlanmalı, sanallaştırma ve bulut bilişim altyapı

ve uygulamaları için usul ve esaslar belirlenmeli, gerekli teknik, idari ve yasal altyapı oluşturularak ve kamu uygulama platformu hayata geçirilmelidir.

Kamu kurumlarına yönelik bir bulut bilişim altyapısı için gerek bulut bilişim altyapısı, gerekse bu altyapı üzerinde çalışması planlanacak ince istemci gibi çözüm ve teknolojilere ilişkin ilke, esas ve standartlar hayata geçirilmelidir. Ayrıca, konuyla ilgili teknoloji ve çözümlere ilişkin Ar-Ge çalışmaları yürütülmeli, e-Posta, içerik yönetimi vs. gibi uygulamalar, kamu bulut bilişim modeli kapsamında değerlendirilmelidir.

Kamuda bulut bilişime geçilmesi ile kamu bilgi işlem birimlerinin, hizmet vermekte oldukları alanlara odaklanarak daha nitelikli e-Devlet projelerinin ortaya çıkması sağlanabilecektir. Ayrıca, bulut bilişim ortak uygulamaların ortak uygulama standartlarında etkin bir şekilde hayata geçirilmesine destek olmakta, felaket kurtarma merkezlerinin hayata geçirilmesi konusunda büyük kolaylıklar sağlamaktadır. Bulut bilişim altyapısının yedekli olarak hizmet verebilecek şekilde tasarlanması ile kamu bilgi sistemleri tarafından verilen hizmetlerin felaket anında da kesintiye uğramaması daha etkin bir şekilde mümkün olabilecektir.

Risk yönetimini sağlıklı bir şekilde yapabilmek için risk yönetim süreçlerinin işletilmesi gerekmektedir. Burada en önemli nokta riski doğuran tehditlere karşı önlem almak ve benzer tehditlerin önünü kesmek için gerekli ARGE çalışmalarının yapılmasıdır.

Güvenlik boyutunda fiziksel güvenliğin yanı sıra dijital güvenliğin de sağlanması gerekmektedir. Dijital veri güvenliğini sağlamak için donanımsal, yazılımsal ve uzman personel ihtiyaçlarına önem verilmelidir.

Tüm kamu kurumlarının ihtiyacını karşılayacak bir veri merkezinin kurulmasında yaşanacak sorunlar birer risk teşkil etmektedir. Bu riski ortadan kaldırmak için veri merkezi kurulmadan önce tüm boyutlarda projelendirmelerin yapılması gerekmektedir.

Veri merkezinin bulunduđu yerin sıcaklıđının kullanılan donanıma zarar vermeyecek düzeyde olması gerekmektedir. Yapay sođutma sistemlerine olan ihtiyacı azaltacak bir konumda bulunması sođutma maliyetini de dűşürecektir. Kurulacak veri merkezinin mevcut fiber alt yapısına uygun bir konumda olması maliyetleri dűşüreceđi gibi hızı da artıracaktır.

Gűney Kore őrneđinde olduđu gibi Kamu Entegre Veri Merkezi en az 3 noktada kurulmalıdır. Kurulacak olan veri merkezinden biri gizli olmalı ve diđer veri merkezlerinin yedeđini tutmalıdır. Her bir veri merkezi ise kendi yedeđini tutmalıdır.

Veri Merkezinde kullanılan donanım ve yazılım tedariki TIER standartlarına gűre olmalıdır. Veri merkezinde alıřacak kiřilerin sadece kendi alanlarında uzmanlařmıř kiřiler olmasına dikkat edilmeli ve alıřan personelin sűrekli test ve eđitimlere tabi tutulması gerekmektedir.

KAYNAKLAR

ALEXA, 2014, The Top 500 Sites On The Web, <http://www.alexa.com/topsites>, (05.08.2014)

ALPARSLAN Erdem, Sanallaştırma Ve Sanallaştırmanın Büyük Oyuncusu VMware, <http://www.enderunix.org/docs/Sanallastirma.pdf>, (18.04.2014)

AFYONLUOĞLU Mustafa, 2014, Kamu Entegre Veri Merkezi ve Türkiye: Bizi neler bekliyor?, <http://www.bthaber.com/kamu-entegre-veri-merkezi-ve-turkiye-bizi-neler-bekliyor/>, (05.07.2014)

ANADOLU BİLİŞİM, 2013, ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı Nedir?, Anadolu Bilişim Hizmetleri A.Ş. , <http://www.abh.com.tr/ebulten/mayis-2013/haber2.htm>, (01.02.2014)

BİLGE Tufan, 2009, Sistem Odası Nasıl olmalı?, Bilişim News, <http://www.bilisimnews.com/sistem-odasi-datacenter-nasil-olmali/>, (04.03.2014)

BTK, 2010, Yeşil Bilişim, BTK Sektörel Araştırma ve Stratejiler Dairesi Başkanlığı, s.28-74.

BTK, 2013, Bulu Bilişim, Bilgi Teknolojileri ve İletişim Kurumu, s.9, Mayıs 2014

ÇAĞLAYAN Yusuf, 2009, SGK Sanallaştırma Süreçlerini Tamamladı, <http://new.bthaber.com.tr/?p=913>, (10.02.2014)

ÇAVDAR Derya, ALAGÖZ Fatih, 2013, Yeşil Veri Merkezlerinde Enerji Verimliliği, Akademik Bilişim Konferansı, s.1

ÇEVİRİM Can, 2013, Facebook'un Devasa Veri Merkezi İnşaatına Başlandı, http://www.tamindir.com/facebookun-devasa-veri-merkezinin-insaatina-baslandi_h-3480/, (10.08.2014)

CHIP, 2012, Google'ın Veri Merkezi Street View'da, http://www.chip.com.tr/haber/google-in-veri-merkezi-street-view-da_36526.html, (10.08.2014)

CISCO, Veri Merkezi ve Sanallaştırma, <http://www.cisco.com/web/TR/solutions/datacenter/architecture.html>, (13.05.2014)

DEMİREL Fırat, 2012, Facebook'un 200 Milyon Dolarlık Veri Merkezi, <http://webrazzi.com/2012/03/05/facebookun-200-milyon-dolarlik-veri-merkezi-bize-ne-anlatiyor/>, (01.08.2014)

DOĞANTİMUR Fulya, 2009, ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği, Maliye Bakanlığı Mesleki Yeterlilik Tezi, Ankara, s.11

e-GOVERNMENT OF KOREA, 2011, Government Integrated Data Center (GIDC), Ministry of Public Administration and Security, s.4-22.

FRIES Todd, TYTON Hellermann, 2009, The ANSI/TIA/EIA-606-A Addendum 1, s.2.

GOOGLE, Data Centers, <https://www.google.com/about/datacenters/>, (01.08.2014)

GÖKCEN Serdar, 2010, Sanallaştırma Nedir?
http://www.chip.com.tr/blog/pcmaker/sanallastirma-virtualization-nedir-i_4601.html, (04.04.2014)

GÖKMEN Hüseyin T., KÜÇÜKSİLLE Ecir U., 2013, Veri Merkezi Tasarımı, s.4, Mart 2013

GÜROL Mehmet, YAVUZALP Nuh, 2011, Okullarda ve Eğitim Kurumlarında Sanallaştırma Teknolojileri, Elazığ, s.5, Şubat 2014

HENKOĞLU Türkay, KÜLCÜ Özgür, 2013, Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme, Sayı 14(1), s.64-66

IDC, 2008, Defining "Cloud Services" and "Cloud Computing, Mart 2008

IDC, 2012-2016, World Wide Public IT Cloud Services, Mart 2014

IDC, 2013, IDC Predictions 2014: Battles for Dominance and Survival on the 3rd Platform, IDC, <http://www.idc.com/getdoc.jsp?containerId=244606>, 2014

IDC, The State of Public Cloud Computing in Turkey's Government Sector, Nisan 2014

ISO, 2010, ISO/IEC 24764:2010 Information Technology, Generic Cabling Systems For Data Centres,

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43543, Mayıs 2014

İNTERSİSTEM TEKNİK SERTİFİKASYON LTD. ŞTİ., ISO 20000 NEDİR?, <http://www.belgelendirme.com.tr/belgelendirme-standartlari/iso-20000-standart/255-iso-20000-nedir>, (04.01.2014)

KEPEKÇİ Steve, 2004, Data Center Standarts Roundup, BCSİ, https://www.bicsi.org/uploadedfiles/PDFs/Presentations/Region_Events/canadian_Lachine,%20QC_4-27-11/Data%20Center%20Standards%20Roundup%20-%20Steve%20Kepekci.pdf, (14.02.2014)

KOÇAK Halil İ., Felaket Kurtarma Merkezi ve İş Sürekliliği, <http://tutev.org.tr/makaleler/felaket-kurtarma-merkezi-ve-is-surekliligi>, (15.04.2014)

KORKMAZ Yakup, Bulut bilişim:Türkiye için fırsatlar, Nisan 2014

KPMG, 2013, Uluslararası Destek Hizmetleri Uygulamaları, Şubat 2014, s.30

- MATARACIOĞLU Tolga, 2013, Veri Merkezlerinin Sahip Olması Gereken Özellikler, TÜBİTAK BİLGEM, <https://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/veri-merkezlerinin-sahip-olmasi-gereken-ozellikler.html>, (04.11.2013)
- MELL Peter, GRANCE Timothy, 2011, The NIST Definition of Cloud Computing. National Institute of Standards and Technology, U.S. Department of Commerce,s.2-3, Haziran 2014
- MİCROSOFT, Server and Cloud Platform, <http://www.microsoft.com/en-us/server-cloud/products/sql-server/#fbid=7v7NOfe2fRv>, (05.04.2014)
- MİRZAOĞLU Ayşe G., 2011, Bulut Bilişimin Teknik, Uygulama ve Düzenleme Boyutuyla Değerlendirilmesi Dünya Örnekleri ve Ülkemize İlişkin Öneriler, BTK Bilişim Uzmanlığı Tezi, Ankara, s.8-65.
- MOHAMED Yehia H.K., 2011, Data Center Resilience Assesment:Storage, Networking and Security, University of Louisville, Louisville, s.8
- NCIA, 2012, 2012 Achievemnts, <http://korea.ncia.go.kr/index2.html>, (03.04.2014)
- NTVMSNBC, Facebook'un ABD Dışındaki İlk Veri Merkezi, <http://fotogaleri.ntvmsnbc.com/facebookun-abd-disindaki-ilk-veri-merkezi.html>, (04.08.2014)
- ÖZDAŞ Muhammed R., 2014, Bulut Bilişimin Kamuda Kullanımı: Dünya Örnekleri ve Türkiye için Öneriler, Kalkınma Bakanlığı Uzmanlık Tezi, Ankara, s.5-14
- ÖZATAY Mustafa S., 2012, Bilişim Sektörü ve TRB1, s.8-9, <http://www.fka.org.tr/ContentDownload/Bili%C5%9Fim%20Sekt%C3%B6r%C3%BC%20ve%20TRB1.pdf>, (03.12.2013)
- RADORE, 10 Büyük Markanın Veri Merkezleri, <http://blog.radore.com/iste10-buyuk-markanin-veri-merkezleri.html>, (10.08.2014)
- RENDA Scott, 2011, 'Cloud First' Policy Insights. EC-ETSI Standards in the Cloud Workshop, Whitehouse, s.4.
- SAHİNASLAN Ender, KANDEMİR R., SAHİNASLAN Ö., 2010, "Examinations Results of International Standard Approaches in Developing Information Security Risk Analyses and Assessment Method", ISCSE 2010, İzmir, Mayıs 2014
- SEZGİN Onur, AKDEMİR Görkem, 2014, E-Devlet ve e-Dönüşüm, Türk Hava Kurumu Üniversitesi, <http://ece581.files.wordpress.com/2013/11/ece581-ulusal-kamu-veri-merkezi.pdf>, (17.03.2014)
- STAMFORD Conn., 2014, Gartner Says Worldwide IT Spending On Pace to Reach \$3.8 Trillion in 2014,Gartner, <http://www.gartner.com/newsroom/id/2643919>, (10.06.2014)

SUPERONLINE, 2012, Superonline Veri Merkezi Hizmetleri,
https://www.turkcellakillibulut.com/assets/images/faq/files/Sunumlar/Turkcell_Superonline_Veri_Merkezi_Hizmetlerimiz_13022012_v12.pdf , (01.02.2014)

SYDGM, 2009, Sanallaştırma Projesi, Sosyal Yardımlaşma ve Dayanışma Genel Müdürlüğü, <http://www.sydgm.gov.tr/tr/html/340/Sanallastirma+Projesi>, (06.03.2014)

STATISTICA, 2014, Number Of Monthly Active Facebook Users Worldwide As Of 2nd Quarter 2014, Ağustos 2014

STEVENS Alan, 2011, When Hybrid Clouds Are A Mixed Blessing, Mart 2014

STRICKLAND Jonathan, How Cloud Computing Works,
<http://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm>, (06.05.2014)

ŞAHİNASLAN Ender, 2011, Bilgi ve Bilgi Teknolojilerine Ait Risklerin Yönetilmesinde Arayış, Yöntem ve Çözüm Önerileri, XIII. Akademik Bilişim Konferans Bildirileri, Mayıs 2014, s.568

TANRIKULU Haluk, E-devlet ve İnternet Veri Merkezleri, Türk Telekomünikasyon A.Ş. Bilişim Ağları Dairesi Başkanlığı, Ocak 2014, s.3

TBD Kamu-BİB, 2010, Sanallaştırma, Türkiye Bilişim Derneği,
http://www.tbd.org.tr/usr_img/cd/kamubib12/raporlarPDF/RP1-2010.pdf, s.17, (10.02.2014)

TBD, 2013, 2023 Vizyonu Çerçevesinde Bilişim Merkezleri ve Yöneticilerinin Değişen Rolü, s.33-65,
http://www.tbd.org.tr/usr_img/cd/kamubib15/raporlarPDF/RP1-2013.pdf, 05.04.2014

TÜRK TELEKOM, Türk Telekom Veri Merkezi,
<http://www.ttv.com.tr/ttvmdp.web/idc/aboutUs.xhtml>, (03.03.2014)

TURAN Serhat, 2011, Bulut Bilişimi Teknolojisi ve Hukuki Problemler, Mart 2014

UBAK, 2005, İnternet Veri Merkezi Uygulamalarının Ekonomisi ve Yapılabilirliği, Teknik Altyapı ve Bilgi Güvenliği Çalışma Grubu, Ulaştırma Bakanlığı, Ankara, s.9-17, (2014)

UDHB, 2013, BYTK'nın 25. Toplantısında Alınan Bakanlığımızın Sorumlu Olduğu Kararlar,
http://www.tubitak.gov.tr/sites/default/files/02_btyk26_udhb_sunum_11062013web.pdf , s.12-14, 20.04.2014

U.E.P.Agency, 2007, Data Center Report to Congress, U.S. Environmental Agency, Tech Rep., s.7

ULUSLARARASI BELGELENDİRME&DENETİM LTD. ŞTİ., ISO 9001 Nedir? <http://belgelendirme.ctr.com.tr/iso-9001-nedir.html>, (03.01.2014)

UPTİME İNSTİTÜTE, 2008, Tier Classifications Define Site Infrastructure Performance, Santa Fe, Ocak 2014.

UPTİME İNSTİTÜTE, 2009-2012, Data Center Site Infrastructure Tier Standard: Topology, New York, Ocak 2014

U.S. ENVİRONMENTAL PROTECTION AGENCY, 2007, Data Center Report to Congress, http://www.theregister.co.uk/2013/08/16/it_electricity_use_worse_than_you_thought, (10.04.2014)

UYANIK İlker E., 2013, Türk Telekom Veri Merkezleri, BGD Veri Merkezleri Konferansı, Mart 2014

WIKİPEDIA, 2013, Sanal Makine, http://tr.wikipedia.org/wiki/Sanal_makine, (10.01.2014)

WIKİPEDIA, 2014a, Veri Merkezi, http://tr.wikipedia.org/wiki/Veri_merkezi, (03.10.2013)

WIKİPEDIA, 2014b, Popek and Goldberg Virtualization Requirements, http://en.wikipedia.org/wiki/Popek_and_Goldberg_virtualization_requirements, (10.03.2014)

WIKİPEDIA, 2014c, Virtualization, <http://en.wikipedia.org/wiki/Virtualization>, (10.04.2014)

WIKİPEDIA, 2014d, Bulut Bilişim, http://tr.wikipedia.org/wiki/Bulut_bilişim, (10.04.2014)

WHITEHOUSE, 2011, <http://www.whitehouse.gov/blog/2011/07/20/shutting-down-duplicative-data-centers>, (04.03.2014)

WORKCUBE, 2014, Bulut Bilişimin Avantaj Ve Dezavantajları Neler? <http://www.workcube.com/bulut-bilisimin-avantaj-ve-dezavantajlari-neler>, (10.03.2014)

YALÇINTAŞ Lebibe, 2013, İnternet Değişim Noktası ve Veri Merkezlerinin Bilgi Güvenliği Perspektifinden İncelenmesi; Dünyadaki Durum ve Ülkemiz İçin Öneriler, Bilgi ve İletişim Teknolojileri Kurumu Uzmanlık Tezi, Ankara, s.71-75

YAZICI Ebru, 2013, Kamuda Ortak Veri Merkezine Hazır mıyız?, <http://www.innova.com.tr/blog/yazi.asp?ID=133&baslik=Kamuda-ortak-veri-merkezine-hazir-miyiz>, (10.04.2014)

YEŞİLİRMAK Umut İ., 2010, Sosyal Yardım Alanında Bilişim Teknolojilerinin Kullanımı: Örnek Model Sosyal Yardım Bilgi Sistemi, Sosyal Yardım Uzmanlık Yeterlilik Tezi, Ankara, s.49-51

YILDIZ Özcan R., 2009, Bilişim Dünyasının Yeni Modeli: Bulut Bilişim (Cloud Computing) Ve Denetim, Sayıştay Dergisi, Sayı 74-75, s.8

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 Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Ulaştırma ve Haberleşme Uzman ve Uzman Yardımcılarının Sınav, Atama, Çalışma Usul ve Esasları Hakkında Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığını 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.

(Tarih)

(İmza)

Günseli AYTAÇ
CANKURTARAN

ÖZGEÇMİŞ

1985 yılında Ankara'da doğdu. İlkokul, ortaokul ve lise öğrenimini Ankara'da tamamladı. 2008 yılında Gazi Üniversitesi, Fen Edebiyat Fakültesi, İstatistik Bölümünden mezun oldu. 2009-2011 yılları arasında Tarla Bitkileri Merkez Araştırma Enstitüsü'nde Programcı olarak görev yaptı. 2011 yılı Mart ayında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nda Ulaştırma ve Haberleşme Uzman Yardımcısı olarak göreve başladı. Halen Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Haberleşme Genel Müdürlüğü'nde Uzman Yardımcısı olarak çalışmaktadır.