T.C.

ALTINBAŞ ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü / Bilişim Teknolojileri

BULUT BİLİŞİMİN GELİŞİMİ VE MICROSOFT AZURE ORTAMINDA ÖRNEK BİR WEB UYGULAMASI

Orhan KAHRAMAN

Yüksek Lisans Tezi

Danışman

Dr. Öğr. Üyesi Sefer KURNAZ

Istanbul, 2019

BULUT BİLİŞİMİN GELİŞİMİ VE MICROSOFT AZURE ORTAMINDA ÖRNEK BİR WEB UYGULAMASI

Orhan KAHRAMAN

Bilişim Teknolojileri

Yüksek Lisans Tezi

ALTINBAŞ ÜNİVERSİTESİ

İstanbul, 2019

Bu tezi okuduğumuzu; kapsam ve nitelik bakımından Yüksek Lisans tezi olarak yeterli bulduğumuzu beyan ederiz.

_____

Dr. Öğr. Üyesi Sefer KURNAZ

Sınav komitesi: (Yazılan ilk isim jüri başkanı, ikinci isim danışman olmalıdır.)

Prof. Dr. Osman Nuri UÇAN	Mimarlık ve Doğa Bilimleri Fakültesi Altınbaş Üniversitesi	_____
Dr. Öğr. Üyesi Zeynep ALTAN	Mühendislik ve Mimarlık F. Beykent Üniversitesi	_____
Dr. Öğr. Üyesi Sefer KURNAZ	Fen Bilimleri Enstitüsü Altınbaş Üniversitesi	_____

Bu tezin Yüksek Lisans. tezi olarak bütün şartları sağladığını beyan ederim.

_____

Dr. Öğr.Üyesi Oğuz ATA

Anabilim Dalı Başkanı

Fen Bilimleri Enstitüsü kabul tarihi:

____/____/____

_____

Prof. Dr. Oguz BAYAT

Enstitü Müdürü

Bu tezdeki tüm bilgilerin akademik kurallara ve etik davranışlara uygun olarak edinildiğini ve sunulduğunu beyan ederim. Ayrıca, bu kuralların ve davranışların gerektirdiği şekilde, bu çalışmada, orijinal olmayan tüm materyalleri ve sonuçları tamamen alıntı yaptığımı ve referans gösterdiğimi de beyan ederim.

Orhan KAHRAMAN

ÖZET

BULUT BİLİŞİMİN GELİŞİMİ VE MICROSOFT AZURE ORTAMINDA ÖRNEK BİR WEB UYGULAMASI

KAHRAMAN, Orhan

Yüksek Lisans Tezi / Bilişim Teknolojileri/ Altınbaş Üniversitesi

Danışman: Dr. Öğr. Üyesi Sefer KURNAZ

Tarih: Temmuz, 2019

Sayfa: 103

Bilişim teknolojileri gündelik yaşamda kurum ve kişiler için olmazsa olmaz hale gelmiştir. Son zamanlarda gelişen teknolojik gelişmeler ve internet bant genişliklerinin arması ile beraber, akıllı telefon ve tabletlerin, akıllı el saatleri ve nabız kontrol bileklikleri vb. cihazların da ortaya çıkmasıyla ticari faaliyet gösteren firmaların sayısında artış gözlemlenmiştir. Bunun sonucunda bilgi teknolojilerinde bulut bilişim olarak bilinen "*Cloud Computing*" kavramı günümüzde popüler olmuştur. Bulut bilişim kısacası fiziki bir bilgisayarın tüm yazılım ve donanımlarının diğer kullanıcıların kullanım ihtiyaçlarına göre ayrılarak kullanılabilmesidir. Bu kullanıcılar zaman ve mekân sınırlamasından kurtarır. Böylece internet kullanımı olan her yerden erişim olanağı sunmaktadır. Bulut bilişim son zamanlarda gelişmesine hız vermiş bir teknolojik yapıdır. Bu gelişme kapsamında şüphesiz bulut bilişimin sanallaştırılması işlemidir. Bu işlemler sayesinde kullanıcıların ekonomik olarak zorluklar yaşadıkları lisans maliyetleri azalmaktadır. Hizmet kullanıcıları tek yazılım lisansıyla birden fazla kullanıcının kullanımına olanak sağlayan bir yapı kullanmaktadırlar. Bulut bilişim kullanıcılarına sunduğu avantajları vardır. Kısacası veri merkezlerine ihtiyaç duymaması, nitelikli eleman çalıştırmaması, lisans maliyetlerinin olmaması, sunucu odaları gibi karmaşalara gerek duyulması vb. gibi olanaklar sağlamaktadır. Bunun yanında birde dezavantajları da bulunmaktadır. Bunlar kısacası veri güvenliğine dayalıdır. Hizmet sağlayıcılarının verilere erişim yetkilerinin

olması ve genel yedekleme alımı durumunda hizmet sağlayıcıları tarafından yapılması, kullanıcılara tereddüt vermektedir. Hukuksal anlamda da Türkiye bulut bilişimde veri kaybına yönelik oluşabilecek bir kayıpta hizmet sağlayıcılarına yönelik bir yaptırım bulunmamaktadır. Çünkü bulut hizmeti sağlayan firmaların veritabanlarını genellikle dış ülkelerdedir. Bu kullanıcıların bir veri kaybı ya da hizmet aksaması yaşaması durumunda elini kolunu bağlamaktadır. Bu çalışmada bulut bilişimin tarihi, temelleri, servis modelleri, bulut bilişim konumlandırma modelleri, bulut bilişimin avantaları, bulut bilişimin dezavantajları, sanallaştırma ve platformları, saldırı tespit sistemleri, güvenilir bilişim ve Microsoft Azure platform incelemesi yapılmıştır. Daha sonra Microsoft Azure ortamında hizmete sunulan Sanal Sunucu kurulumu, SQL veritabanı kurulumu ve bunlar üzerinde host edilen bir kişisel bir web sitesi uygulaması yapılmıştır.

Anahtar Kelimeler: Bulut Bilişim, Bulut Bilişimin Avantajları, Bulut Bilişimin Dezavantajları, Sanallaştırma, Sanallaştırma Platformları, Microsoft Azure, Sanal Sunucu Kurulumu.

ABSTRACT

DEVELOPMENT OF CLOUD INFORMATICS AND A SAMPLE WEB APPLICATION IN MICROSOFT AZURE ENVIRONMENT

KAHRAMAN, Orhan

M.Sc. / Information Technologies/ Altınbas University

Supervisor: Asst. Prof. Dr. Sefer KURNAZ

Date: July, 2019

Pages: 103

Information technologies have become indispensable for institutions and individuals in daily life. With the recent technological advances and the emblem of Internet bandwidths, smartphones and tablets, smart watches and pulse control wristbands etc. the number of firms operating in commercial activity increased. As a result, olarak cloud computing oloj, which is known as cloud computing in information technologies, has become popular today. Cloud computing is in short, all the software and hardware of a physical computer can be used according to the needs of other users. This saves users time and space limitation. This allows you to access from anywhere with internet use. Cloud computing is a technological structure that has accelerated its development recently. Within the scope of this development, it is undoubtedly the process of virtualizing cloud computing. These processes reduce the licensing costs of users experiencing economic difficulties. Service users use a structure that allows multiple users to use a single software license. Cloud computing has the advantages it offers its users. In short, it does not need data centers, does not employ qualified personnel, does not have licensing costs, such as server rooms, etc. need to complex. facilities such as; There are also disadvantages. In short, they are based on data security. The fact that service providers have access to data and is made by service providers in the event of a general backup is hesitating to users. There is no sense in legal sanctions against a loss service providers for data loss that may occur in my cloud Turkey. Because the companies providing cloud services are usually in foreign countries. This handles the user in the event of a data loss or service disruption.

In this study, the history, basics, service models, cloud computing positioning models, the advantages of cloud computing, the disadvantages of cloud computing, virtualization and platforms, intrusion detection systems, reliable informatics and Microsoft Azure platform review were conducted in this study. Then, a Virtual Server installed in the Microsoft Azure environment, SQL database installation and a personal website hosted on them was implemented.

Keywords: Cloud Computing, Advantages of Cloud Computing, Disadvantages of Cloud Computing, Virtualization, Virtualization Platforms, Microsoft Azure, Virtual Server Installation.

İÇİNDEKİLER

Sayfa

TABLO LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

KISALTMALAR

BT	Bilişim Teknolojileri
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AES	Gelişmiş Şifreleme Standardı
ARGE	Araştırma Geliştirme
BT	Bilişim Teknolojileri
BTK	Bilgi Teknolojileri Kurumu
DDOS	Dağıtık Hizmet Saldırıları
e-devlet	Elektronik Devlet Sistemi
GB	Gigabyte
IAAS	Altyapı Servisi
IP	Internet Protokol
IT	Bilişim Teknolojisi
KOBİ	Küçük ve Orta Ölçekli İşletmeler
MB	Megabyte
NCIA	Ulusal Bilişim ve Bilgi Ajansı
NIST	Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü
PAAS	Platform Servisi
Polnet	Polis Bilgi Sistemi
RDP	Uzak Masaüstü Bağlantısı
SAAS	Yazılım Servisi

SOA	Servis Odaklı Mimari
VPN	Sanal Özel Ağ

1.GİRİŞ

Gelişen teknolojiler ve yazılımlar, kullanıcıların zihinlerinde yer edinen bilgisayar algısını yok edip, artık kendisini masaüstü bilgisayarlardan; akıllı telefonlara, tabletlere, saatlere bırakmaktadır. Kullanıcı farkındalığının da artmasına bağlı olarak geniş bir ürün yelpazesiyle pazarda önemli bir yer edinen bu teknolojik gelişmeler hayatımızda hatırı sayılı bir yer edinmektedir. Ve bu teknolojik gelişmeler yapılan Pazar araştırmalarıyla ortaya çıkmaktadır. Örnek olarak Juniper araştırma şirketinin raporuna[1] göre 2013 yılının sonunda 8 milyar dolar olarak verilen satış hasılatının 2019 yılına 53,2 milyar dolara ulaşması bekleniyor.

Bulut bilişim ismini son zamanlarda çok fazla duyduğumuz bir kavram olmuş oldu. Bulut teknolojisi ile kaynakla ve verilere mekandan bağımsız bir şekilde erişme ve kontrol edebilme imkanı sağlıyor. İlk olarak 2006 ayılında Amazon şirketi tarafından verilmeye başlanan bulut hizmetleri[2], günümüzde birçok kullanıcı ve firma tarafından kullanıma hazır olarak kullanıcıların hizmetine sunulmuştur. Bu gelişmelere paralel olarak yazılım ve donanım şirketlerinin yeni kazanç kapıları da aralanmış oldu. Her bir firma kendine göre yazılımları geliştirmeye ve daha iyi hizmet verebilmek için yarışır hale gelmelerine olanak yaratmıştır. Bu da paralel olarak pazarın büyümesine ve gelişmesine, kullanıcıların daha ucuz ve güvenilir platformları kullanımına olanak sağlamıştır.

2010'un başlarından itibaren akıllı mobil teknolojileri hızla gelişmiş ve hayatımızın ayrılmaz bir parçası haline gelmiştir. Özellikle akıllı mobil teknolojiler (cep telefonları, akıllı saatler vs.) günümüzde hemen hemen herkes tarafından kullanılmaktadır. Bu teknoloji ile beraber verilere erişim her yerden ulaşılabilir olmuştur. Günümüz veri merkezleri (Data Center) alt yapılarını oluştururken bunları göz önünde bulundurmak ve yatırımlarını buna göre oluşturmak zorundadırlar.

2. BULUT BİLİŞİM

Bulut bilişimle ilgili günümüzde farklı farklı terimlerle tanımlanmalar yapılmaktadır. Ancak bu konuda yetkin bir kurum olan ABD Ulusal Standartlar ve Teknoloji Enstitüsü NIST[2] yayınında bulu bilişimi "düşük seviyede yönetim çabası ya da hizmet sağlayıcı etkileşimi ile hızlı bir şekilde sağlayıp serbest bırakabilen, bilgisayar ağları, sunucular, depolama, uygulamalar ve servisler gibi ayarlanabilir (configurable) bilişim kayaklarının müşterek/ortak havuzuna her yerden, elverişli bir şekilde istenildiğinde ağa erişim sağlayan bir model" şeklinde tanımlamaktadır (NIST, 2013, s.8). Başka bir deyişle bulut bilişim, esnek ve dinamik olarak ölçeklenebilir ve yoğun bir şekilde sanallaştırılabilir kaynakların internet üzerinden sağladıkları hizmetler olarak yeni bir bilişim türüdür(Furht, 2010, s.3).

Dijital dünyanın yaşantımıza sunduğu yeni sayılmayan çok yeni sayılmasa da yeni bir teknoloji olarak tüm dünyada hızlıca bir biçimde yaygınlaşmaktadır. Bulut bilişim özellikle İnternetin kullanılmaya başlaması ile ortaya çıkmış ve gelişmesi ile önemlini arttıran bir bilişim hizmeti halini almıştır. (Laudon ve Laudon, 2012, s.170). Günümüzde insanların sosyal medyayı aktif kullanması ve buna bağlı olarak Web 2.0 teknolojisinin gelişimi ile birlikte hız, güven, süreklilik gibi kavramlar önem kazanmaya başlamıştır. Sonucunda gmail+, picasa, Flickr, Dropbox vs. gibi daha birçok sosyal medya aracı hem sosyal medya hem de bulut bilişim örnekleri olarak kullanılmaktadır. (O'Reilly, 2005). Bu açıdan bakıldığında web yazılım ve teknolojilerinin gelişimi ile bulut bilişim ve sosyal medya araçlarının yaygınlaşması aynı zamana denk gelmekte, arada ortak noktalar bulunmaktadır.

Şekil 2.1: Bulut Bilişimin Geçmişten Günümüze Gelişimi

Bulut hizmetlerinde bir hizmet alımı ve hizmet sunumu vardır. Bu durum hizmeti sunan için pazar payını arttırmaya yöneliktir ve müşteri memnuniyeti için önem arz etmektedir. Bu durumda çalışmalarına bu yönde yol verir ki kendisi için önemli olan yapı ve malzemeler, hizmet vereceği müşterileri içinde önem oluşturmaktadır. Pazarda söz sahibi olmak ve hizmetini pazarda yaşatabilmek için bunlara dikkat etmesi gerekmektedir. Öte yandan bulut hizmetleri dolayısıyla bir hizmet alımı ve hizmet sunumu söz konusu olmakta, bu durum bir harcama ve elde edilen bir kazancı ortaya çıkarmaktadır. Böylece vergi konusu doğmaktadır.

2.1. BULUT BİLİMİN TARİHİ

1960 ve 1970'lerde, bilişim ihtiyaçları sadece büyük ölçekli kurum ve kuruluşlar tarafından tarafından sahip olunabilen kişisel işlerden ziyade, büyük ve yoğun işlerde kullanılan oda büyüklüğünde pratik olamayan (mainframe) kullanılarak karşılamaktaydı. Üstelik söz konusu işlemler gerçek zamanlı olmamakla birlikte, kullanıcılar sadece kendileri ile ana bilgisayar arasında arayüz görevi gören terminaller aracılığı ile bu ana bilgisayarları kullanmaktaydılar.

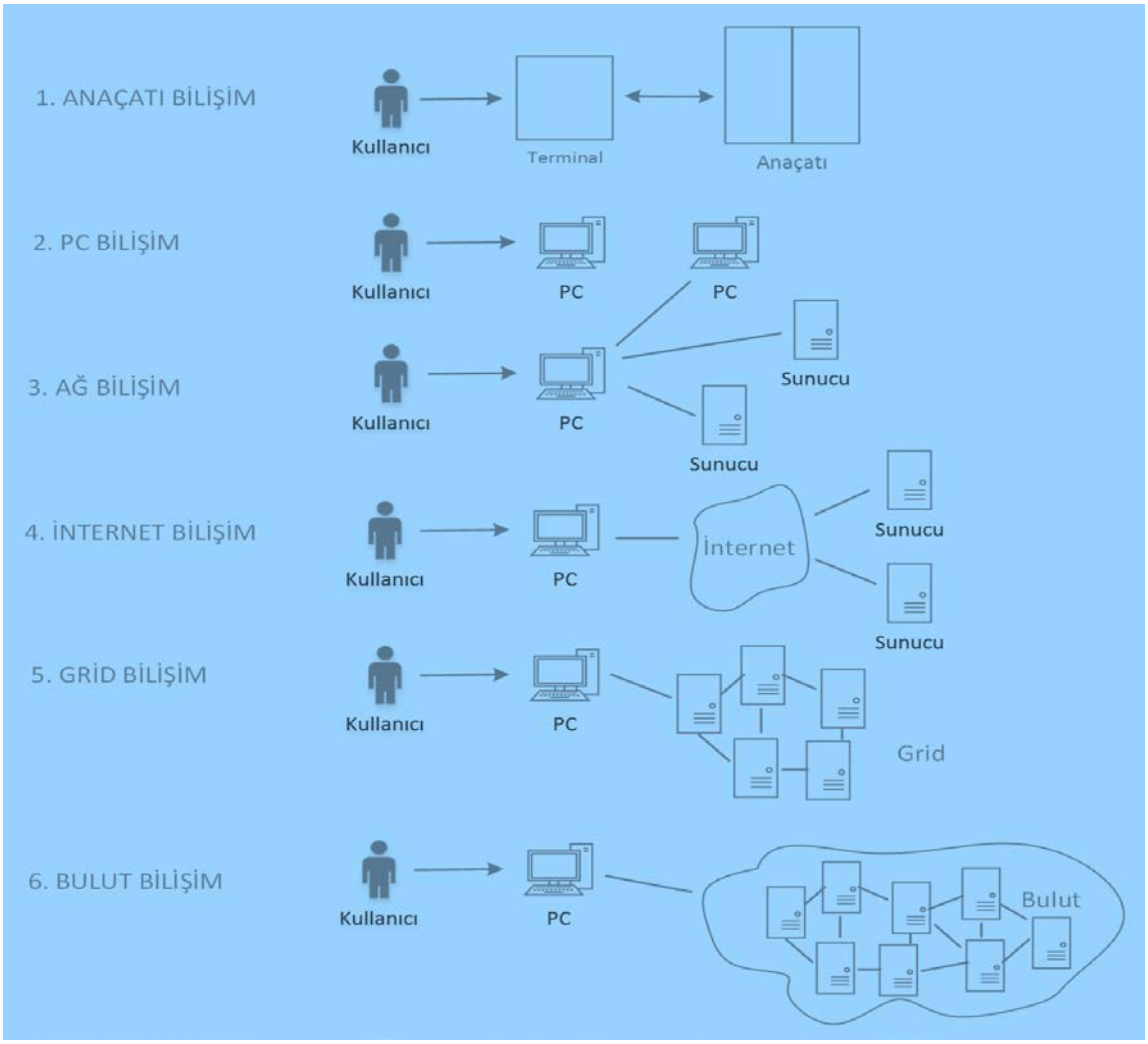
Şekil 2.2: IBM 360 entegre devre elemanlarının kullanıldığı ilk bilgisayar

1980'lerde terminal bilgisayarlar gelişen teknolojik gelişmeler ışığında daha küçük daha işlevsel olarak evlerde iş yerlerinde hizmet vermeye başladı. Bunun sonucunda da bellek ve işlemci kapasite ve performans arttırılarak kişisel bilgisayar (PC) niteliği kazanarak evlere girdi. Önceleri kontrol mekanizmasının ana bilgisayarın elinde olması ve işlemlerin kısıtlı yapılabilirliği, artık yerini daha çeşitli ve hızlı işlemlerin yapılabildiği kullanıcı lehine olan bilgisayarlara bıraktı. Bilgisayar bu sayede merkezcilikten sıyrılıp dağınık bir yapıya gelmiştir. Daha sonra PC artık donanım, yazılım ve işletim sistemleriyle çok büyük ve gelişimi açık bir pazar oluşturmuş oldu.

1990'ların sonunda ise, uzaktaki bilgi ve belgeleri paylaşmak amacıyla birbirine bağlanan veri aktarımı yapan LAN'lar İnternet'i meydana getirmişlerdir. İlk başlarda haberleşmek amacıyla ortaya çıkan İnternet, bant genişliği (bandwidht) ve bağlantı hızında ki artış, yaygınlaşması ve buna paralel olarak ücretlerde ki düşüş sayesinde temelde içerik paylaşımına dönük olarak kullanılır hale gelmiştir. İnternet hatlarının yaygınlaşması ile birlikte güvenlik açıkları doğmuştur. E-posta, web, adli ve idari evrak paylaşımı ve depolaması gibi avantajlarının bulunmasından dolayı buna paralel olarak yeni bir iş kolu ortaya çıkmıştır. Saldırı ve sızıntı (virüs-trojen vs.) yapmak kolaylaşmış ve önlem olarak şirketler (Ant-Virüs) adını verdikleri yazılımlar geliştirmişleridir. Bu şekilde veri ve bilgi koruyucu bir yapı çıkarmışlardır.

2000'lerde bilişim hizmetlerinde bakım, onarım, güvenlik ve personel vs. masraflarını azaltmaya yönelik arayışlar, bilişim teknoloji ve hizmetlerinin dışardan alınması arayışına sevk etti insanları. Bu arayış dağıtımlı bilişim (grid computing), kamu hizmeti bilişimi (utility computing) ve barındırma (hosting) gibi kavramları doğurmuştur. Dağıtımlı bilişim, homojen olmayan bilgi teknolojilerinin kaynaklarının (sunucu, depolama sistemlerinin, ağ elemanlarının vs.) ortak bir yerde toplanmasına (ızgara-grid) bu ortak yerde bilişim sistemi olarak kullanıcılara sunmasıdır. Bu projelerin kullanımı ve kullanımı kadar ödeme mantığıyla kamuya açık bir yapı şekline de kamu hizmeti bilişimi olarak tanımlanır.

Kısıtlı bir şekilde verim sağlayan dağıtımlı bilişim, kamu hizmetleri bilişimi, barındırma ve benzeri hizmet modelleri, ihtiyaca göre kapasite attırımı yad a azaltımı gibi temel özelleri sağlayamamış ve bulut bilişim modelinin temeline zemin hazırlamıştır. Veri gelişim süreci Furht ve Escalente [3]'te Sekil 2.3'te gösterilmektedir.



Şekil 2.3: Veri gelişim süreci Furht ve Escalente

2.2. BULUT BİLİŞİMİN TEMELLERİ

Bulut bilişimin mantığı, verilerin ve uygulamaların yer aldığı veri merkezlerinin fiziki araçlar ve gereçlerinin dahil olmak üzere ayrı coğrafi konumlarda yer alması ve kullanıcıların ortak olarak bu kaynaklardan yararlanması mantığına dayanır.

Bulut bilişim yapı teknolojisi yakın bir zamana dayanmaktadır. Kullanılan teknolojilerin mantığının değişmediğinden dolayı bu yapının hayata geçmesinden web hizmetleri, sanallaştırma ve grid bilişim teknolojilerin kullanılması ile mümkün olmuştur.

Bulut bilişim sektöründe hizmet veren bütün şirketler kendi platformlarını kullanabilme özgürlüğüne sahiptirler. Microsoft. Net platformu ile yol alırken, Sun şirketinin Java platformu

kullanması temel örnek olarak görülebilir. Hizmetlerinin sunan şirketler farklı platformları destekleyecek yazılımlar oluşturmaktadırlar.

2.2.1. Web Hizmetleri Teknolojisi

Web hizmetleri global internet teknolojisi üzerinden erişilebilen açık kaynaklı yazılımlardır. Yazılım açık kaynaklı kod olarak tasarlanmaları durumunda, farklı platformlara uygulanabilirliği doğmakta ve bağımsız kullanıcılar tarafından geliştirilerek hızlı bir gelişim ve kolaylık doğurur.

Açık kaynaklı bir yapı olması dolayısı ile her geçen gün her yazılımcı ayrı ayrı katkılar sunarak, sunulan hizmetlerde pratiklik sağlar. Web hizmetleri internet ortamında SOAP ve XML gibi standart protokoller ve ara yüzleri altyapı olarak kullandığından düşük maliyetli olmasının yanı sıra yazılım geliştiricilere daha hızlı bir geliştirme imkânı sunmaktadır. Bu sayede yazılım geliştiriciler programlarını internet ortamındaki diğer hizmetlerle pratik bir şekilde bütünleştirerek daha düşük maliyetli programlar ortaya koyabilmektedirler .

2.2.2. Sanallaştırma Teknolojisi

Sanallaştırma, fiziksel bir yapıyı ihtiyaca göre istenilen oranda mantıksal parçalara bölerek, sunucu verimliliği optimizasyonu sağlayan bir teknolojidir. Sanallaştırma teknolojisi ile fiziksel bilgisayar sayısı azalırken sanal bilgisayar sayısı artmakta ve mevcut donanım kapasitesi oldukça optimal bir şekilde kullanılabilmektedir. Bu sayede maliyet azalırken iş gücü verimliliği ve esneklik artmaktadır (Çelik, 2009).

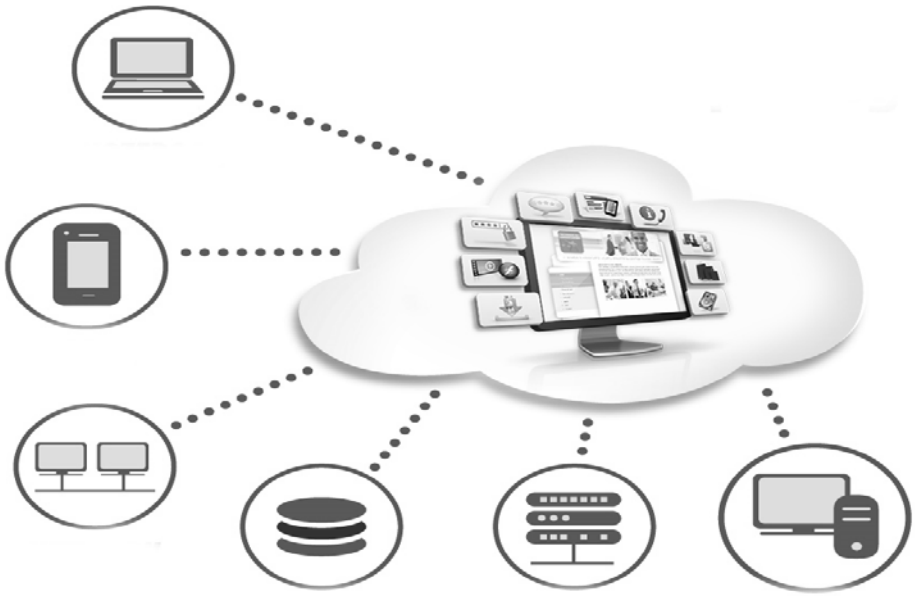
Giderek artan bir ihtiyaç vardır. Bunu fiziksel olarak bilgisayarlar kurmakla çözmek çok güçtür. Donanım ve yazılım maliyetlerinin yanında daha büyük bir fiziksel barındırma alanına ihtiyaç duyulacaktır. Kurumsal işletmeler ve büyük çaplı veri işleriyle uğraşanlar için, kaynak planlama (Enterprise Resource Planning; ERP) ve müşteri ilişkileri yönetimi (Customer Relationship Management; CRM) gibi birçok iş uygulamasının barındırma işlemlerini büyük çaplı sunuculara depolama ihtiyacı doğacaktır. Donanım ve yazılım maliyetlerini minimuma indirgemek adına, üzerinde birçok farklı uygulama ve yazılım sistemi bulundurabilen sanallaştırma teknolojisini tercih etmek mantıklı olmaktadır. Bir fiziksel bilgisayar üzerinde biden fazla sanal sunucu yapısı oluşturmak mümkündür. Bu sayede işlemlerin daha az maliyetli olması sağlanabiliyor. Bakım sermaye ve yatırıma önemli azalmalar sağlamasının yanı sıra

bakım ve sermaye yatırımlarından tasarruf sağlamak ve enerji tasarrufuyla daha çevreci bir sistem oluşturulmuş olmuştur.

Sistemlerin kesintisiz hizmet vermesi işletmeler için hayati önem taşımakta olduğundan, bu sistemlerin bakım ve yönetimi işletmeler için oldukça önemlidir, sanallaştırma teknolojileri sayesinde de bu önemli süreçte önemli avantajlar sağlanmaktadır.

2.2.3. Grid Bilişim Teknolojisi

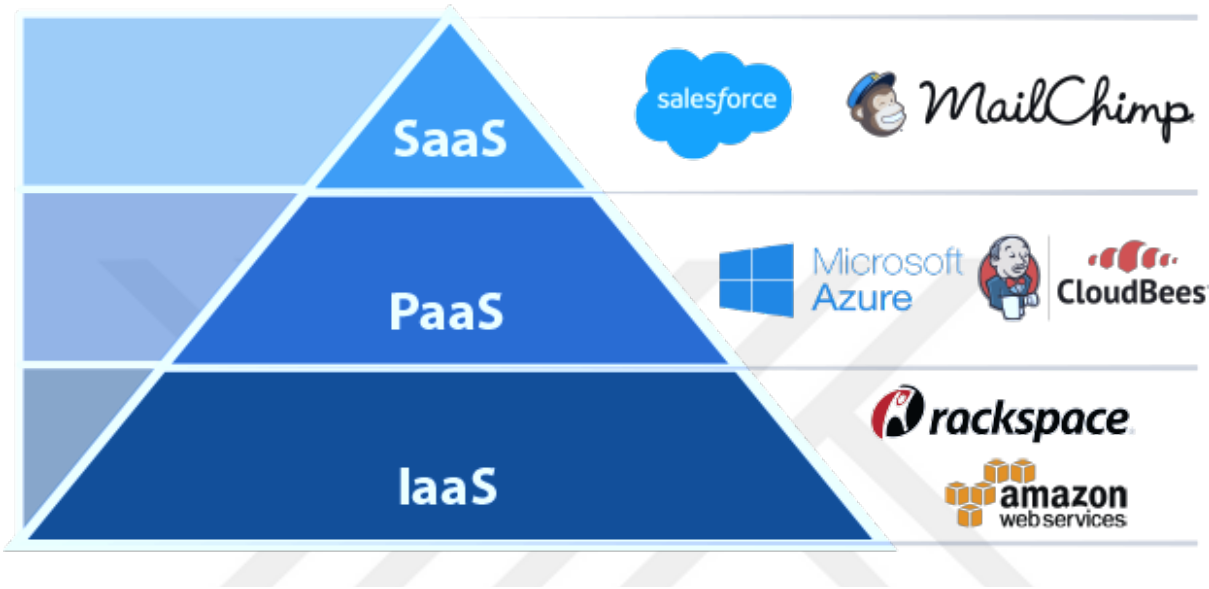
Grid teknolojisi fiziki sunucu ve bilgisayarların yüksek hızlı ağlarla bir araya getirilerek paylaştırılması işlemidir. Bilgisayarların gerçekleştirdiği hesaplama, depolama ve yazılımsal kaynakların atıl olan kapasiteleri değerlendirilerek daha da ha yüksek kapasitelere ulaşmasıyla verimlilik artışı sağlamaktadır[14].



Şekil 2.4: Fiziki Bir Bilgisayarın Grid Bilişim Mantığı ile Paylaştırılması

2.3. SERVİS MODELLERİ

Bulut bilişim servis modelleri Servis Olarak Yazılım (Software as a Services (SaaS)), Servis Olarak Platform (Platform as a Service (PaaS)) ve Servis Olarak Alt Yapı (Infrastructure as a Service (IaaS)) olmak üzere üç temel hizmet modelinden oluşmaktadır [Bulut bilişim hizmeti kullanıcısı kendi ihtiyacına göre modellemeler seçebilirler (Şekil 2.5).



Şekil 2.5: Bulut bilişim servis modelleri

Bu servis modellerine göre kullanıcılar SaaS ile herhangi bir kuruluma ihtiyaç duymadan internetin bağlı olduğu bir konumdan bu hizmetten faydalanabilirler. PaaS ile kullanıcılar kendi ihtiyaçlarını karşılayacak uygulamalar geliştirebilir ve kullanabilecekleri bir platforma dönüştürebilirler. IaaS ise müşterilerin ihtiyaçlarına göre depolama, işlemci, fiber optik ağ kaynaklarının temini servis sağlayıcıları tarafından sağlanmaktadır. Yine bu servis modelinde de kullanıcılar kendi uygulama ve yazılımlarını kurabilmektedirler. Aşağıda ki tabloda servis modellerindeki kullanımı olan teknolojiler yer almaktadır (Şekil 2.5 Bilişim Servis Modellerinde Kullanılan Servisler.

Tablo 2.1: Bilişim Servis Modellerinde Kullanılan Servisler

SERVİS TÜRÜ	Servis Olarak Altyapı (IaaS)	Servis Olarak Platform (SaaP)	Servis Olarak Yazılım (SaaS)
Servis Kategorisi	Sanal Makine (VM) Kiralama, Online Depolama	Online Veri Tabanı, Online İşlem Ortamı, Online Mesaj Sıralama	Uygulama ve Yazılım Kiralama
Servis Özelleştirme	Sunucu Modeli	Yerel Kaynak Modeli	Uygulama Modeli
Servis Sağlama	Otomasyon	Otomasyon	Otomasyon
Servis Erişim Katmanı	Uzaktan Kontrol, Web 2.0	Online Gelişme ve Hata Ayıklama, Çevrimdışı Geliştirme Araçları ve Bulutun Entegrasyonu	Web 2.0
Servis Görüntüleme	Fiziksel Kaynak Görüntüleme	Yerel Kaynak Görüntüleme	Uygulama Görüntüleme
Servis Seviyesi Yönetimi	Fiziksel Kaynakların Dinamik Orkestrasyonu	Yerel Kaynakların Dinamik Orkestrasyon	Uygulamaların Dinamik Orkestrasyon
Servis Kaynak Optimizasyonu	Ağ Sanallaştırma Sunucu Sanallaştırma	Büyük Ölçekli Dağıtılmış Dosya Sistemi, Veri Tabanı Özel Yazılımı	Çoklu Kullanım
Servis Ölçümü	Fiziksel Kaynak Ölçümü	Yerel Kaynak Kullanım Ölçümü	İş Kaynak Kullanım Ölçümü
Servis Entegrasyon ve Kombinasyonu	Yük Dengesi	Servis Odaklı Mimari	Servis Odaklı Mimari
Servis Güvenliği	Depolama Şifreleme ve İzolasyon, Sanal Makine İzolasyon, VLAN, SSL/SSH	Veri İzolasyonu, İşletim Ortamı İzolasyonu, SSL	Veri İzolasyonu, İşletim Ortamı İzolasyonu, SSL, Web Kimlik Doğrulama ve Yetkilendirme

2.3.1. Servis Olarak Yazılım (SaaS)

Bu yapı bulut bilişim altyapısı üzerinde çalışan uygulama, yazılım ve servislerin kullanıcılara sunulmasıdır. Bunlara internet tarayıcısı gibi programlar aracılığı ile ulaşılması mümkündür. Sadece kullanıcılara kendilerine sınırlı yetki ve haklat tanımlanır örneğin; sunucu, ağ, depolama, işletim sistemi gibi uygulama ve yazılımlara erişme ve yönetme yetkisi yoktur. SaaS, BBHS merkezi bir yazılımın birden fazla kullanıcı tarafından aynı zamanlı kullanımına olanak sağlar. Kullanıcıların fazladan lisans almalarına gerek kalmadan tek lisansla birden çok kullanıcının ihtiyaçlarına göre yararlanmaları büyük bir maddi yükten kurtarmıştır.

Servis olarak yazılım hizmeti çok büyük bir kavramdır. Bulut bilişim hizmetlerinde servis olarak yazılımlara örnek (Thinkfree, Google Docs), elektronik posta uygulamalarına örnek (Google, Google, yahoo, Outlook, İcloud) verebiliriz. Bu hizmetlerin kullanıcılara fiyatlandırmaları değişiklik gösterebilir) .

2.3.2. Servis Olarak Platform (PaaS)

Bu hizmet modelinde, bulut sağlayıcıları genellikle işletim sistemleri, programlama dili yürütme ortamı, veri tabanı ve web sunucularını içeren bir bilgi işleme platformu dağıtmaktadır (Bulut bilişim- Wikipedia). Kullanıcılar sadece üzerinde barındırdıkları yazılım ve uygulamaların ayarlarını yönetebileceklerdir. Servis olarak platformu örneklendirsek; Microsoft Azure, Google App Engine, Heroku, IBM Bluemix ve Amazon Elastic Beanstalk olarak sıralayabiliriz.

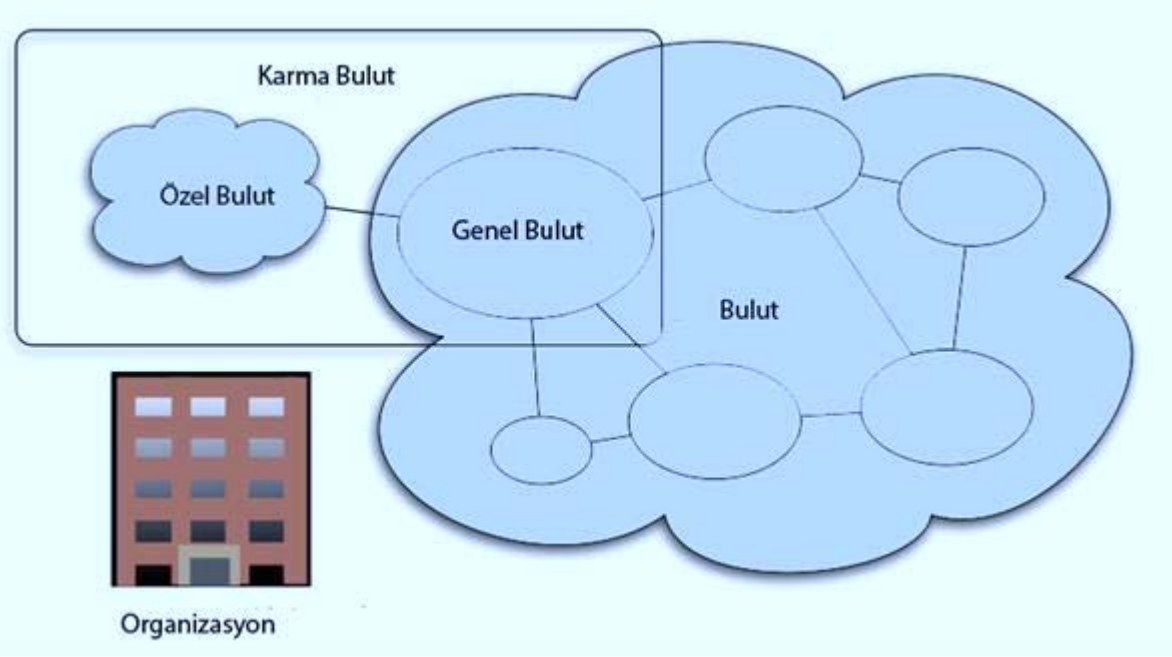
2.3.3. Servis Olarak Altyapı (IaaS)

Genel anlamda BT iş ve işlemlerinin hızlıca sağladığı avantajları sağlamasıdır. Burada kullanıcılar işletim sistemi, uygulamalar ve kendilerine özgü yazılımlar çalıştırabilirler. Ancak kullanıcılar temelde bulut alt yapısını kullanamazlar sadece işletim sistemlerini, depolama birimlerini platform üzerindeki kontrolleri ve güvenlik duvarları gibi kısıtlı ağ bileşenleri üzerinde de kısıtlı bir kontrol mekanizmasının olabileceği belirtilmektedir [30]. Dolayısı ile bu hizmet modelinde kullanıcılara fiziksel donanım olarak sunucu-depolama alanı- veritabanı gibi olanaklar sunulmaktadır. En bilinen IaaS örneklerinin önünde olan Amazon şirketler grubunun

EC2 yapısıdır. Amazon şirketler grubunun sunucular ihtiyaçları içinde Amazon – Wen altyapısı, Vmware Esx altyapısı, Microsoft Hyper –V altyapısı ile bu hizmetlerin devamlılığının sağlandığı bilinmektedir.

2.4. BULUT BİLİŞİM KONUMLANDIRMA MODELLERİ

NIST (2011)'e göre yapılan tanımlamada, bulut hizmeti alıcıları 4 farklı hizmet modelinde hizmet verebilmektedir. Sırasıyla; genel bulut (Public Cloud), özel bulut(private cloud), karma bulut (Hybird cloud), topluluk bulutu (community cloud) (Şekil 2.6).



Şekil 2.6: Bulut bilişimin yerleştirme çeşitleri

2.4.1. Özel Bulut (Provite Cloud)

Bu hizmet türünde verilen bilişim hizmetleri sadece bir kurum veya kuruş için verilmektedir. Kendi yerinde olabileceği gibi farklı bir konumda da olabilir. Kurum kendisi hizmetleri yönetebileceği gibi üçüncü taraflardan da yazılım ya da yönetim desteği alabilir. Bu şekilde özel bulut oramı güvenlik duvarları arkasında daha korunaklı olabilir. Bulut bilişim mimarisinin avantajlarından faydalanmak için kurum ve kuruluşlar için özel oluşturulmuş yapılardır.

2.4.2. Topluluk Bulutu (Comminty Cloud)

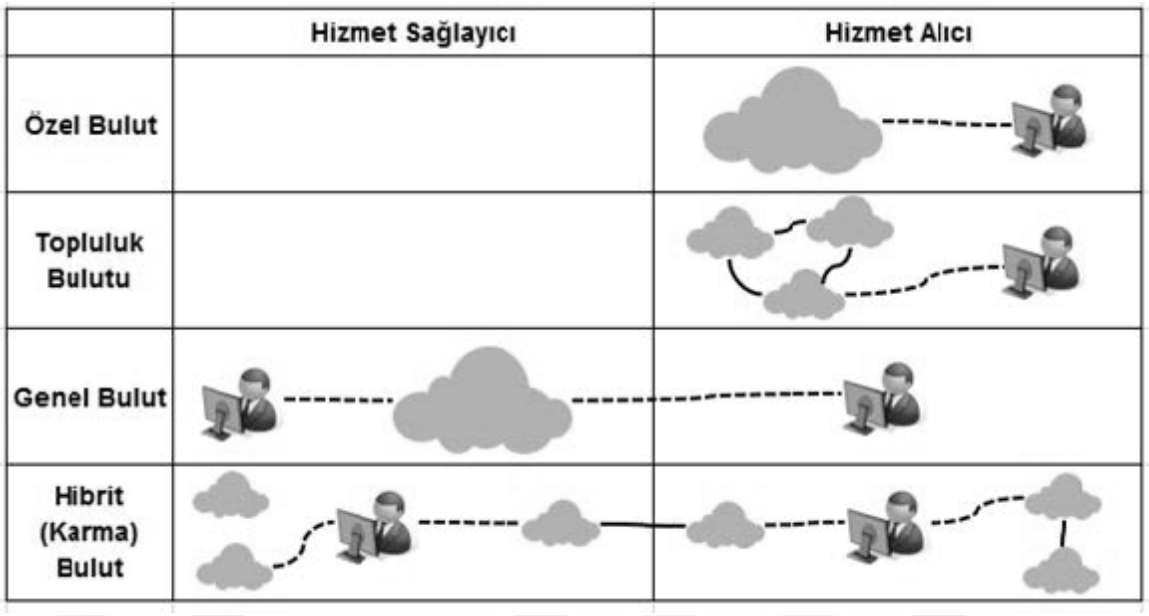
Bulut bilişim teknolojisi ver olan bir yapıyı maksimum fayda sağlayacak şekilde paylaşmaya yönelik bir yapı olmasında dolayı Topluluk Bulutu genel anlamıyla bunu sağlamaktadır. Kurum ve kuruluşlar aynı alt yapı hizmetini paylaşırlar. Kendilerini özgün olacak şekilde bulut toplulukları yaparlar. NIST'in (NIST, 2011)'de yaptığı tanımada; yaptıkları iş, güvenlik ihtiyaçları gibi ortak özellikleri olan kurum ve kuruluşların aynı bulut altyapısını kullanarak bir topluluk bulutu oluşturmasıdır. Bulut alt yapısını beraber paylaştıkları için kurum ve kuruluşların misyon, güvenlik gereksinimleri, şirket politikaları ve uyumluluk konuları gibi bazı endişeleri olabilir [20].

2.4.3. Genel Bulut (Public Cloud)

İnternet ortamında herkesin kolayca erişebileceği bir bulut yapısıdır. Kullanılan bulut altyapıları kurum ve kuruluş, akademik ya da devlet sahipliğinde ve yönetiminde bir alt yapı olabilir. Bu bulut türü genel olarak kişisel yani bireysel kullanımlarda (ticari vasıf taşımayan) örneklerden oluşur. Bu bilişim türünde ki örneklere en çok Microsoft ve Google uygulamaları ile karşılaşılabiliyor. Ücretlendirme yöntemlerinde farklılıklar vardır. Kullandığın kadar öde ya da ödediğin kadar kullanama hakkı gibi kalaylıklar sağlamaktadır.

2.4.4. Melez Bulut (Hybird Cloud)

Melez ya da karma bulut sistemi, adından da anlaşılacağı üzere 2 yada daha fazla bulut türünün (özel bulut, topluluk bulut, genel bulut) bir arada kullanılmasıdır. Global ağ (internet) olmadan yerel ağlardan (local) bağlanma olanağı sağlar. İnternet kullanımına ihtiyaç duymaz. Melez bulut sisteminde kullanılan uygulama ve yazılımları güvenilir, kolay erişilebilir, ve esnek olmalıdır. Kısacası işletmelerin aşırı ve büyük yoğunluktaki iş ve işlemlerinde genel bulutu kullanabilmeleri, normal işleyişlerine döndüklerinde ise özel bulut sistemlerini kullanabilmelerine olanak sağlamaktadır. Karma bulutta güvenlik özel buluta nazaran daha pasiftir. Güvenlik derecesi yüksek olan verilerin özel bulutta tutulması, güvenlik ihtiyacının en az olduğu verilerin ise karma bulutta kullanılması uygundur.



Şekil 2.7: Bulut yerleştirme modellerinin hizmet sağlayıcı ile hizmet alıcı arasında konumlandırılması

2.5. BULUT BİLİŞİMİN AVANTAJLARI

Bulut bilişim kullanıcıların kolay ulaşılabilir, verilerin kullanılmaya hazır, bilgisayar kaynaklarının bütün kullanıcılar ve dahil olacak kullanıcılara da paylaşabilme potansiyeli olan bir ağ havuzu bağlantı modelidir. Bulut bilişim iş ve işletme maliyetlerinin düşürülmesi verimliliğin daha maksimize edilmesi gibi temel kavramların temeli şeklinde bir yapı modelidir. Ancak bunun yanında da verilerin gizliliği veri mülkiyetlerinin bulut bilişim hizmeti veren şirketlere geçmesi, yerel yada global internet kullanma zorunluluğunun olması, bağlantının yavaşlaması ve siber saldırılar üzerinde daha tam kontrol sağlanamaması gibi bir takım dezavantajları da bulunmaktadır.

2.5.1. Düşük Donanım Maliyeti

Uygulamalar kullanıcıların düdük donanımlarda ki bilgisayar ve iş makinalarında kullanılmasını hedeflemektedir. Bu sayede web uygulamalarının çalışması netbook gibi ufak çaplı bilgisayarlarda bile kayda değer sonuçlar elde edilebilir. Bu şekilde kullanıcıların iş ve işlerinin yönetmeleri için gerekli olan sabit disk, ram, işlemci gibi donanımlara gerek kalmamaktadır. Bu sayede bağımsız düşük maliyetli ve yüksek performans sağlamaktadır[4].

2.5.2. Düşük Yazılım Maliyeti

Kurum ve kuruluşlarda her ayrı bilgisayar için ayrı ayarı yazılım almaya ve ayrı paralar ödemeye gerek yoktur. Ayrıca tüm bilgisayarlara ayrı ayrı güncelleme ve bakım gibi zaman alan bir uygulamada söz konuşu değildir. Bulut üzerinde kurulan bir yazılımı tüm kullanıcılar tarafından herhangi ayrı bir ücret ödemeden kullanmak mümkündür. Bulut bilişim ortamında yazılım satın almak yerine yazılımı kiralamak daha mantıklı bir seçenek olarak önümüze çıkmaktadır. Tablo 2.2. de Normal BT altyapısı maliyetleri ile bulut bilişim teknolojileri maliyetlerinin karşılaştırılması [8] gösterilmiştir. Bu karşılaştırmada da görüldüğü üzere Normal BT alt yapısının kurum ve kuruluşlar üzerinde ki maliyet yükü bulut maliyet oranın 2 katına denk gelmektedir.

Tablo 2.2: Klasik BT altyapısı maliyetleri ile bulut bilişim teknolojileri maliyetlerinin karşılaştırılması

NORMAL BT ALT YAPISI MALİYETLERİ	YIL	Donanım	Yazılım (Lisans)	Yazılım (Bakım)	Sistem Bakımı	Veri Merkezi
	1. Yıl	100.000$	100.000$	-	200.000$	50.000$
	2. Yıl	-	-	20.000$	200.000$	50.000$
	3. Yıl	-	-	20.000$	200.000$	50.000$
	4. Yıl	-	-	20.000$	200.000$	50.000$
	5. Yıl	-	-	20.000$	200.000$	50.000$
	Toplam	100.000$	100.000$	80.000$	1.000.000$	250.000$
GENEL TOPLAM 1.530.000$						
BULUT BİLİŞİM TEKNOLOJİLERİ MALİYETLERİ	YIL	Donanım	Yazılım (Lisans)	Yazılım (Bakım)	Sistem Bakımı	Veri Merkezi
	1. Yıl	-	120.000$	-	-	-
	2. Yıl	-	120.000$	-	-	-
	3. Yıl	-	120.000$	-	-	-
	4. Yıl	-	120.000$	-	-	-
	5. Yıl	-	120.000$	-	-	-
	Toplam	-	600.000$	-	-	-
GENEL TOPLAM 600.000$						

2.5.3. Ölçeklenebilir Olma Özelliği

Normal BT uygulamaları kullanan yer ve kuruluşların kullanıma dayalı yoğunlukları devamlı farklılık göstermektedir. Zaman zaman iş yoğunluklarında işletmelerin yoğunluklarında dolayı alt yapı ve bilgisayar donanımlarına yatırım yapmaları gerekebilir. Dolayısı ile bu zaman aralıklarında yatırım yapmak şirketler için işlerin yoğun olmadığı zamanlar için atıl yatırım olacaktır. Ancak bu şekilde ki sorunları en iyi çözüme kavuşturan seçenek bulut bilişim olarak öne çıkmaktadır. Çünkü maksimum bir yapının minimum maliyetlerle kullanılmasını sunmaktadır. Bu şekilde bulut bilişim sistemleri normal BT altyapısını kullanan kullanıcılar için pozitif bir ölçeklenebilirlik sağlamaktadır.

2.5.4. Güncel Olma Özelliği

Servis sağlayıcı firmalar yazılım şirketlerini takip etmek zorundadırlar. Dolasıyla bu şekilde kurum ve kuruluşların takip etmelerine ve zaman kaybetmelerine gerek kalmadan ortadan kalkıyor. Ayrıca güncellemeler için teknik desteğe ya da artı bir ücret ödemeye gerekte kalmaz.

2.5.5 Sınırsız Depolama Olanağına Sahip Olma

Dünya gelişmekte ve üretilen verilerin boyutları da devamlı bir şekilde artmaktadır. Verilere istenilen yerden kolayca erişme gibi kolaylıklar ister. Kişisel bilgisayarların depolama alanlarının sınırlı ve küçük boyutlarda olması insanları farklı arayışlara sokmaktadır. Burada bulut bilişimin devreye girmektedir. Ekonomik yönden bulut bilişim kaynakları normal kaynaklardan daha ucuz olma gibi avantajlara sahiptir. Ayrıca verilerin herhangi bir sebepten dolayı bilinçli ya da bilinçsiz bir biçimde silinmesine karşıda önlem alınmıştır. Birden çok sunucu üzerinden hizmetler verildiğinden bir sunucunun çökmesi diğer bir sunucunun yerine cevap verebiliyor olmasıyla güvenlik önlemleri sağlanmış olmaktadır.

2.5.6. Veri Güvenliği

Bulut ortamında veriler birden çok sunucuda depolanır ve işlenir. Sunucular güvenlik sertifikaları ve güvenlik duvarlarıyla korunur. Ayrıca verilerin silinmesi gibi durumlarda geri

alma ve kurtarma gibi seçeneklerde mevcuttur. Sunucuların bozulması ya da işlevsiz kalması durumunda yedekleme sistemi gibi sistemlerle güvenceye alınmaktadır. Bu sayede veriler ne şekilde olursa olsun olası bir tahribat ya da saldırıda fiziksel bilgisayarlara oranla daha güvenliklidir.

2.5.7. Bakım Maliyetlerinin Olmayışı

Normal bir sunucunun ve bilgisayarın bakımı planlıdır ve bakım zamanlarında verilere ulaşmak veri işlemek zor bir durumdur. Ayrıca maliyetli bir iştir. Çünkü bakım yapacak kalifiyeli elemanlar ve donanımlar temin etmek zorunludur. Olası hatalı bakım onarım gibi işlemlerin geri dönüşü zordur. Burada bulut bilişim teknolojisi hizmetlerinde kullanıcıların böyle bir işle uğrasının önüne geçmektedirler. Bütün bakım ve onarımlarını servis sağlayıcıları kendileri yaptıklarından bununda önüne geçilmiş olmaktadır.

2.6. BULUT BİLİŞİMİN DEZAVANTAJLARI

Yukarıda avantajlarından bahsettiğimiz bulut bilişimin dezavantajları da ne yazık ki bulunmaktadır. Mevcut yazılım ve uygulamaların bulut altyapısına uyumsuzlukları, güvenlik ve gizlilik açıkları, kontrol mekanizmalarının sınırlı olması, bant genişliğinin maliyetlerinin fazla olması, güvenlik önlemlerinin bazen saldırılara karşı etkili olmayışı gibi durumları mevcuttur.

2.6.1. Mevcut Yapıların Bulut Ortamı Altyapısına Uyumsuzlukları

Yazılımlar ve uygulamalar kullanılacakları işletim sistemleri ve erişme protokolleri gibi yapılar düşünülerek tasarlanır ve kullanıma sunulurlar. Bulut alt yapılarında Microsoft Windows, Mac OS, Linux gibi uygulamaları desteklemeyebilir. Dolayısıyla bu altyapıları kullanan ve sunucularını bulut sistemine taşımak isteyen kurum ve kuruluşlar zorluk çekmektedirler. Yeniden bir yazılım ve uygulanabilirliği olan yapılar inşa etmek zorundadırlar.

2.6.2. Güvenlik ve Gizlilik Açıklarının Olması

İnternet ortamında kullanılıyor olması ve birden çok kurum ve kuruluşun verilerini barındırmasından dolayı kötü niyetli kişilerin iştahını kabartmakta ve saldırı ihtimalini öne çıkarmaktadır. Verilerin çalınması en büyük tehlike olarak görünür. Ayrıca bulut bilişim hizmeti veren şirketlerin verileri görme, yönetme yetkileri vardır.

2.6.3. Kontrol Mekanizmasının Sınırlı Olması

Kullanıcıların kontrolleri sınırlıdır. Veri ekle, veri sil, veri güncelle vb. Bulut hizmeti sağlayan firmalar sunucuların tamamının kontrolünü elinde bulundurmak zorundadırlar. Gerektiği yerde yedekleme bakım ve onarım yapmak sürekliliği sağlamak adına. Bunu yaparken bütün müşterilerinin kendilerine sunmuş oldukları kontrol mekanizmalarını kullanırlar. Kullanıcılar ise sadece belirli iş ve işlemleri yapabilmektedirler. Verileri silseler dâhil sistem yöneticileri verileri diğer sunuculardan çekme olanağına sahiptirler.

2.6.4. Bant Genişliği Maliyetlerinin Yüksek Olması

Bulut bilişiminde karşılaşılan en büyük sorunların başında bant genişliğinin maliyetli olmasıdır. Kullanıcılar bulut bilişim sistemlerine geçerken servis sağlayıcılarına ulaşmakta zorluklar çekerler. Büyük ölçekli verilere sahip olan şirketlerin yeterli bant genişliği olmadığı zamanlar datalarını taşımaları epeyce güç olabilir. Bu şekilde ki zaman kayıplarının önüne geçmesi için Amazon S3 servis sağlayıcısıyla bant genişliğini 5-18 Mbit olacak şekilde örnekleyebiliriz . Bu bant genişliğine göre 1 TB'lık veriyi kesintisiz bir şekilde 5,5 gün gibi bir sürede ancak transfer etmek mümkündür. Bu gibi sıkıntıların ve maliyetlerin önüne geçmek amacıyla verilerin HDD gibi yapılarla servislere gönderilmesi çözümleri meydana gelmiştir.

3. SANALLAŞTIRMA ve PLATFORMLARI

Sanallaştırma donanım ve işletim sistemlerinin üzerinde uygulama ve yazılımların çalıştırıldığı yazılım bölümüdür. Bilgisayar ve donanımlarının kullanıcılardan soyutlamasıdır. Soyutlamanın olabilmesi için kaynakların paylaşımı ya da birleştirme işlemlerinin yapılması gerekmektedir. Katmanların; Sanal Makine Denetleyicisi (Virtual Machine Monitor - VMM) ya da hipervizör (hypervisor) adıyla adlandırılmaktadır. Temelde bilgisayar sistemlerinin fiziksel olan kaynaklarını işletim sistemlerinden gizlemektedir. Bu sayede bir donanım üzerinde birden fazla işletim sistemi kullanılmasına izin vermektedir.

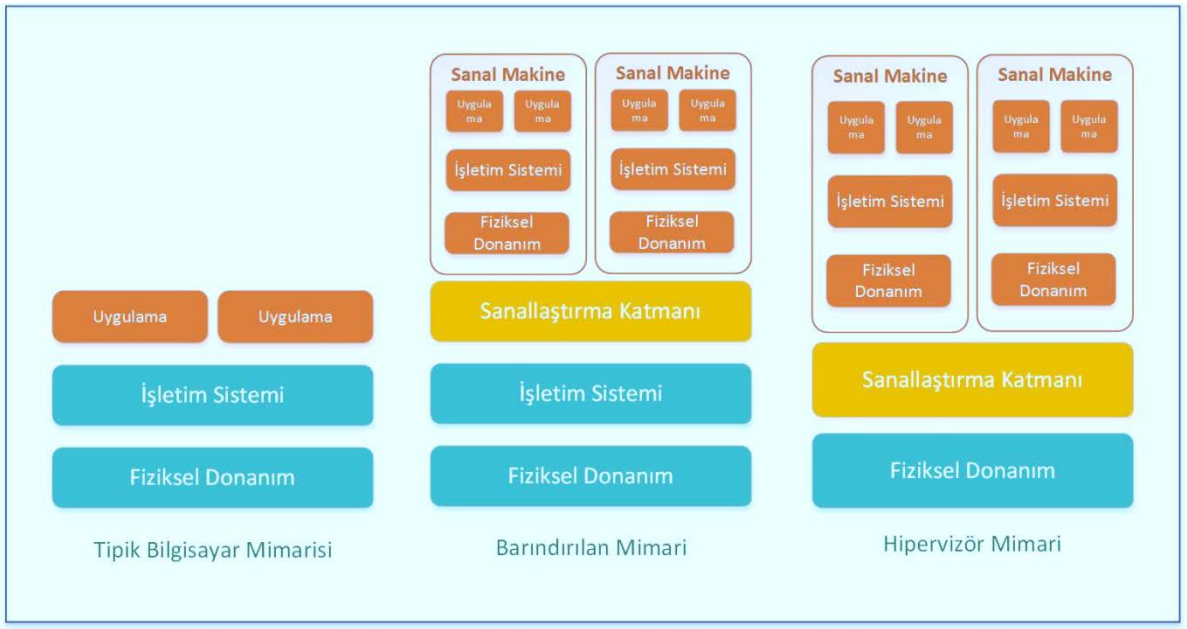
Sanallaştırma teknolojisi 1960'lı yılların başında günümüz IBM şirketler grubunun (MAİNFRAME) sistemlerinde "Zaman Paylaşımı" fikrini ortaya çıkardığı ve büyük ana çatı bilgisayarları birkaç mantıksal örneğe ayırması amacıyla geliştirdiği günden bu yana bilişim dünyasında yer almaktadır [5]. Sanallaştırma teknolojisi günümüze kadar gelişimini sürdürmüş ve bulut bilişimin vazgeçilemez haline gelmiştir. Depolama, işlemci, yazılım ve ağ servisleri vb. neredeyse tüm teknolojik oluşumlara uygulanmıştır. Temelde fiziksel bir bilgisayarı birden çok sanal kopyayla paylaşma mantığı taşır. CPU (işlemci), RAM (hafıza), HDD (depolama), WLAN-LAN vb.(ağ bağdaştırıcıları) gibi fiziksel olan araçları mantıksal bölümlere ayırarak her kullanıcıya mevcut gerçekte olan fizikselmiş gibi hizmet verebilecek şekilde kurguyla hizmet verir.

Bu teknolojide *Kaynak Paylaşımı* ve *İzolasyon* gibi iki kavram vardır. Kaynak Paylaşımı; Çalışan yazılım ve uygulamalar için host edilen hafıza, disk ve ağ cihazları gibi fiziksel olan kaynak yapılarının sanallaştırılmış makinalar aracılığı ile paylaşılmasıdır. İzolasyon ise fiziksel sunucular üzerinde birden fazla sanal makine kurgusunun birbirine karışmasını engeller ve sanal makinalar başka bir sanal makinayı göremezler.

3.1. SANALLAŞTIRMA (VİRTUALİZATİON)

Sanallaştırma teknolojisi fiziki sunucu ya da bilgisayar yapısının ortadan kalkıp, tek bir merkezden birden çok sunucunun kullanılabilir olmasını, yönetilmesi, maliyetlerin minimuma indirilmesini, yönetiminin tek elden yapılmasını, iş ve işlemlerin daha kısa sürmesi, bir sunucu üzerinde birden fazla işletim sisteminin kurgulanabilir olması gibi oldukça yaygın olan bir teknolojik yapıdır.

Sanallaştırma günümüzde hızlıca kullanılmaya ve gelişmeye devam etmektedir. Bulut bilişim sistemleri sanallaştırılacak diye bir olay söz konusu değildir. Ancak sanallaştırılmış bir bulut yapısı altyapı, kaynak, esneklik ve kolaylık gibi avantajları kullanıcılara sunar. Bourguiba M. Ve E1 Korbi I. Özellikle I/O performansında, paketlerin gönderilmesinde 10 kata kadar bir artış yaşandığını tecrübe etmişlerdir[6]. Sanallaştırma teknolojisi eğitim alanlarında da kullanılmaya başlanmış ve merkezlerinde bulunmayan fiziki sunucular ile laboratuvarlar sanallaştırma teknolojisi ile hayata geçmiştir[7]. Şekil 3.1.: Sıradan bir bilgisayar ile sanallaştırılmış bir yapının karşılaştırılması' şablonunda farklı mimarilerde ki yapılar karşılaştırılmıştır.



Şekil 3.1: Sıradan bir bilgisayar ile sanallaştırılmış bir yapının karşılaştırılması

3.1.1. Tam Sanallaştırma

Sanal makine denetleyicisi (VMM) olan host bilgisayarda kullanıcılar alanında işletim sistemleri üzerinde çalışır. Sanla makinalar (VMS) uygulama ve işletim sistemlerinin üzerinde sanal bir donanımla çalışır. Tam sanallaştırma işlemlerinde misafir iletim sistemlerinin herhangi bir değişiklik yapmaksızın çalışmasına izin verir. Giriş ve çıkış (I,O) aygıtları VMM'deki fiziksel aygıtları temsil eden sanal makinalar tahsis edilir ve sanal ortamdaki bu aygıtlarla etkileşimler iki yolla olur. Bunlar ya host ya da VM süsücüsüdür[16] ve fiziki donanımlara sevk edilirler.

Bu sanallaştırma yöntemi kullanıcılarına kolaylık sağlamak ve ortak bir yapıda diğer kullanıcılarla işletim sistemlerini her hangi bir yazılım gibi eklemeyi sağlar.

3.1.2. Donanım Sanallaştırma

Donanım sanallaştırma teknikleri, işletim sistemlerinin aksine, işletim sistemleri ile donanımları birbirinden ayırarak çalışan uygulamaları bağımsız bir yapıda çalışır olmalarına olanak sağlar. Her işletim sistemi başka bir veri merkezine taşınabilir ve veri kaybı oluşmaz[9].

3.1.3. İşletim Sistemi Sanallaştırma

İşletim sistemleri (Operating System- OS) sanallaştırılması işlemi yazılım ve uygulamaların taşınması, sistem güvenliği ve bakımı gibi avantajlar sunar. İşletim sistemlerinin sanallaştırılmasında uygulamalar aynı veri merkezini kullansalar bile diğer uygulamaların zarar görmemesi ya da karışıklığı engellemek adına izolasyon sağlamaktadır. Eğer kullanılan yazılımlar sistemlerde çalışmıyor ise taşındıkları diğer platformlarda da çalışmayacaklarıdır. İşletim sistemleri üzerinde çalışır durumda taşınması uygulamalardaki kesinti zamanlarını en aza indirir[8].

İşletim sistemleri sanallaştırılmasında üzerinde çalışan uygulamalar birbirine karışmaz ve tek başlarına sanal ortamlarda çalışırlar. Taşınma işlemlerinde bu büyük avantaj sağlamaktadır. Dolayısıyla taşınan uygulama ve yazılım karmaşaya sebep olmaz yeniden kurulum gibi işlemler gerektirmez. Bu sistemin esnekliğini gösterir.

3.1.4. Uygulama Sanallaştırma

Bu sanallaştırma tekniğinde bir uygulama kurulumu olmadan istemciler üzerinden çalışmasına izin vermedir. Herhangi bir kullanıcı grubu bilgi birimleriyle, bir uygulamayı kurabilme potansiyeline sahip olamayabilir. Bu durumda uygulama kurma karmaşası yaşamadan uygulamayı kullanabilme olanağı sunmaktadır. Bu sadece uygulamanın yürütülebilmesi için tasarlanmış küçük bir sanal yapıdır. Her bir kullanıcı izolasyon edilmiş bir ortamda iş ve işlerini yürütebilirler. Bu şekilde ki izolasyon ise uygulama, host ve işletim sistemleri arasında ki katman olarak görev görmektedir.

3.2. SANALLAŞTIRMA PLATFORMLARI

Sanallaştırma platformları donanım sanallaştırmasını sağlayan yazılım platformlarıdır. Tüm oluşturulan donanım parçaları yazılımlar sayesinde bir araya gelir ve burada havuz oluşturulup ihtiyaca göre paylaştırılır. İşletim sistemiyle kurulabileceği gibi işletim sistemi sonrasında da bu yapı oluşturulabilir.

3.2.1. Microsoft Hyper-V

İlk versiyonu Microsoft Viridian olan Hyper-V Server, Microsoft firması tarafından X64 mimariye sahip bilgisayarlar için sanallaştırma platformu olarak geliştirilmiştir. Windows tabanlı sunucular üzerinde kurulmaktadır[10]. Ancak şu an kullanıcılar Windows dışındaki işletim sistemlerini verimli bir şekilde kullanabilirler.

Hyper-V üzerinde, veri merkezleri kesintiye uğramadan taşınabilir. Veri merkezlerine ayrılan bir donanım yapısı esnek kullanılabilir. Herhangi bir veri ekleme ya da çıkarma yapmak sorun teşkil etmez. Hyper-V sanallaştırma yeteneği VLAN ağlarının yerine işlem görebilmektedir. Hyper-V 32 çekirdek işlemci özelliğine sahip bütün sistemleri yönetebilir, 1TB depolama birimine kadar kullanım olanağı sağlayabilir.

3.2.2. VMWare

VMWare şu anda pazarın lideri konumundadır. Günümüz masaüstü görünüme sahip neredeyse en ön sıralarda yer almaktadır. İşletim sistemleri üzerinde çalışmasına karşın ESX ve ESXI donanım üzerinde sanallaştırma teknolojilerinde de versiyonları kullanılmaktadır. Sanal makine oluşturmak ve yönetmeyi sağlayan tip-1 hipervizörüdür. Bireysel kullanımı ücretsiz sunulmakta olan VMWare sanallaştırma platformu x64 tabanlı mimaride kullanılabilmektedir. 64 mantıksal işlem çekirdeği 256 sanal işlemci ve host başına 1TB RAM miktarı ve yüksek birleşme (consadilation) oranı gibi özellikleri taşımaktadır[11].

3.2.3. Vitrualbox

İnnotek şirketi tarafından ortaya çıkan ve 2008 yılında Sun şirketler grubuna, 2010 yılı itibariyle de Oracle şirketi tarafından gelişimini sürdüren Vitrualbox kullanıcılar tarafından en çok tercih

edilen sanallaştırma platformudur. Windows, Linux, Machintosh ve Solaris gibi işletim sistemleriyle uyumlu olması, x86-x64 tabanlarını desteklemesi, uzak masaüstü bağlantı, kolay kullanım ve açık kaynak kodlu bir yazılım olmasından dolayı GNU General Public Licence Versiyon 2(GPLv2) lisanslarına da sahip olmasından dolayı rakiplerine fark atmıştır[12,13]. Host üstünde çoklu bir işletim sistemi barındırma işlemi yapılabilmektedir. Dolayısıyla misafir olarak adlandırılan geçici verilerin işlenmesi, durdurulması, yeniden devam ettirilmesi, anlık görüntü alınması vb. iş ve işlemler yazılım benzetim modunda ya da donanım destekli modlarda yapılabilir.

3.2.4. Xen

Xen, 2003 yılında Cambridge Üniversitesinde bir araştırma grubu tarafından geliştirilmiş yarı sanallaştırılmış tip-1 hipervizörüdür[14]. Şu anda Xen Server adı altında hem açık kaynaklı bir yapıyla gelişip hem de Citrix Firması bünyesinde faaliyet göstermektedir.

Bu sanallaştırma platformu ilk çıktığında sadece modifiye edilmiş Linux misafir sanal makinalarıyla çalışırken şimdilerde qumu işlemci emilatörünü kullanmaktadır[15]. Dolayısıyla Intel ve AMD işlemcileri destekliyor. Windows ve modifiye edilmiş Linux gibi işletim sistemlerini desteklemektedir. Xen bulut sanallaştırma platformunda sanal makinaların canlı taşıma işlemleri mümkün olmaktadır. Xen sisteminde tüm veri merkezlerine domain adı verilmektedir. Yönetim sahipleri Dom0 ile isimlendirilirken kullanıcılar ise DomUs olarak isimlendirilmektedir. Bulut bilişim ortamında sanallaştırma işlemleri için kullanılacak platform eğer Xen ise Dom0 ile alt yapı bağlantılarının yapılması gerekmektedir.

4. BULUT BİLİŞİM GÜVENLİK MEKANİZMALARI

Bulut bilişim kullanıcılarına ekonomik ve kolaylık gibi faktörlerde kolaylıklar sağlar ancak bu kolaylıkların yanında da güvenlik gibi sorunlar mevcuttur. Bu gibi sıkıntılardan dolayı kullanıcılar bu sistemin avantajlarından kaçınmayı tercih etmektedirler. D.Teneyuca'nın yaptığı bir araştırmada[17] bulut kullanıcı eksikliğinin %36'sı güvelik kaygısından kaynaklanmaktadır. Bulut bilişim servislerinin güvelik ile ilgili sorunlarına yaklaşımda iki temel konu üzerinde durulmaktadır. Birincisi servis sağlayıcılarının güvenirliği ve diğeri ise müşterilerin kullandığı servislerin güvenilirliğidir.

Bulut bilişim gelişmekte olan bir modeldir ve saldırganların iştahını kabartmaktadır. Buna karşı güvenlik mekanizmalarıda hızla gelişip artmaktadır. Veri merkezlerinde güvenliğin sağlanması ve yetkisiz kişilerin veri bankalarına ulaşması engellemek amacıyla ilk olarak kimlik doğrulama ve erişim kontrolleri gibi temel güvenlik prosedürleri geliştirilmiştir. Tehditlerin artışıyla birlikte kullanıcıların güvenlikleri de çeşitlenmeye başlamıştır. Güvenlik duvarları (firewall), güvenlik açığı tarayıcıları (vulnerability) ve saldırı tespit sistemleri de kullanılmaktadır[18]. Sistemlerin güvenlik önlemleri tek başlarına genellikle çözüm sağlamaz, hepsi farklı farklı bir mekanizmayı desteklediği için beraber kullanılması gerekmektedir.

Güvenli bulut bilişim için var olan farklı güvenlik mekanizmaları geliştirilmiş ve çeşitli yönetim modellerine odaklanılmıştır[19]. Bu modellemeler genellikle Saldırı Tespit Sistemleri, Güvenli Bilişim Sistemleri ve Veri Şifreleme Sistemleri gibi sistem modelleridir.

4.1. SALDIRI TESPİT SİSTEMİ

Bir kaynağın, verinin; güvenini, bütününü, gizliliğini veya erişimini kesme (engelleme) amaçlı bütün fiil ve oluşumlar saldırı (intrusion) olarak tanımlanmaktadır. Saldırı tespit sistemleri (Intrusion Detection System - IDS), bir veri tabanı ya da ağında meydana gelebilecek saldırı ve tespitleri otomatik izlenmesine olanak sağlayan, bilgisayar güvenlik mekanizmaları ve güvenlik politikalarına karşı oluşacak bütün saldırıları otomatik olarak yönetim birimlerine raporlayan yazılım ve donanım araçlarıdır[20]. Saldırı tespit sistemi özetle bir alarm sistemidir. Bir saldırı tespit sistemi birden çok sistemden (bileşenlerden) oluşmaktadır[21]. Algılayıcılar (Ajanlar), Monitörler, Merkezi Motorlar gibi sistemlerle saldırılara karışı önemler alınmaktadır.

Algılayıcılar: Güvenlik ilkelerini ve saldırı olaylarını gösterir.

Monitörler: Saldırı ve olayların algılanması, izlenmesi, kontrollerinin sağlanması gibi olguların kontrolü için kullanılmaktadır.

Merkezi Motorlar: Kayıtların tutulması ve uyarıların oluşumu için bu sistem kullanılmaktadır. Bu sistemde algılayıcılar tarafından belirlenen kayıtların işlenmesiyle oluşmaktadır.

Bir saldırı tespit sisteminde (IDS), oluşan bir saldırıya anında cevap verip korumaya yönelik bir önlem alınabiliyorsa eğer buna **aktif**, oluşan saldırıyı kayıt altına alıp daha sonra incelenmek üzere kayıt altına alınıyorsa **pasif** sistem olarak adlandırılmaktadır. Bir saldırı olayının tespiti tetikleme mekanizmalarının kullanımı ile anlaşılabilir. Saldırı tespit sistemleri ikiye ayrılır; Sunucu Tabanlı ve Ağ Tabanlı saldırı tespit sistemleridir.

4.1.1 Sunucu Tabanlı Saldırı Tespit Sistemi (HIDS)

Bu saldırıların hedefi dış kaynaklar olan ana çatı bilgisayarların [22] olduğu, ilk saldırıları tespit etmeye yarayan yazılımlardandır. Sunucu tabanlı saldırı sistemlerinde (HIDS) başka bir iş ve işlemde kullanılmayan bir bilgisayarda çalışır. Bilgisayar sistemlerinin kontrolünü sağlar ve gelen giden bağlantıları izleyip tespit oluşumu sonrasında 1 gibi değerle kullanıcılara uyarılar verir. Genel kullanılır bir saldırı tespit sistemi değildir. Önemli verilerin olduğu yapı gruplarının korunması amacıyla kullanılmaktadır. Belirli bir makinada oluşabilecek saldırılara karşı koymak amaçlı bir saldırı tespit sistemi olarak kullanılmaktadır. Bu sistemde işletim sistemlerinin de denetim ve log kayıtlarını almak mümkündür. Bu kadar avantajlı yapının oluşumunun yanında bir de hoş olmayan yönleri vardır. Her yapının yani sunucudan elde edilen verilerin ayrı ayrı işlenmesi gerekir. Sunucu tabanlı bir saldırı tespit sisteminin(HIDS) bu şekilde yönetimi de zordur. Bilgi kaynaklarının ve analiz motorlarının aynı yerde depolanıp işlenmesi gerektiğinden oluşabilecek saldırılara karşı denetimleri dikkat ve bilgi istemektedir. Bilgisayar ve sunucular üzerinde izleme yaparken de bir performans eksikliğine sebep olacağı da göz ardı edilmemelidir. Saldırı tespit sistemleri (IDS)'lerde olduğu gibi Sunucu Tabanlı Saldırı Tespit Sistemlerinde (HIDS) de güvenlik sistemleri vardır. Bunlar; Algılayıcı ve Ajanlar, Sunucular, Kullanıcı Makinaları, Uygulama Servisleridir.

4.1.2. Ağ Tabanlı Saldırı Tespit Sistemi (NIDS)

Ağ tabanlı saldırı tespit sistemleri, sunuculara saldırmak yerime ağın kendisini hedef alan saldırıları önleme amaçlı bir güvenlik sistemidir. NIDS ağ ve veri trafiğini görüntüler. Ağ trafiği ağ kartı geçirgen (promiscuous) modunda tüm veri trafiğini gözlemler ve inceleyip saldırı tespit sistemlerini kontrol edip inceler. Ağda dolaşan veri paketleri, hedeflenen yere ulaşabilmek için belirli noktalardan taranarak geçmek zorundalar. Analizler ve tehdit varlığı sorgulanır. Algılayıcılar üzerinde herhangi bir sorun olması durumunda hemen raporlanır ve kullanıcıların tedbir almasına olanak tanır. NIDS'lerde algılayıcı ile monitör arasındaki trafiğin şifreleme, algılayıcı ve monitörlerin ayrı ayrı ağlara dâhil edilmesi güvenliğin sağlanmasında önem arz etmektedir. Monitörlerin ve algılayıcıların farklı yerlerde olması Servis Reddi (Denial of Services - DoS) saldırılarından hasar görecekse kullanıcı minimuma indirger.

Ağ tabanlı saldırı tespit sistemleri (NIDS) ikiye ayrılmaktadır. Araç ve servis olarak karşımıza çıkmaktadır. İşletim sistemleri, uygulama ve programlamalar, ağ servis kartlarının tümünü araçlar içinde değerlendirilmektedir. Ağ yazılımları ve kullanıcılar tarafından kullanılan sitemlerden oluşmaktadır. NIDS fiziksel olarak bir mekanizma anlamında olmasa da birden fazla donanımları bünyesinde barındırdığı için fiziksel bir cihaz olabilmektedir.

4.2 GÜVENİLİR BİLİŞİM

Güvenilir bilişim (Trusted Computing - TC); Trusted Computing Group (TCG) tarafından geliştirilen ve desteklenen bir metodolojidir[22]. Yazılım ve donanımların iyileştirilip, veri ve veritabanlarına izinsiz ve yetkisiz gerişlerin engellenmesi, kullanıcı güvenliğini çözmek için öneriler oluşturan bir kavramdır. Bilişim sistemlerini oluşturan sistemler uyumu olmak zorundadır. Bunlar gizlilik, bütünlük, erişebililirlik ve kurtarılabilirlik ilkelerine dayanarak güvene dayalı bir yapı oluştururlar. Dünyanın en büyük donanım ve yazılım üreticileri bu yönde Trusted Computing (TCG) ile iş birliği yapmaktadır [22]. Son kullanıcıların var olan haklarına saygı duyarak bunu ihlal etmeden, kötü niyetli saldırı ve kullanıcıların verilerin korunması için şirketlere özellikler sunmaktadır.

4.2.1 Trusted Platform Modül (TPM)

Verilerin korunması ve yetkisiz girişlerin, veri kayıplarının oluşmaması için TC yaklaşımının bir parçası sayılan Trusted Platform Module (TPM) hizmetleri kullanılmaktadır. TPM, anakart

üzerinde bir devredir. Sistem üzerinde ki yazılımlar tarafından iyi ya da kötü tanımlı olan komutların kontrolünü sağlar[23]. TPM, genellikle şifreleme işlemlerinden yararlanılarak güvenlikle ilgili var olan sınırlı iş ve işlemleri yapma için tasarlanmıştır. TPM içerisinde bulunan Platform Configuration Registers (PCRs) bilgi akışını depolar ve geçerli olan veri akışlarını doğrular. TC birçok teknoloji içermektedir; güvenilir, ön yükleme uzaktan doğrulama, mühürlü depolama.

Kullanıcılar uzaktan doğrulama modülü ile platformda ki yazılımların raporları alınabilmektedir. Bu raporlar TMP tarafından imzalı onaylı PCRs yapılandırma değerlerinin bir parçasıdır[24]. Bir bilgisayar yapısı TPM gibi bir yapıya sahipse, şifreleme anahtarları gibi anahtarlar oluşturabilirler ve bu anahtarların güvenli olabilmesi için yalnız TPM tarafından çözülebilecek şekilde şifreme yapmak mümkündür. Bu şifrelemelerde kaydırma ve bağlama gibi terimlerin kullanıldığı ve şifrelerin herhangi, bir sebeple başka birine gösteriminin engellendiği de unutulmamalıdır. Dolayısıyla TPM gibi bir doğrulama platformu güvenlik önlemleri için önem arz etmektedir.

5. BULUT BİLİŞİM SİSTEMLERİNDE GÜVENLİKTE MALZEME VE YÖNTEMLER

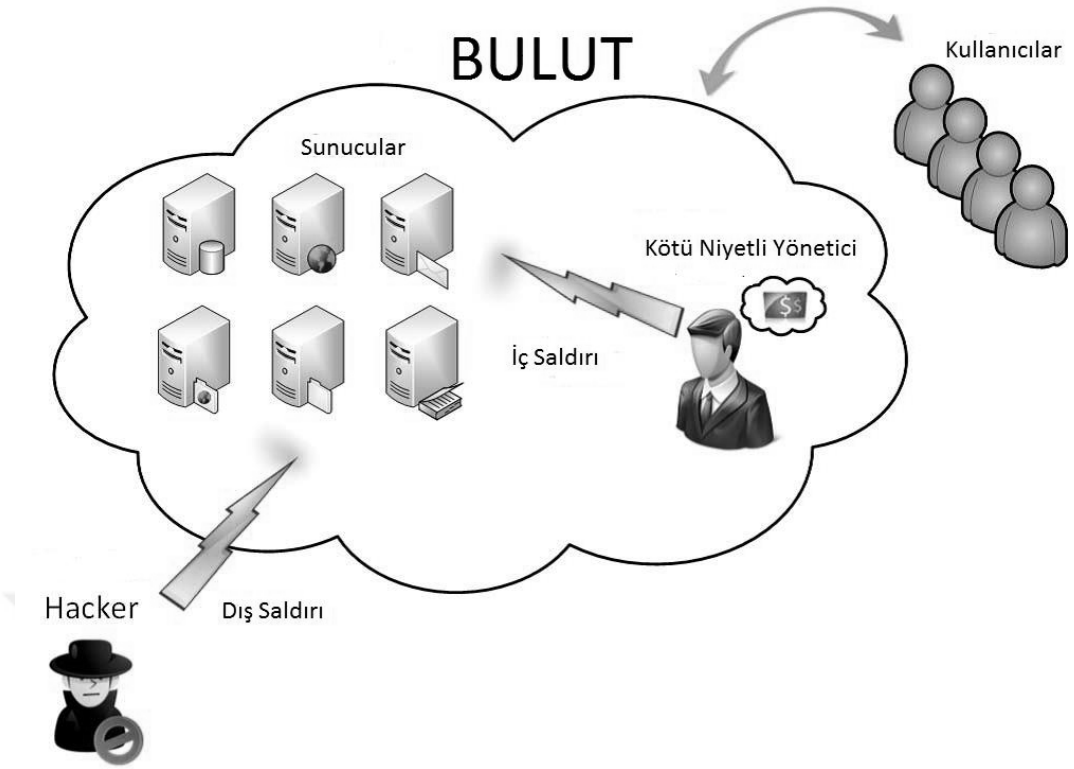
Dünya genelinde gelişmesini sürdüren bir bilişim yapısının elbette güvenlik malzemelerinin ve yöntemlerinin gelişmesi son derece doğal bir olaydır. Ancak günümüzde yapılan araştırmalar ve teknolojik gelişmelere paralel olarak teknoloji korsanlarının da saldırı araçlarında gelişmeler olmaktadır. Kullanıcıların veri güvenlikleri ve kişisel bilgilerinin gizliliğini %100 garanti bir şekilde sağlayan bir firma çıkmamaktadır. Buna paralel olarak yapılan yazılımlarında kullanıcılar açısından bir güvenlik sorunu taşıdığı açıkça görülmektedir. Bu sorunların en aza indirgenmesi amaçlı çalışmalar devem etmektedir. Kullanıcılar ve bulut hizmet sağlayıcıları için en önemli sorunların başında gelmektedir.

5.1. Bulut Bilişim Sistemlerinde Güvenlikte Genel Bilgiler

Bulut bilişim işletim sistemi, işlemci, depolama, ağ, uygulama, gibi bilgisayar kaynaklarının ve servis paylaşımını sağlayan dağıtık bir hesaplama yöntemidir[25]. Bu sistemlerin kabul görmesi ile birlikte askeri, finans ve kamusal alanlarda ki kullanımının yaygınlaşmasıyla olmuştur. Forbes [26] dergisinin yayımların bir araştırmasına göre 2014 yılında pazarlama departmanlarının %47'si iki yıl içerisinde uygulamalarının %60'şını bulut bilişim sistemleri platformlarına taşıyacaklardır. Veritabanları, e-posta, iş ve işlemlerin artık neredeyse yarısına yakını bu bulut bilişim yapısında yapılacaktır. Daha önce de bahsedildiği gibi bu sistemin güvenlik konusunda kullanıcılar temkinli davranmaktadırlar. Şirketlerde bu konuda çalışmalar yürütmektedirler

Bulut bilişim sistemlerinin sanallaştırma işlemleri önemli yet tutmaktadır. Servis Olarak Altyapı (IAAS), Servis Olarak Platform (PAAS),Servis Olarak Yazılım (SAAS) teknolojileri kullanıcıların kullanılabilirliğini ve bu yöndeki maliyetleri en aza indirmenin önemli yolarından biridir. En önemlisi de bulut kullanıcısı için güvenlik ve bulut hizmetini sunan kurum güvenliğidir.

Bulut bilişim dağınık bir yapıyla meydana gelir. Saldırganlar bir bütüne saldırmak yerine hedefte en çok hasar verebilecekleri konumları seçerler. Çalışmalarla sabit olmuştur ki; veri ve hak mahremiyetlerin garanti altına alınması için bu konumdaki kuruluşlara güvenmek zor bir konudur[27]. Bulut bilişimde iç ve dış saldırılar olmak üzere ikiye ayrılırlar(Şekil 5.1 [28]).



Şekil 5.1: Bulut bilişim saldırı türleri İç ve Dış Saldırılar [28].

Yukarıda ki şekilde de görüldüğü gibi bulut bilişimde genellikle iki tür saldırı planlaması yapılmaktadır. *Dış Saldırılarda*; tüm sanal platformları yönetme ve görme yetkisine sahip domain(Dom0) bulut dışında ki bir saldırgan işletim sistemleri olduğundan dolayı Dom0'ra saldırabilir ve başarılı olması durumunda da zarar verebilir, yönetebilir ya da sanal ortamdaki Veri Merkezlerini çökertebilir. Bu gibi saldırılara dış saldırılar denir. Bir sunucuya yapılan saldırırlar da kaba kuvvet(brüte force), port tarama, UDP/TCP saldırısı, SQL sızmalar olarak göze çarpmaktadır[25]. *İç Saldırılarda;* bulut hizmeti sağlayıcıları ya da kullanıcılar her zaman güveni bozacak çıkarları doğrultusunda verilerinize erişmek isteyebilirler. Bu saldırganlar içerdedirler ve amaçları doğrultusunda gizli kalması gereken bilgilerin çalınmasında rol oynayabilirler. Kullanıcıların izni olmadan sanal olan sunucular fiziksel sunuculara bağlanması gibi riski durumlar bunlara örnek olarak gösterilebilir.

Güvenlik mekanizmalarının önemi, kullanıcıların sistemlerini devamlı izlemesiyle daha üst seviyelere çıkmaktadır. Bu gibi durumları için sistemlerde en iyisi IDS kullanılması tercih edilmektedir. IDS çalışma prensibi var olan sistem saldırılarını ya da zararlı faaliyetleri tanımlamaya yönelik çalışmasıdır. IDS tabanlı bir karma (hibrit) mantığı sunan

AndroitVM[23] iyileştirme modelleri ve yapıları ekleyen U.Oktay ve Arkadaşları[28] tarafından Döngüsel Zincir Veri Merkezi Koruma Modeli ile beraber testler yapmışlar ve kullanıcıların durumlarını karşılaştırmışlardır. Bu modelde gizlilik bulut sağlayıcısına ve yöneticilerine bırakılmaksızın, kullanıcılar kendi gizlilik ayarlarını kendileri yapabilmektedirler. Bu modelde temel hedef zincir halkası gibi tüm VM'leri birbirini denetleme mekanizmasına bürünerek iş ve işlemleri daha faydalı hale getirmeyi hedeflemiştir.

Bu çalışmada güvenli bulut bilişimin gelişini ve veri güvenliğini sağlamaya yönelik veri merkezleri ve kullanıcıların sürdürülebilir bir yapıyı ele almaktır. Microsoft Azure ile yapacağımız örnek bir uygulama üzerinden verilerin kullanımı, güvenliği, erişilebilirliği ve avantajları ile dezavantajlarını karşılaştırması yapılacaktır.

5.2. BU YÖNDE YAPILAN BİLİMSEL ÇALIŞMALAR

Kullanılan veri merkezlerinin korunması ve koruma sağlaması gibi konularda bilimsel çalışmalar günümüzde de devam etmektedir. Bilgi üzerine kurgulanmış bütün yapılar gelecek için önemlidir ve korunmaya değerdir. Böyle bir yapı olunca gizlilik ile ilgili bir kurgu için sorumluluk bulut sağlayıcısının ve yöneticilerinin eline bırakılmadan kullanıcılara gizliliklerini yönetebilecekleri adımlar oluşturulmuştur. Döngüsel Zincir Veri Koruma Modeli, AndjoidVM modelinin daha işlevsel olmasını amaçlar[28].

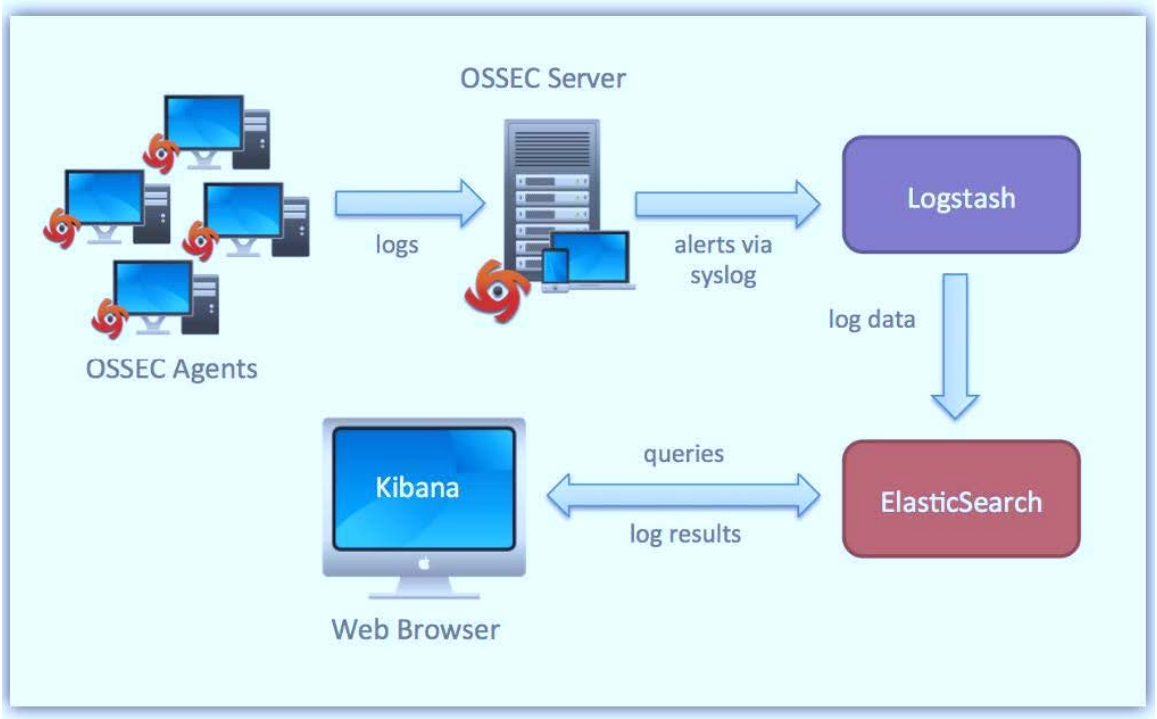
5.2.1. AndjoidVM – Döngüsel ZincirVM – MeshVM Koruma Modelleri

J.Kong[24], güvenli olmayan bulut sağlayıcılarına IDS mekanizması oluşturmuştur. Temel amaç güvenilir olmayan sunucuların veri akışlarını önlemek. IDS mekanizması geliştirerek bunun önüne geçebileceğini ve sanal ağlar üzerinden gelecek tehditlere karşı veya gerçek ağlar üzerinde oluşacak saldırı düzeneklerine karşı sanal makine izleyicisi (Virtual Machine Monitor - VMM) ile karşılık vermeyi amaçlar. Bunun temelde amacı karma saldırılara karşı koruma mimarisi geliştirmek olmuştur.

İlk olarak ele alacağımız model AndjoidDM koruma modelidir. Bu model açık kaynak kodlu bir yapıya sahip olan sanallaştırma ortamı olan Xen Hypervisor platformunu kullanmaktadır. HİpervizÖr, Dom0, DomU olarak üçe ayrılmaktadır. Hipervizör verimerkezleri için sanallaştırmada donanım soyutlaştırma ve paylaştırma gibi yöneten modüllerdir. Dom0 ve DomU ise veri merkezlerinin yönetiminde ve sanallaştırma araçlarını da içinde barındıran,

sanallaştırma özelliklerini sunan yönetim uygulamalarıdır. Bu sayede sanallaştırma ve teknolojik kolaylıklar insanlar için daha duruma gelmektedir. Sanallaştırma da Trusted Grup[24] güvenli ön yükleme aracı olarak kullanılır. Bu şekilde sistemler önyükleme yapma olanağına sahip olabilirler. I/O Memory Management Units (IOMMU) gibi yapıların sunduğu avantajlar ile atanmış olan bellek izolasyonu sağlanabilir[29]. Bu sistemin çalışmasından önce olaması gerek bir durumdur. Kullanımı basit ve mantıksal işleyişe ters düşmez. IOMMU sistemden önce çalışır vaziyette olmalıdır ki hipervizör IOMMU'yu kontrol edip ön yükleme işlemlerini durdursun.

AndjoidVM modelinde sistemin çalışma mantığı farklıdır. Her bir VM ayrı ayrı AndjoidVM tarafından izlenir ve koruma sağlanır. Bir veri merkezi kurumu sırasında Xen değier VM'lerinin adreslerini eşleştirir ve izleme takip etme kullanıcı sınırlama gibi VM bellek alanlarının takibini sağlar ve bunları farklı yollarla raporlar. VM güvenliğinin sağlanması için karma bir modelleme bir IDS yapısı yapılmış ve sunucu yapılı bir IDS olan Opearting System Securty (OSSEC) (Şekil 5.2.de[31] gösterilmiştir) ve HIDS ile işletim sistemlerini barındırıp takip eden Kernel Monitor Deamon (KMD) kullanımı sağlanmıştır. OSSEC Sunucu ile beraber çalışan Kibina[32] motoru; veri görselleştirme motorudur. ElasticSearch[33]'da ki anlamlı verileri sorgular ve görselleştirmek için kullanır[18]. Logstash[34] ise log kayıtlarının tutulması ve işlenmesi gibi işleri yapan bir açık kaynak kodlu sistemdir. Log kayıtlarının belirli sunucu ve istasyonlara göndererek bir web ara yüzü sayesinde kullanıcılara sunar. Şekil 5.2'de[31] gösterilmektedir.



Şekil 5.2: OSSEC Sunucu ile Logstash, ElasticSeach ve Kibina çalışma yapısı[31].

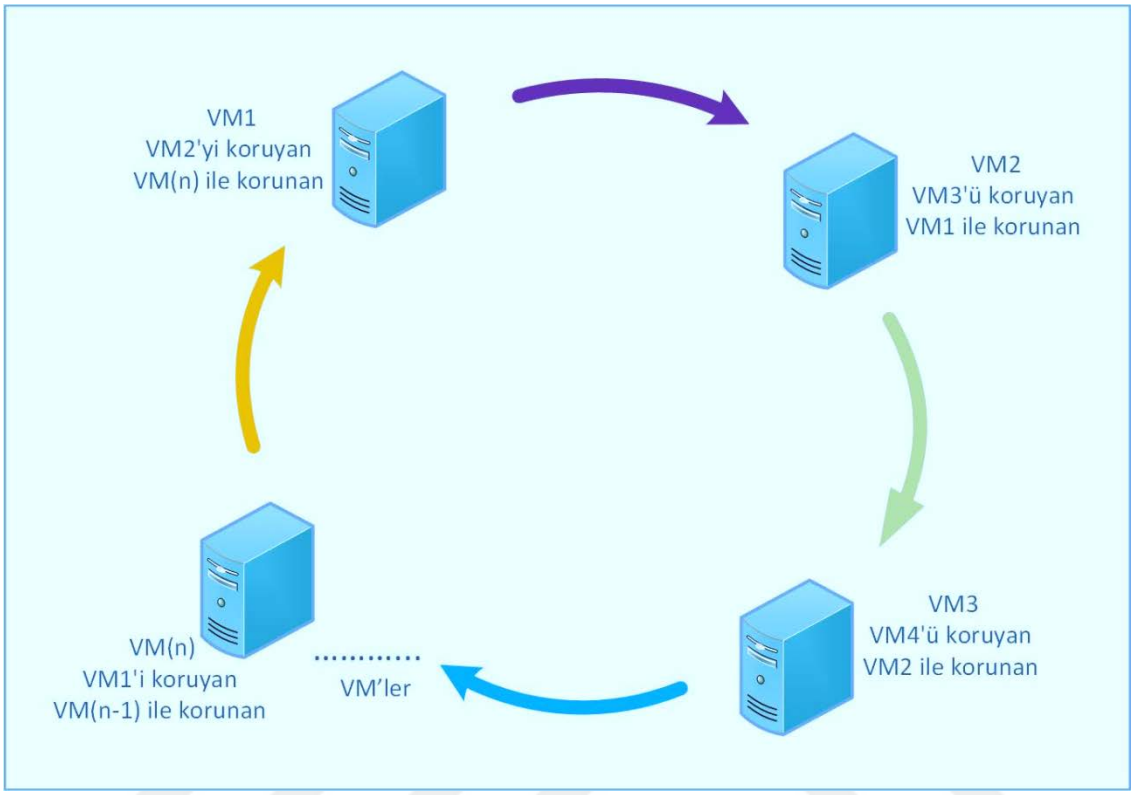
Saldırılara karşı işletim sistemi çekirdeği izleyicisi Karnel Monitör Deamon (KMD) kullanımı yapılması sunucu tabanlı bir saldırıya karşı önlemlerden biridir. Ayrıca bu şekilde bir yöntem ile arka planda çalışan bir rootkid varsa tanımlar. KMD güvenliğini sağlamayı amaçlayan VM çekirdeğini haritalandırır[18]. Güvenli veri merkezi başlangıç protokolünün kullanımı ile yerel ya da uzak bağlanımlara karşı bir duvar olma sabit ya da sanal disklere kullanıcı bilgisi dışında erişimin önüne geçmeyi sağlamıştır. AndjoidVM koruma modeli mimarisi Tablo 5.2'de[28] gösterilmektedir.

Tablo 5.1: AndjoidVM koruma modeli mimarisi tablosu[28].

<table>
<tr><th>Korunan VM</th><th colspan="2">AndjoidVM</th></tr>
<tr><td>Misafir Uygulamaları</td><td colspan="2">IDS Politika Motoru</td></tr>
<tr><td rowspan="2">OSSEC Ajanı</td><td rowspan="3">OSSEC Sunucusu</td><td>Karnel Monitörü Deamon (KMD)</td></tr>
<tr><td rowspan="2">Misafir Karnel Mapper</td></tr>
<tr><td>Misafir Kernel</td></tr>
<tr><td colspan="3">Hipervizör</td></tr>
</table>

Döngüsel ZincirVM Koruma Modeli ise, bir veri merkezi diğer başka bir veri merkezi izlemek ve korumak için oluşur. İzlenen veri merkezide başka bir veri merkezinin denetimini sağlamaya yönelik izleme gerçekleştirmektedir. Bu şekilde elde bulunan tüm veri merkezlerinin korunması hedeflenecektir. Bu şekilde AdjointVM koruma modelinde koruyan VM ve korunan VM'lerine eklemeler yaparak başka bir yapıda olan VM koruma, diğer bir VM oluşumunda izleme gibi bir zincir oluşumu sağlanmaktadır. Bu şekilde n adet bir VM koruması olanağı sağlanmış olmaktadır[28]. Bu modellemenin sağlanması için eklenen her bir VM bir öncekinin sorumluluğunu almak zorundadır. Örneğin yeni bir VM'nin n tabanlı bir VM'ne eklenmesi için VM1 sorumluluğunu alması gerekmektedir. VM1'i koruyan VM2 kontrolünü sağladığı VM'ni

dâhil edilen VMn olacak şekilde döngüye sokmak zorundadır. Bu kurgu bir VM'nin çıkması durumunda da aynı şekilde kurgulanmalıdır



Şekil 5.3: Döngüsel Zincir Veri Koruma Modeli[28].

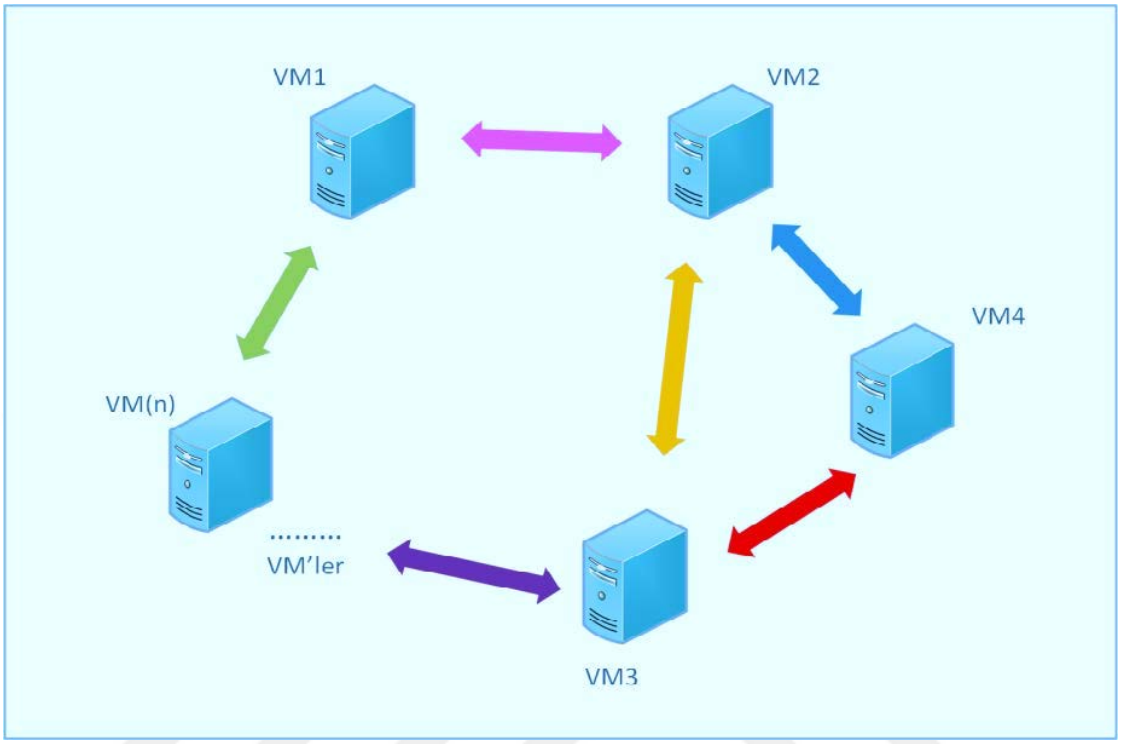
Bu modelleme örneğinde unutulmaması gerek durumlar vardır. İstemciler daima kontrol altında tutmak zorundadırlar VM'lerini. Her bir VM ekleme gibi bir olayda istemciler kar ve zararlarını yani VM güvenliği ile sanal ortam durumlarını ve izleyici durumlarının güçleşeceğinin hesaplarını yapması gerekmektedir. Bunların en önemlisi ne kadar VM dâhil edilirse o kadar sanal ortam harcaması artacak ve güvenliği sağlama duyusunda da azalmalar olacaktır. AdjointVM Koruma Modeli iyileştirmeler sonrasında kendi aralarında ki VM'lerinin güvenliğini sağlama konusunda daha iyi bir başarı sağlamış ve başka bir koruma modeli ihtiyacı olasılığını da minimize etmiştir.

Tablo 5.2: AndjoidVM ile İyileştirilmiş AndjoidVM kıyaslaması[28].

Özellikler	AndjoidVM	İyileştirmeden Sonra AndjoidVM
Zengin Bilgi	Evet	Evet
Düşük Yanlış-Pozitif Oranı	Evet	Evet
İstismar Direnci	Evet	Evet
Yapılandırılabilir Güvenlik Politikası	Evet	Evet
Saldırganlar İçin Görünmezlik	Hayır	Hayır
Kötü Niyetli Yönetici veya Sağlayıcıya Karşı Gizlilik	Hayır	Evet
Ölçeklendirme	Kolaydır	Daha Zordur
Koruyan VM'in Güvenliğinin Sağlanması	Hayır	Evet
n adet VM Güvenliği İçin Gereken VM sayısı	2n	n
Gider	Azaltır	Daha Azdır

MeshVM modelinde de Döngüsel Zincir Veri koruma modelinin güvenli bulut bilişim için daha etkili olabilmesi ve saldırılar karşısında kendine yetmesi için ortaya konmuş bir modeldir. Burada modelin var olan ve saldırılar karşısında eksikliği tesbit edilen açıkların iyileştirmelerle kapatılıp kapatılmayacağı amacıyla çıkmıştır. Döngüsel zincir koruma modelinde her bir VM diğer bir VM koruması sağlamaktadır. Ancak bir VM'nin çökmesi, saldırıya uğraması, fiziki bir aksaklığa maruz kalması vb. gibi sorunlarda korumakta olduğu VM korumasız kalacaktır ve bunun gibi sorunlar oluşması durumunda bile VM garanti altına alınmak zorundadır. Mesh yapısıyla zincir yapısından farklı olarak örgü şeklinde bir yapıyla durum kontrol altına alınması hedeflenmektedir. Bu şekilde bir yapının ağ üzerinde ki tüm sanal makinaların birbirlerini izlemleri mümkün olacaktır[28]. Ancak karmaşık yapısından ve daha yeni bir model

olmasından dolayı hem güvenlik risklerini barındırmaktadır hem de kurgulanmasının daha yüksek maliyetler çıkarmaktadır.



Şekil 5.4: MeshVM Modeli[28].

5.3. BULUT BİLİŞİMDE SALDIRILARDAN KORUNMAK İÇİN GELİŞTİRİLEN YÖNTEMLER

Bulut bilişimde kullanıcılar kendi verilerinin nasıl saklandığıyla ilgili kesin ve detaylı bir bilgi sahibi olmadıkları için servis sağlayıcılarına güvenmek zorundadırlar[30]. Sistemler düzeyli algoritmalar, biyometrik tabanlı yazılımlar, kimlik ve kullanıcı doğrulama mekanizmaları, erişim kontrolleri, veri şifreleme, verilerin güvenle aktarılması gibi yöntemlerle kontrol altına alınmaya çalışılır.

Saldırı Tespit Sistemleri(Intrusion Detection System-IDS) bir saldırının oluşumunun önlemlerinin alınmasına rağmen oluşabilecek saldırıların tespiti ve raporlanması gibi işlemleri yapar[35]. Saldırı Önleme Sistemleri(Intrusion Prevention Sysstem-IPS) IDS yapısının bir eklentisi şeklinde hizmet sağlar. IPS'ler IDS'lerde tespiti yapılan saldırılara karşı aktif önlemler

alarak saldırıyı önlemeye çalışır. Kullanılan VM'lerinde bu iki sistem birlikte çalıştırılırlar. Bunlara Saldırı Tespit ve Önleme Sistemi(Intrusion Detection and Prevention System-IDPS) olarak adlandırılırlar.

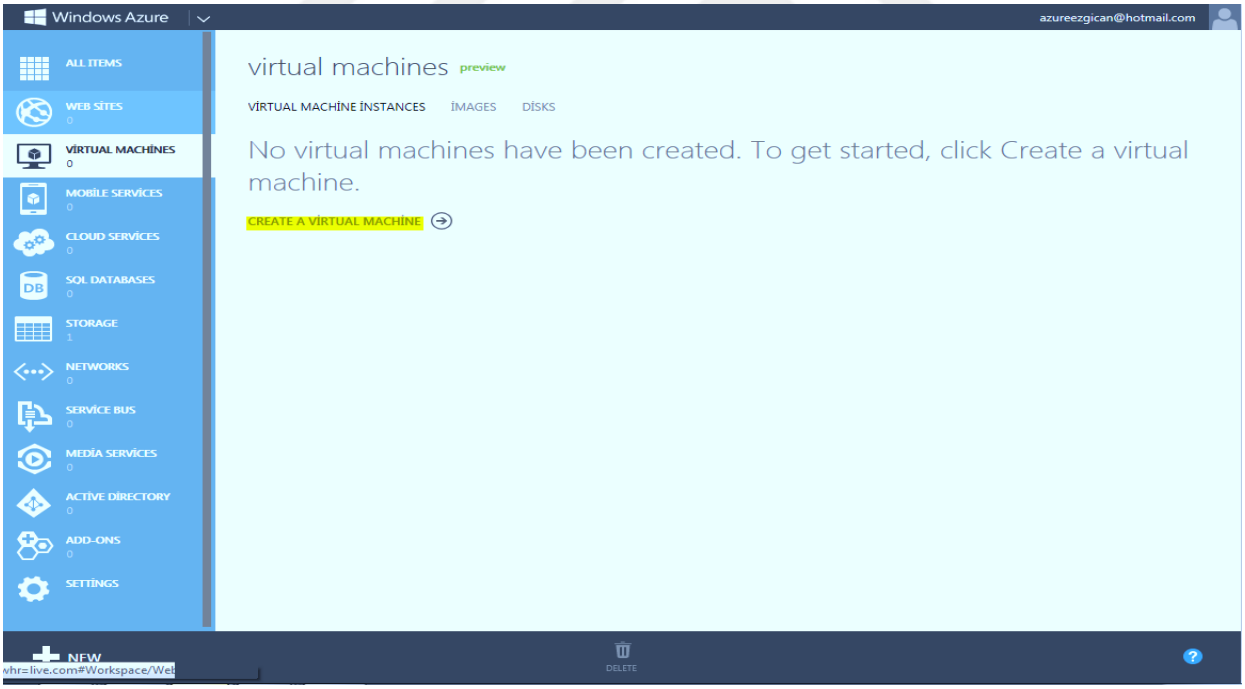
Bu tez çalışmasında Microsoft Azure ortamında örnek bir sanal makine oluşturup, var olan veri güvenlik mekanizmalarını incelenmesi hedeflenmiştir.

6. ÖRNEK SİMÜLASYON

Örnek simülasyon ortamında Windows Azure bulut sistemlerinde kişisel bir veri tabanı ve sanal sunucunun kurulumu ve bunun yanında Azure ortamında host edilecek kişisel bir web sitesi oluşturma yapılacaktır.

6.1.MİCROSOFT AZURE PLATFORMUNDA SANAL SUNUCU KURULUMU

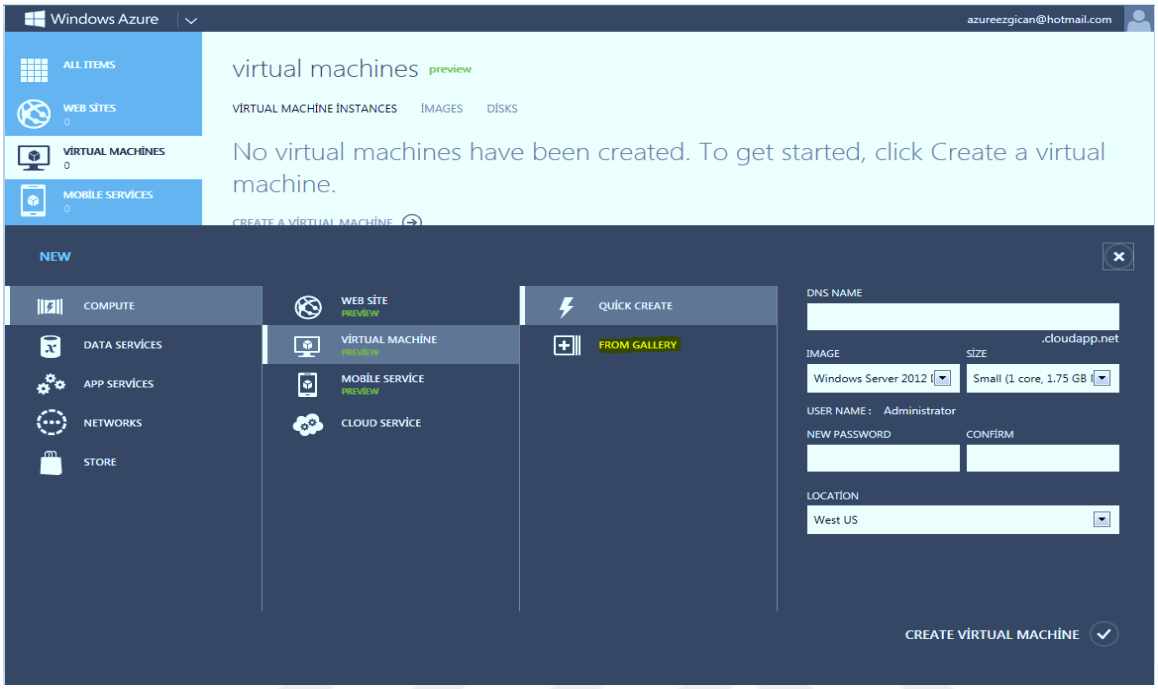
Adım 1: Windows Azure sanal sunucularının kurulum aşamaları yapılan son iyileştirmeler sonrasında günümüzde kullanım kolaylığı ve işlevselliği açısından ön plana çıkmaktadır. Kullanım ve kurulumunda https://signup.azure.com/ adresinden erişim yapılması gerekmektedir. Kayıt işlemlerinin gerçekleştirilmesinden sonra sanal makine oluşturma işlemleri için "Virtual Machines" başlığına oradan "Create a Virtual Machine" seçeneği ile devam edilir.



Şekil 6.1: Microsoft Azure Platformunda Sanal Sunucu Kurulumu

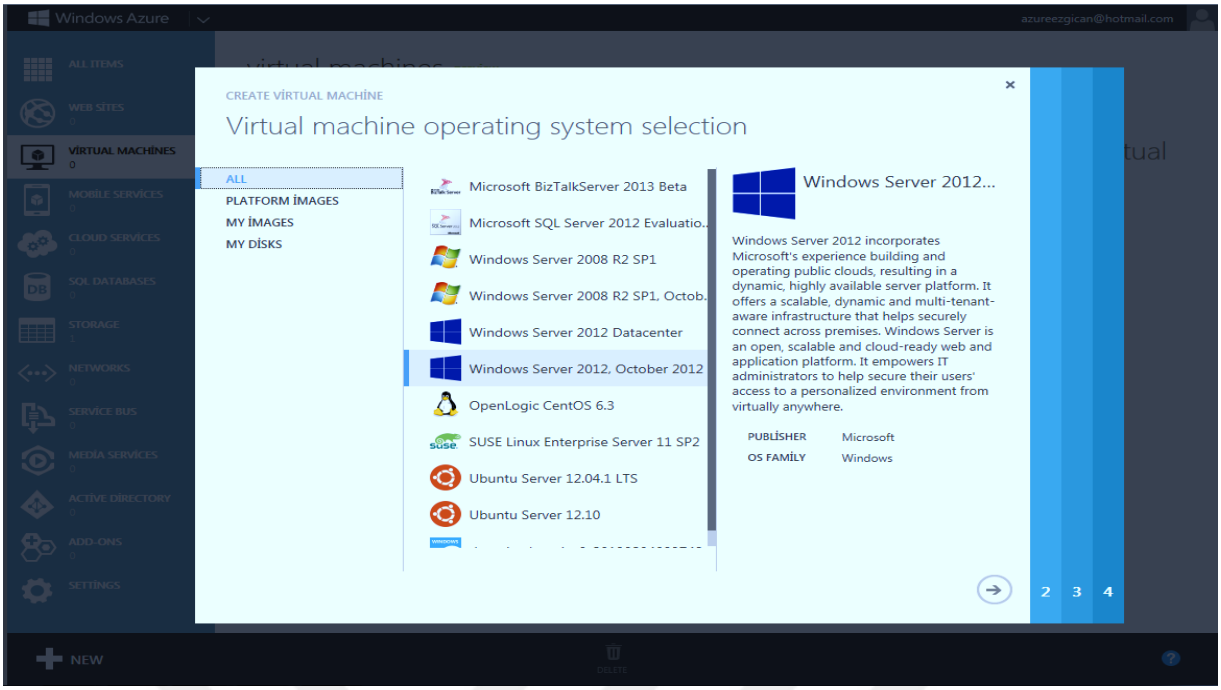
Adım 2: İlerleyen aşamada "Create a Virtual Machine" seçeneğinin işaretlenmiş olması ve bir sonra ki ekrana geçilir. Sol tarafta bulunan "Compute " ve "Virtual Machine" seçenekleri tıklandıktan sonra "Quick Create" ile "From Gallery" açılacaktır. Quick Create seçeneğinde sıfırdan bir imaj dosyasının oluşumu From Gallery seçeneğinde ise Microsoft Azure ortamında

var olan bir imaj üstünde işletim sisteminin kurulması seçeneklerinden birini tercih ederek devam edilir. Bu kısımda biz From Gallery seçeneği ile hazır bir işletim sistemi imajı oluşturacağız.



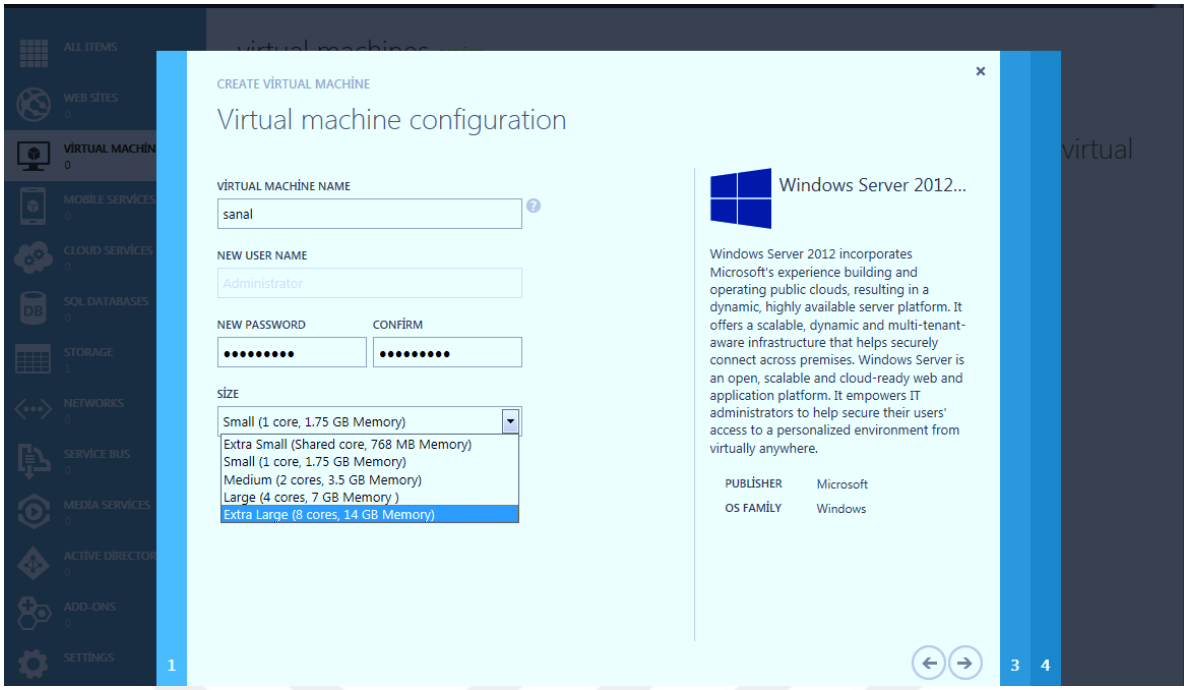
Şekil 6.2: Microsoft Azure Platformunda Sanal Sunucu Kurulumu

Adım 3: Yukarıda ki adımladan sonra önümüze gelen ekranda "Virtual Machine Operating Sysetem Selection" sanal sunucuya işletim sistemi kurulumu yapacağımız ekran gelecektir. Bu ekranda dünya üzerinde hatrı sayılır kullanıcı kitlesi tarafından kullanılan bütün işletim sistemlerinin olduğunu görmemiz mümkündür. Windows Server 2008 R2, Microsoft SQL Server 2012 Avaluation, Microsoft BizTalk Server 2013 Beta, Windows Server 2012 Datacenter, OpenLogic CentOs 6.3, Ubuntu Server 12.10 gibi çeşitli işletim sistemlerinin imajları yer almaktadır[36]. Burada kurulumunu yapacağımız işletim sistemi Windows Server 2012, October 2012 ile kurulum işlemlerimize devam edilir.



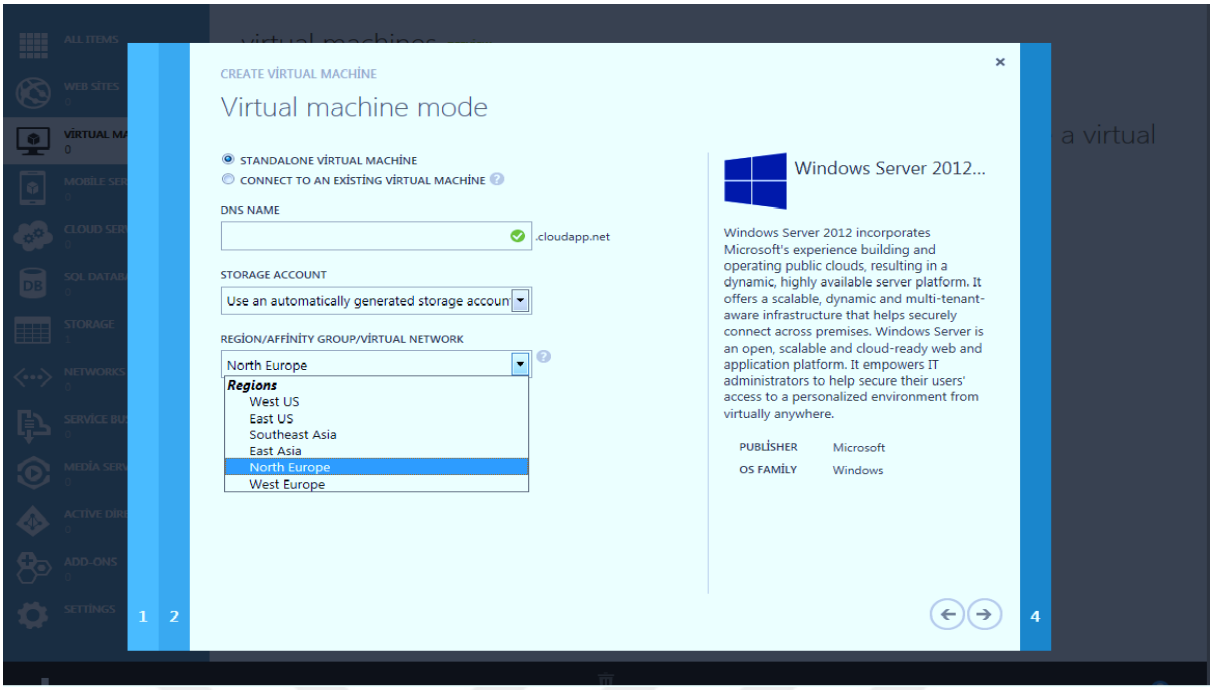
Şekil 6.3: Microsoft Azure Platformunda Sanal Sunucu Kurulumu

Adım 4: İlerleme sonrasında açılan pencere de "Virtual Machine Congfiguration" oluşturacak olan sanal makine için bazı tanımlamalar yapmak gerekmektedir. "VİRTUAL MACHİNE NAME" kısmına sanal makine adı "NEW USER NAME" kısmına ise kullanıcı hesabı olan Administrator olarak belirlenir. Ardından sırasıyla "NEW PASSWORD" şifre "CONFİRM" oluşturulan şifrenin tekrarı yazılır. "SİZE" yazan bölümde kullanıcının ihtiyaç duyduğu sanal sunucunun donanımsal bölümlerinden uygun olan seçilmesi gerekmektedir. Bu kısımda "Ekstra Small = Shared core, 768MB memory, Smal = 1 core, 1,75GB memory, Medium = 2 cores 3,5GB memory, Large = 4 cores 7GB memory Extra Large = 8 cores 14GB memory " seçenekleri mevcuttur. Bu kısımda biz "Extra Large" seçeneği ile kurulum işlemlerine davam ediyoruz.



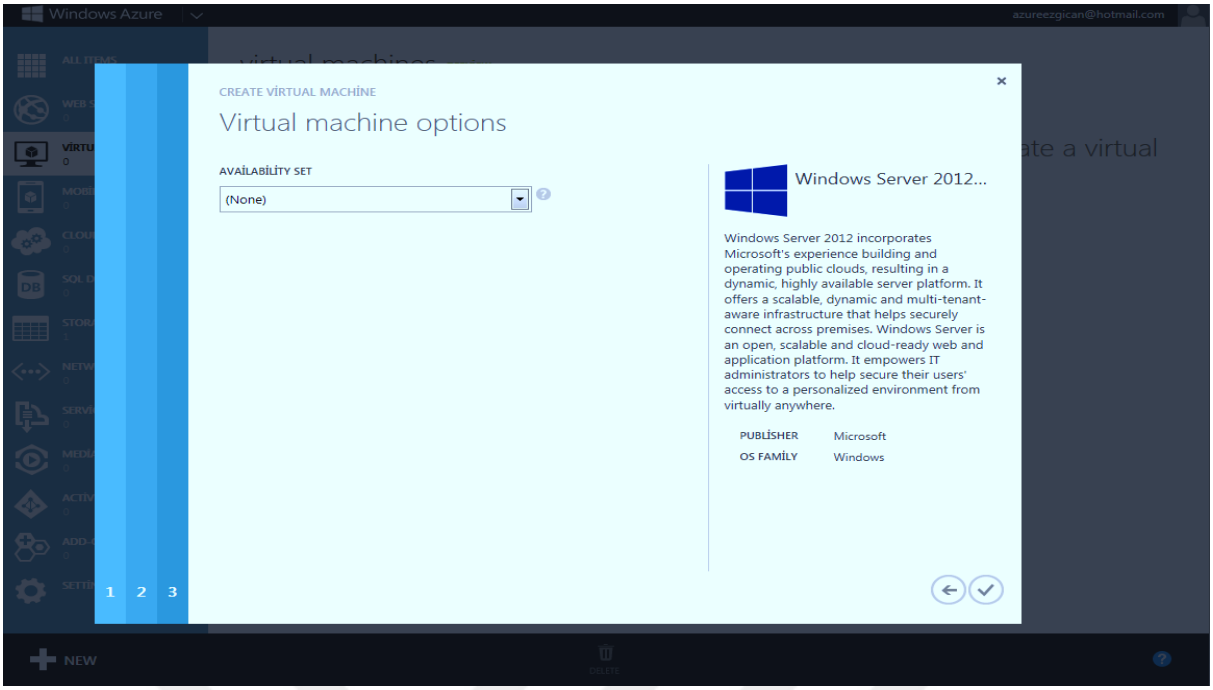
Şekil 6.4: Microsoft Azure Platformunda Sanal Sunucu Kurulumu

Adım 5: Bu aşamada “Virtual Machine Mode” ekranında sanal makine kurulumu yapılacaksa “Standalone Virtual Machine” seçeneği var olan bir sanal makineye bağlanılacaksa da “Connect To Existing Virtual Machine” seçenekleri seçilir. Bu ekranda ayrıca DNS ismi, Storage hesabı ve verilerin hangi bölgede saklanmasını gibi araçlarında belirlenmesi gerekmektedir.



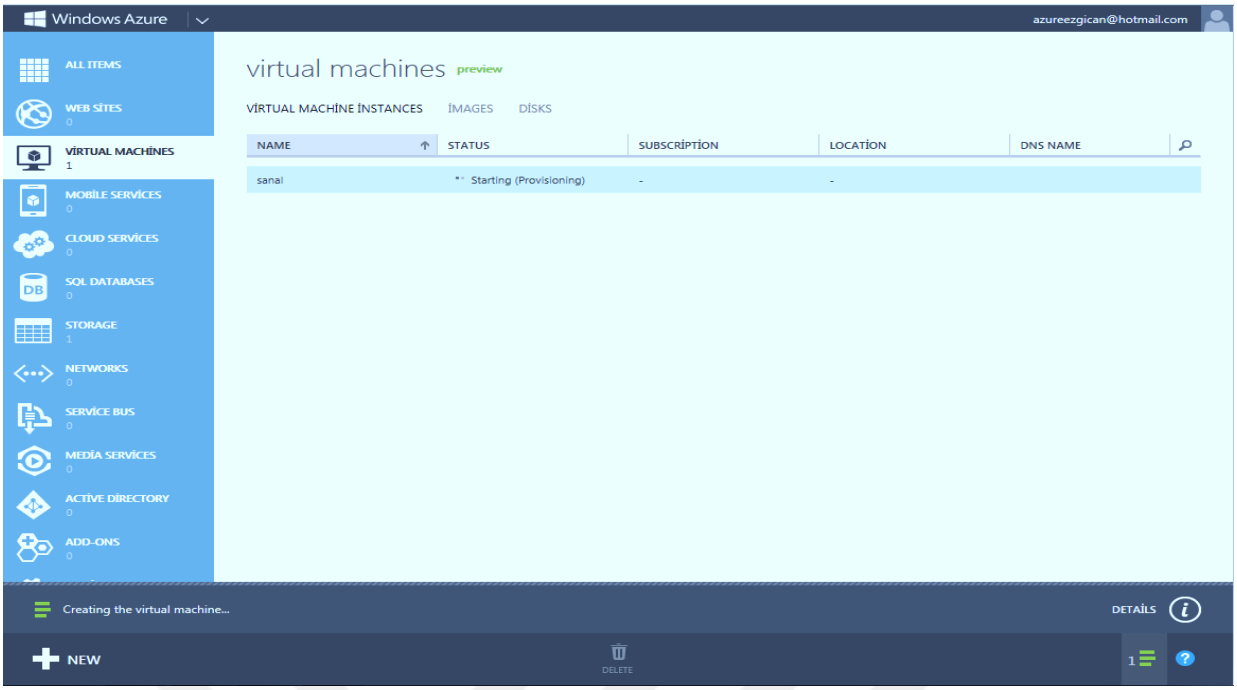
Şekil 6.5: Microsoft Azure Platformunda Sanal Sunucu Kurulumu

Adım 6: Bu aşamada kurulum tamamlanma aşamasına gelmiş sayılır. “Virtual Machine Option” ekranında kurum network üzerinden erişimlere açık bir şekilde paylaşılmak isteniyorsa “Availability Set” seçimi yapılması gerekmektedir. Ya da standart ayarlar ”None” üzerinden ileri devam edilebilir. Bu adımdan sonra sanal makine kurlum işlemi tamamlanmış olmaktadır. Diğer ayarlamalar sonrasında kullanıcıların iş ve işlemlerini sağlayacak niteliğe gelecektir.



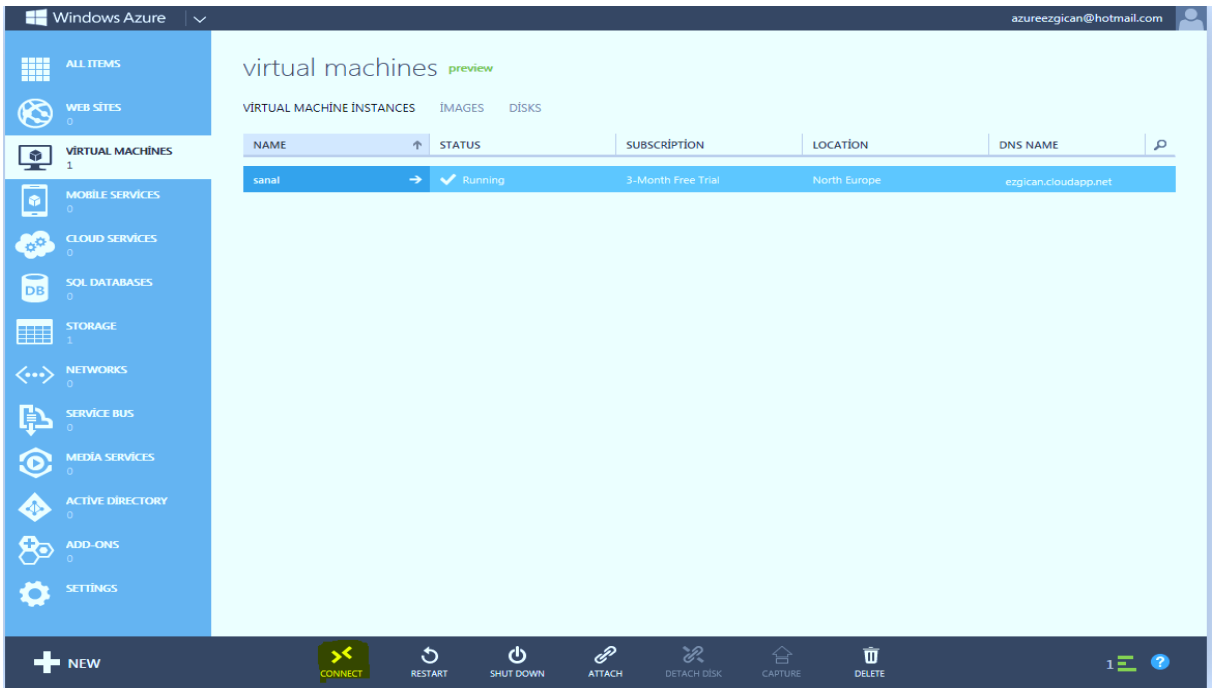
Şekil 6.6: Microsoft Azure Platformunda Sanal Sunucu Kurulumu

Adım 7: Windows Azure ortamında bir sanal bir makine kurulumu yapılmış oldu. Bu ekranda "Web Sites, Virtual Machine, Mobile Services, Cloud Services, SQL Databases, Storage, Networks, Services Bus, Media Services, Active Directory, Addı-Ons" gibi iş ve işlemler yapılabilmektedir. Bu ekranda kullanıcıların oluşturduğu tüm sanal makinalar ve durumları görülebilmektedir.



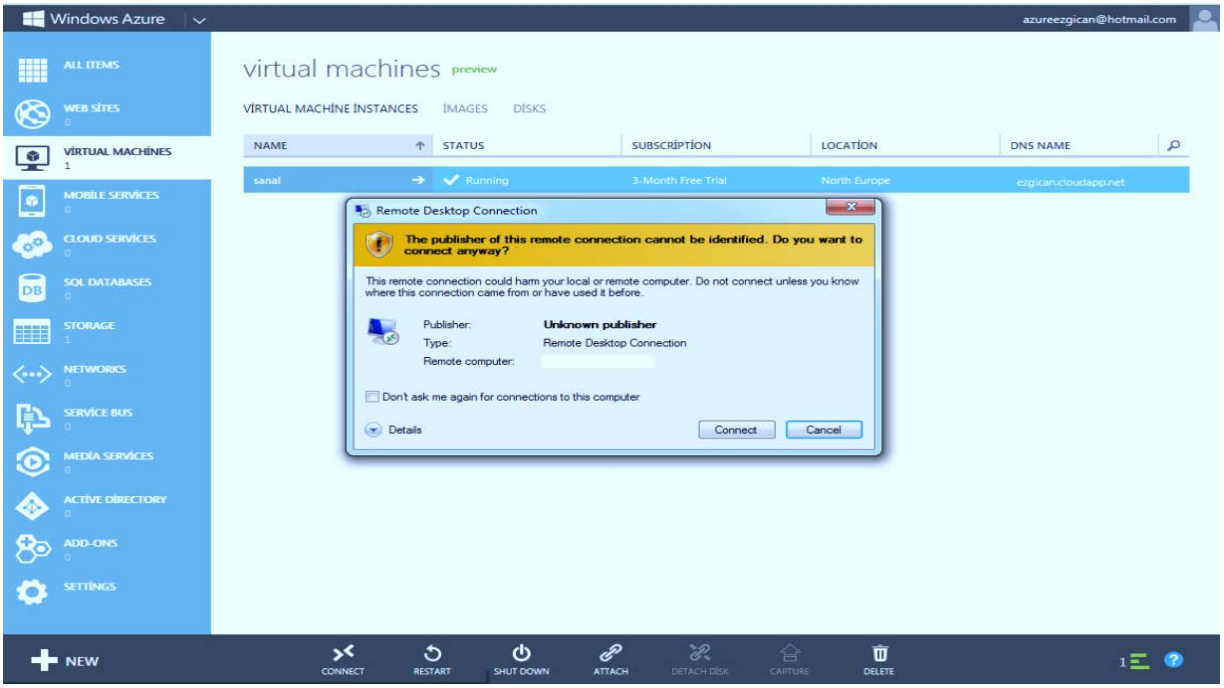
Şekil 6.7: Microsoft Azure Platformunda Sanal Sunucu Kurulumu

Adım 8: Sanal makinalar kurulumundan sonra bağlanma, silme, kapama, resetleme gibi iş ve işlemler yapılabilir. "Connet" ile sanal makinaya bağlanma, "Restart" sanal makinayı resetleme, "Shutdown"sanal makinanın kapatılması, "Attach" sanal makinada var olan diskleri biçimlendirme yada disk ekleme, "Delete" ile sanal makine silme gibi işlemlerin yapıldığı ekrandır.



Şekil 6.8: Microsoft Azure Platformunda Sanal Sunucu Kurulumu

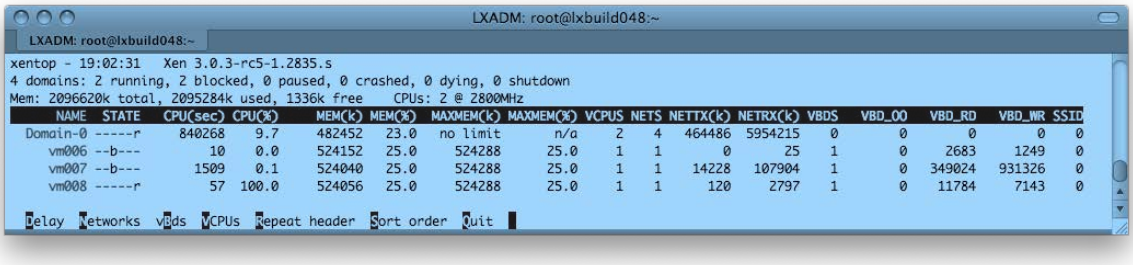
Adım 9: Bir önceki adımda kurulum ve yapılaşma ekranlarının bitirilmesi sağlanmış oldu. Artık sanal sunucunun kurulduğu ve veri tranferleri, kullanıcılara özel uygulamaların yükleme işlemlerinin yapılması işlemleri yapılabilmektedir. Burada CONNECT tıklayarak "Microsoft Uzak Masaüstü Bağlantısı" ekranının açılması sağlanır Şekil 6.1'de. Kullanıcı profil ayarlarını girerek kullanıcılar artık makinaya bağlantı sağlarlar.



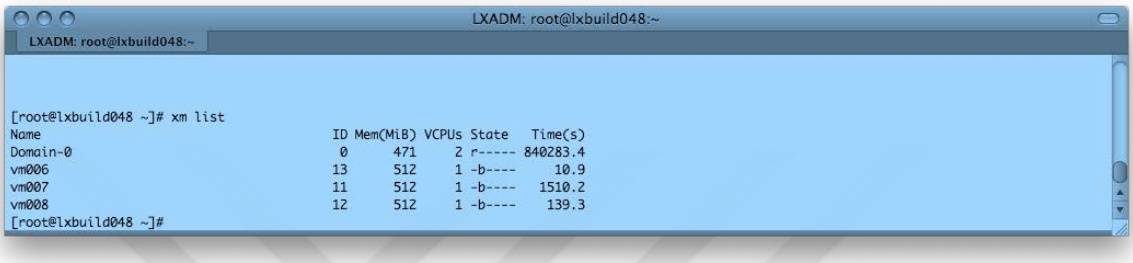
Şekil 6.9: Microsoft Azure Platformunda Sanal Sunucu Kurulumu

6.2. İşlemci Kullanımı Etkisi

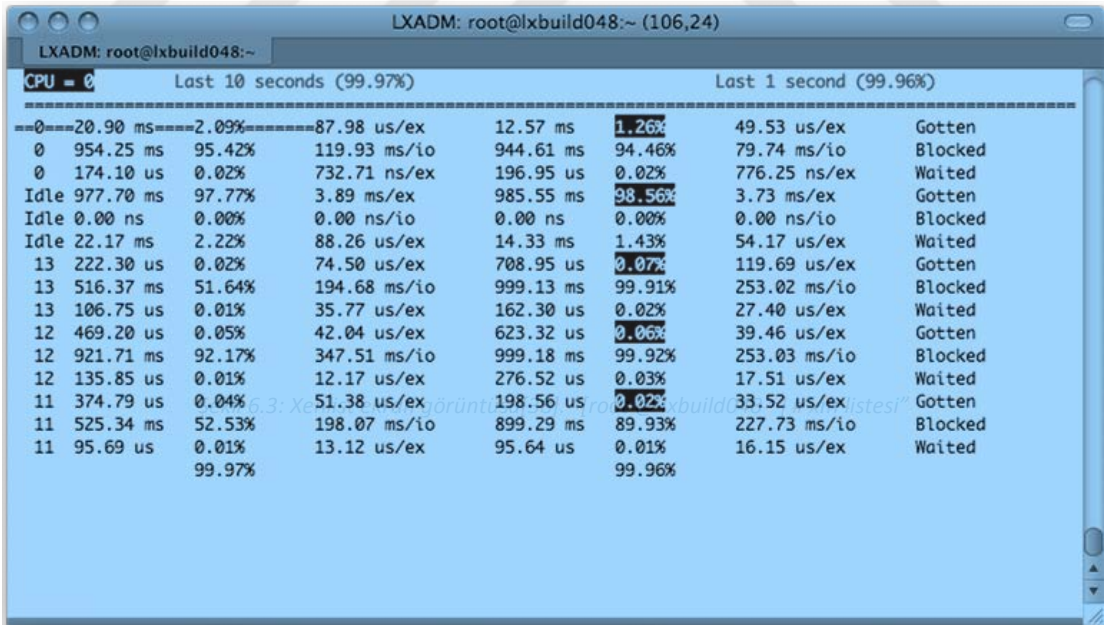
Sanallaştırma VM'lerinin işlemci gibi bilgilerin kontrolü için xen sanallaştırma teknolojilerinin ortam monitör araçlarından olan "xentop" gibi yazılımlara ihtiyaç vardır. Xentop bir Xen sistemi hakkında detaylı anlık bilgiyi verir[37]. VM üzerinde kurulan bütün sanal makinaların kullanım grafiklerini detaylı kullanıcılara sunan bu yazılım Sekil 6.2'de ekran görüntüsü vardır. Xentop yazılımının çeşitli özellikleri vardır bunlar aşağıda sıralanmıştır[37]. Ayrıca XenList, Xenmon.py, gibi yazılımlarda yine Xentop gibi kullanıcılara detaylı birlileri vermektedir Şekil 6.3-4-5'de gösterilmiştir.



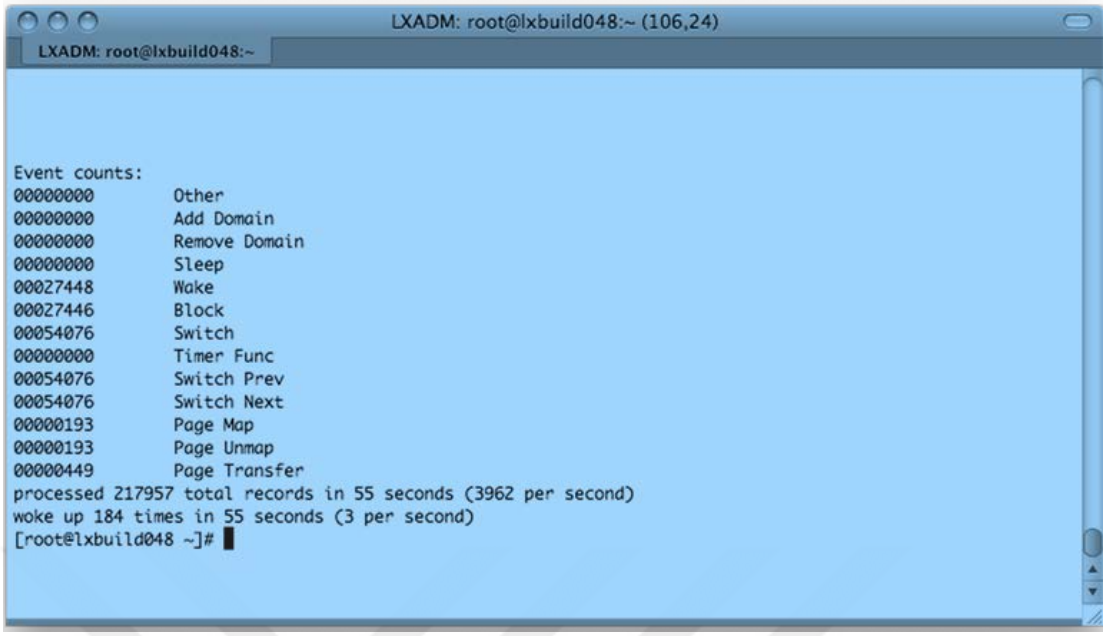
Şekil 6.10: Xenlist ekran görüntüsü[38]. “[root @ lxbuild048 ~] # xm listesi”



Şekil 6.11: Xentop ekran görüntüsü[38]. ” [root @ lxbuild048 ~] # xentop”



Şekil 6.12: Xenmon.py ekran görüntüsü[38]. [root @ lxbuild048 ~] # xenmon.py



Şekil 6.13: Xenmon.py ekran görüntüsü[38]. "[root @ lxbuild048 ~] # xenmon.py"

Xentop Yazılımı;

- CPU(sec)=Domain İşlemcisinin Saniyelik Kullanımı
- CPU(%)=İşlemci Kullanım Oranlarının Yüzdelik Miktarı
- VCPUS=Sanal İşlemcilerin Gerçekte Var Olan İşlemci Sayısı
- NETS=Sanal Ağların Sayısı
- MEM=Geçerli Hafıza Miktarı
- MAXMEM(k)=KB(Kilobayt) Cinsinden Domain Hafıza Bilgisi
- MAXMEM(%)=Domain Hafıza Bilgisinin Kullanılan Sunuculara Yüzdelik Oranı
- NETTX=Ağda İletilen bayt/1024 Değeri
- NETRX=Ada Alınan bayt/1024 Değeri
- VBDS=Sanal Bağlı Blok Aygıtlarının Miktarı
- VBO OO, VBD_RD,VBD_WR=Hataların ve Okuma Yazma Gibi Değerlerin Sayısı
- R=Dom0 ve Dom1 Aktif
- P=Dom Hazır Bekliyor
- C=Dom Üzerinde ki Verilerin Çökebilir
- B=Dom Engeli
- S=Dom Kapanması

Xentop yazılımı yukarıda ki verileri 3'er saniye aralıklarla kullanıcıların bilgisine sunar. R_P_C_B_S gibi fonksiyonlarla da sanal makinanin kullanım pratikliğini sağlar. Yaptığımız örneklemde donanım yukarıdaki opsiyonlarla çalıştırılmış olup, 2sn ile 100sn zaman aralığında 100 iterasyon ile 2,6,10sn zamanlarla yenilenmiştir. Yaptığımız çalıştırma kaynak kodları;

[root @ lxbuild048 ~] #xentop –i 100 –d 2 –b

[root @ lxbuild048 ~] #xentop –i 100 –d 20 –b

[root @ lxbuild048 ~] #xentop –i 100 –d 6 –b

Yaptığımız örnekte xentop yazılımının kullanımı ve kullanıcılara sunduğu faydalar görülmüştür. "-i" parametresi ile 100 iterasyon sayısının gecikmeden dolayı 2,6,20 gibi değerler sunduğu görülmüştür.

6.3. RAM KULLANIMI ÜZERİNE ETKİSİ

Fedora OS işletim sistemleri ortamında "top" yazılımı kullanılarak yapacağımız deneme de ana sunucu ve VeriMerkezlerinin RAM kullanımlarının ölçümü yapılmıştır. Kullanıcak olan "top" yazılımı Fedora OS işletim sisteminin dahili bir yazılımıdır. Bu yazılım; işletim sisteminin kullandığı tüm verilerin Ram'e yüklemesi gerekmez. Bunun yerine bu kodun depolandığı sanal bellek adı verilen bir harita oluşturur. Bu bir uygulamanın bir kerede sistemden daha az bellek kullanırken, çok fazla miktarda belleği işleyebileceği anlamına gelir. Bu yazılımla bu gibi görünmez Ram kullanımlarının ve gizli çalışmaların denetimi gerçekleşmektedir. Sistemde anlık CPU ve Ram gibi fiziki donanım kullanımlarını ele almak gibi kolaylık sağlar. Ayrıca varsa istem dışı çalışan uygulamalarında VM'den kaldırılması işlemlerinin de yapılabilirliği sağlar. "Top" yazılımıyla yaptığımız çalışmanın ekran resmi ve parametreleri aşağıda açıklamalarıyla gösterilmiştir.

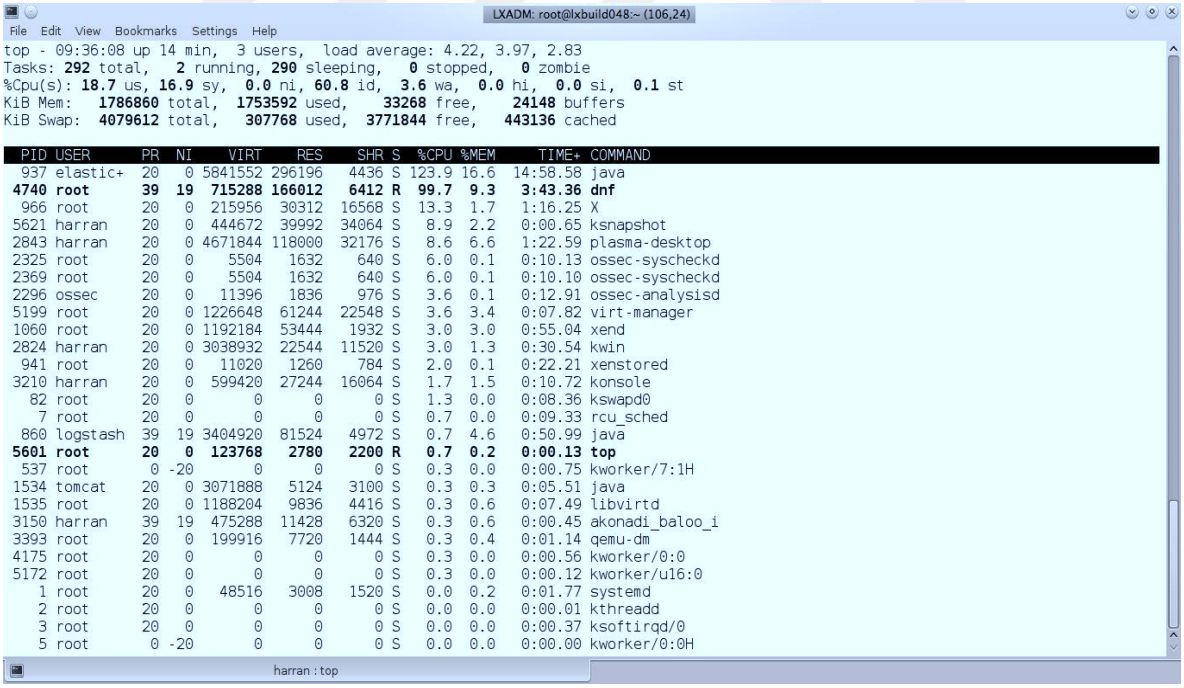
Ekranda yer alan bilgiler kısaca;

- Top komutu çalışama saati
- Sistemin toplam çalışma süresi
- Aktif olan kullanıcı sayısı
- 1-5-15dk gibi zaman aralıklarında yük çizelgesi
- Belli zamanlarda ki CPU kullanımı

- Çalışmakta olan uygulama sayısı
- Durdurulmuş, kullanılmayan işlem sayısı
- CPU çalışma ayrıntılarının detaylı oranları
- Kullanılabilir hafıza
- Fiziksel hafıza kullanım durumu
- Sanal hafıza kullanım durumu

Bu yazılımın sağladığı birçok avantaj vardır kısaca verilerin incelenmesi ve gerektiğinde müdahale edilmesi gibi faydalar sağlamaktadır. Yazılım sayesinde işlemciyi hangi program, yazılım, uygulama ne kadar kullanıyor bunları maximum seviyeden minimuma doğru sıralar.

Bu yazılım sayesinde sırasıyla Çalışan yazılımların "ID" numaraları, Çalıştıran kullanıcı "USER" isimleri, Çalışan uygulamaların önem sıralaması "PR", işlemlerin önem sıralamalarının değişimi "NI", sanal hafıza kullanım miktarı "VIRT", hafıza kullanım değerlerinin kilobayt cinsinden gösterir "RES". Şekil 6.3'te ekran görüntüsü gösterilmiştir.

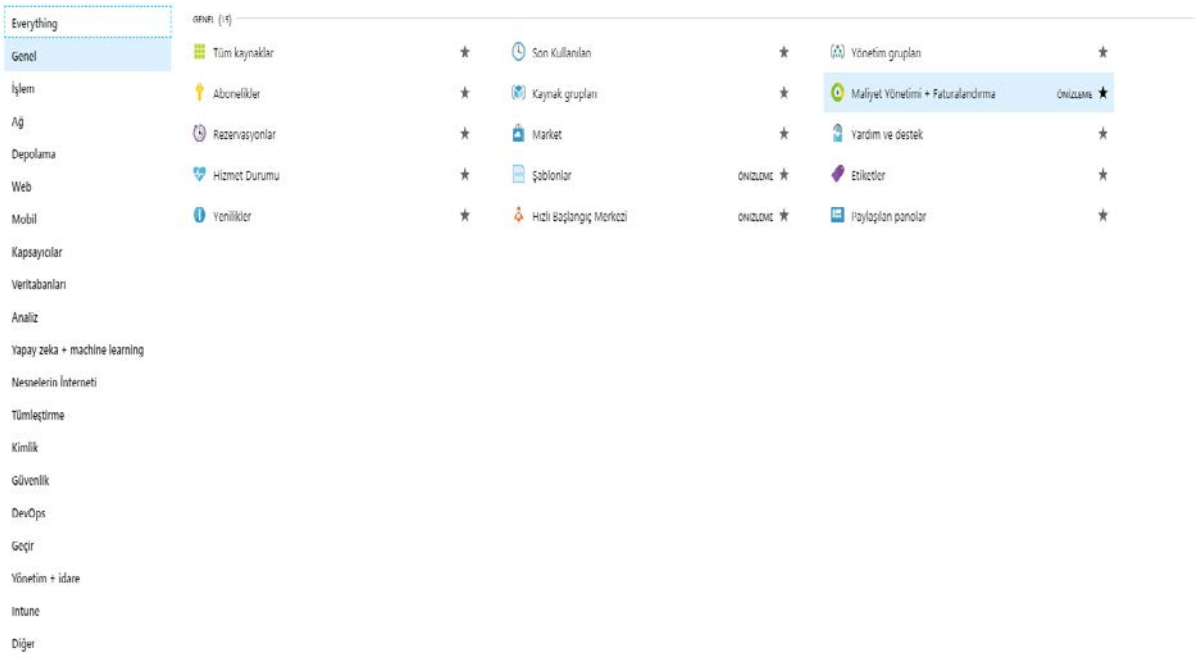


Şekil 6.14: Top yazılımı ekran görünümü

7. MİCROSOFT AZURE PLATFORMU VE GENEL HİZMET SUNDUĞU UYGULAMALARI

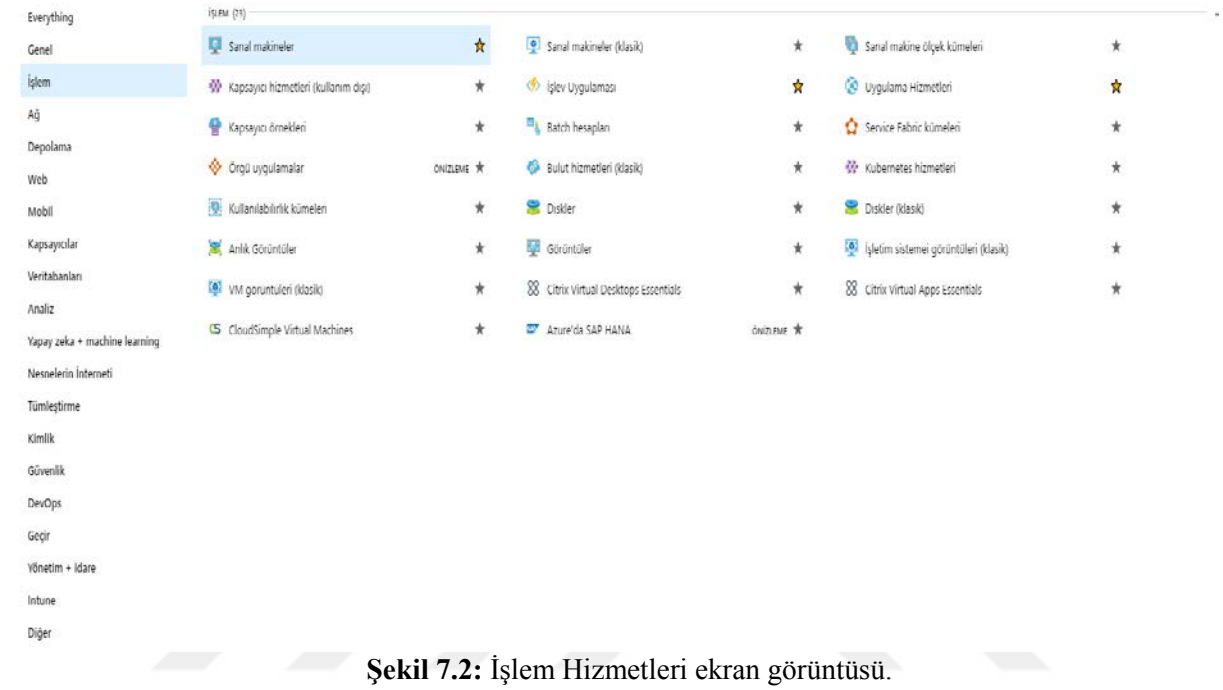
Bulut bilişimin en büyük aktörlerinden olan Microsoft hem kullanıcılara sunduğu kolay anlaşılabilir arayüzü ile hem de ücret fiyatlandırma çeşitliliği ile farklı avantajlar sunmaktadır. Bu bölümde kullanıcıların hizmetine sunduğu uygulama ve hizmetlerini inceleyeceğiz.

Genel Hizmetler bölümünde kullanıcların Abonelik, rezervasyon ve hizmet durumlarını gösteren uygulama grupları bulunmaktadır. Şekil 7.1 :Genel Hizmetler Ekran görüntüsü



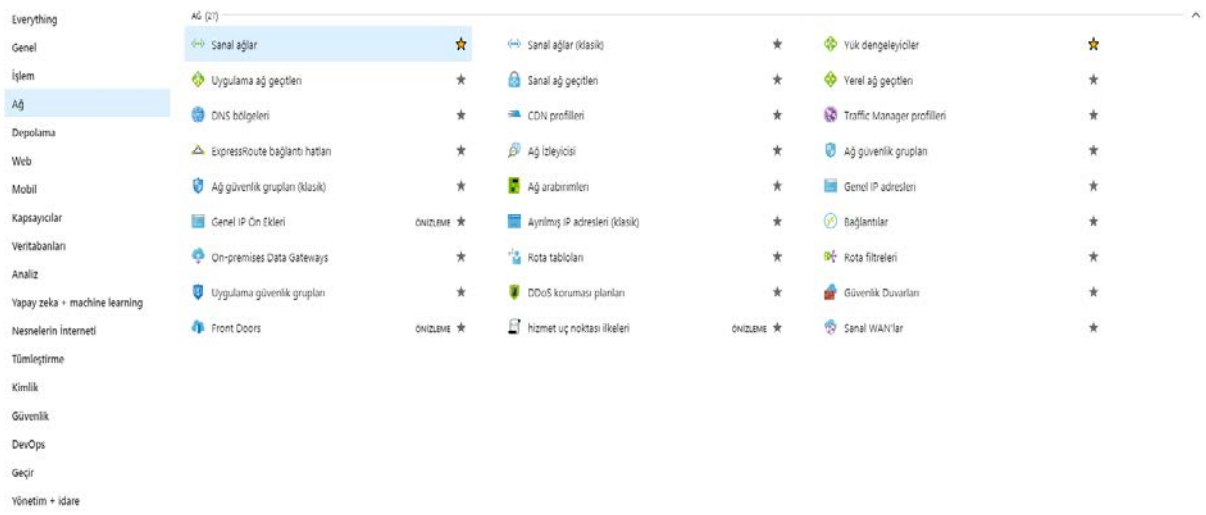
Şekil 7.1:Genel Hizmetler Ekran görüntüsü

İşlemler bölümünde kullanıcıların oluşturmak istedikleri sanal makinalar işlem uygulamaları, batch uygulamaları, anlık uygulamalar, VM görüntüleri, işletim sistemleri gürüntülerinin izlenmesi ve kontrollerinin sağlanması vb. işlemlerinin yapıldığı ekrandır. Şekil 7.2 : İşlem Hizmetleri ekran görüntüsü.



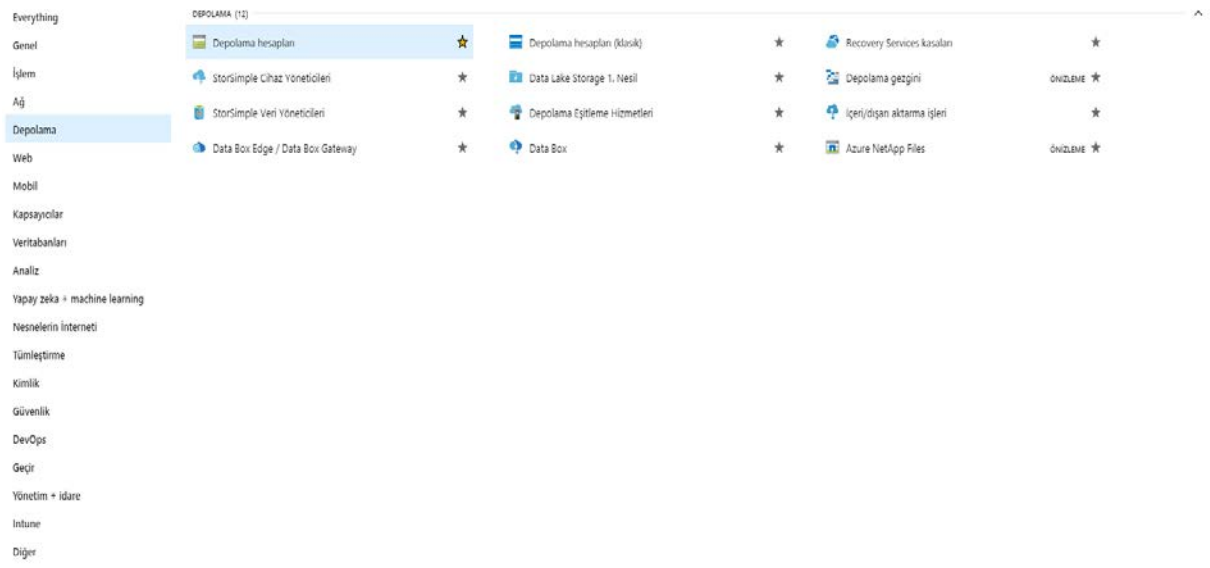
Şekil 7.2: İşlem Hizmetleri ekran görüntüsü.

Ağ Hizmeleri kısmında DNS, ağ güvenlik grupları, ağ izleyicisi, uygulama güvenlik gruplayıcıları, DDos Koruma planları, güvenlik duvarları vs. hizmetlerin sunuldupu ve gerekli ağ güvenlik önlemlerinin kontrol makanizmalarının sağlandığı akrandır. Şekil 7.3: Ağ Hizmetleri ekran görüntüsü



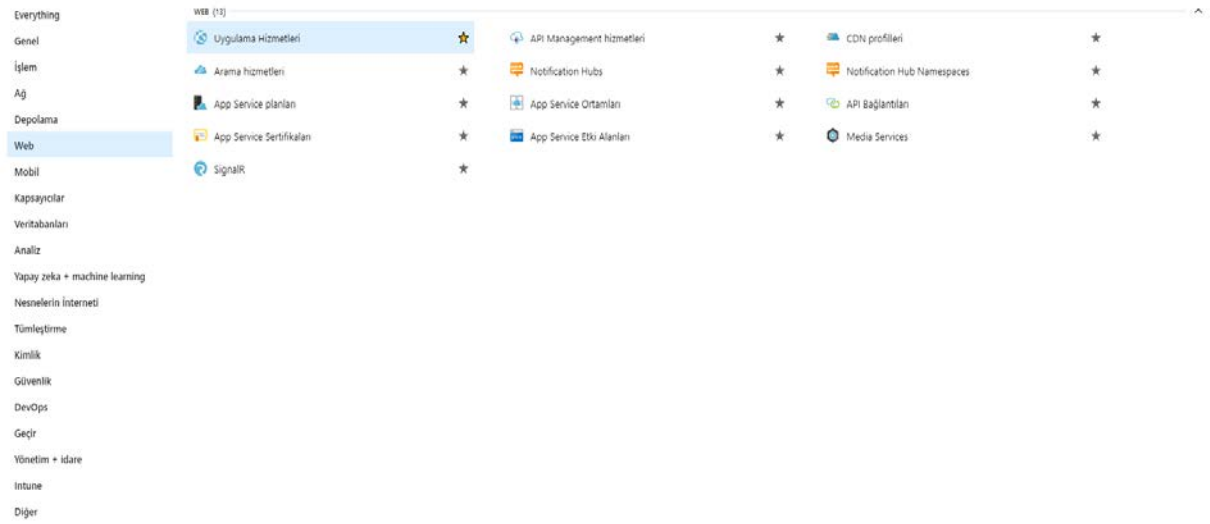
Şekil 7.3: Ağ Hizmetleri ekran görüntüsü

Depolama hizmetlerinde; bulut bilişimin temel mantığı olan sanal sunucuların ve depolama hesaplarının oluşturulması ve bunların takiplerinin edilmesi, StorSimple Cihaz Yöneticileri, StorSimple Veri Yöneticileri, İçeri-Dışarı aktarma işlemleri gibi işlemlerin yapıldığı ekrandır. Şekil 7.4: Depolama Hizmetleri Ekran Görüntüsü.



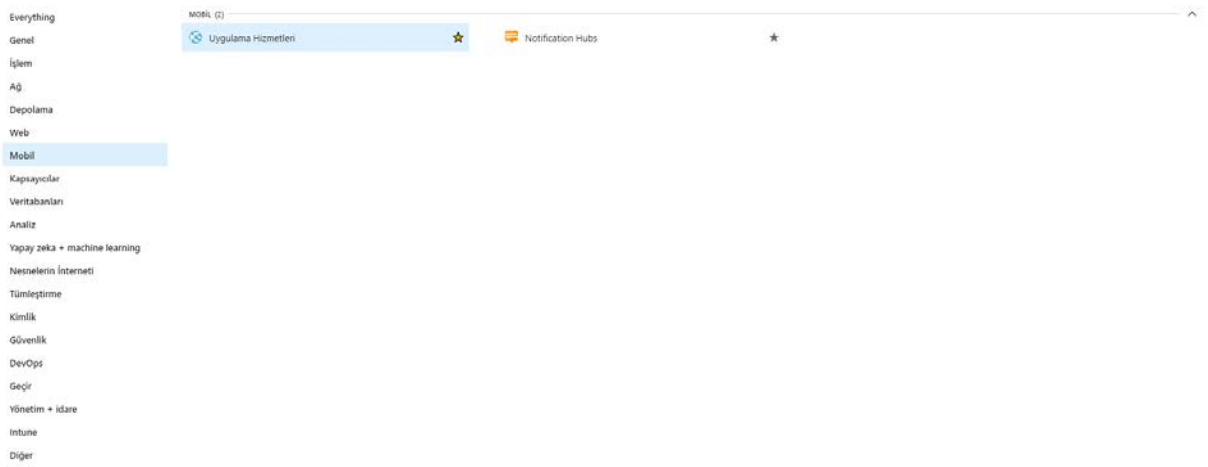
Şekil 7.4: Depolama Hizmetleri Ekran Görüntüsü.

Web Hizmetleri; internet ağında tanımlacak olan bütün yazılım ve uygulamaların bağlantı-servis, etki alanları gibi işlemlerin yapıldığı hizmet alanıdır. Bu kısımda Uygulama Hizmetleri, App Service Planları, App Service Serfitikaları, CND profilleri, API Bağlantıları vb. gibi işlemler yapılabilmektedir. Şekil 7.5: Web Hizmetleri Ekran Görüntüsü.



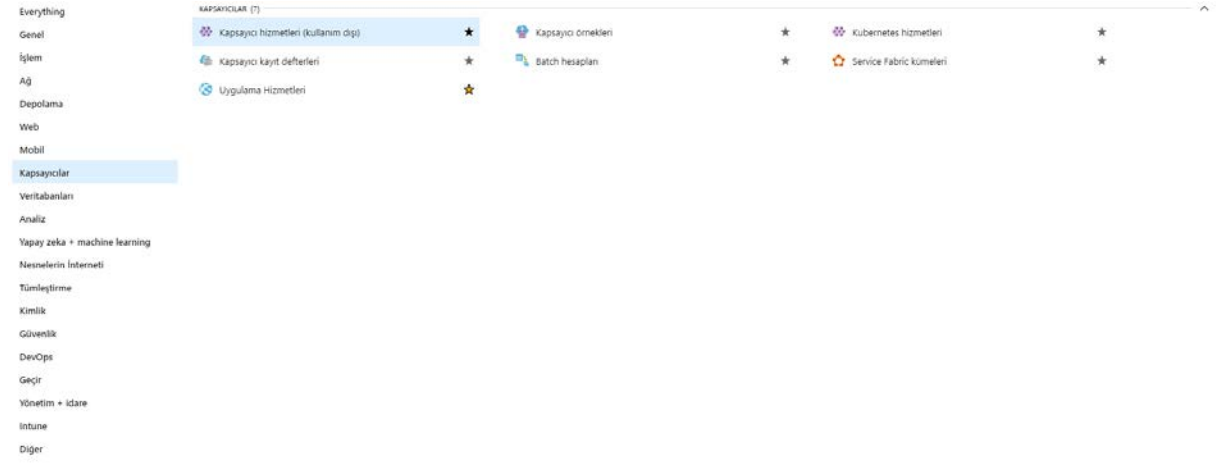
Şekil 7.5: Web Hizmetleri Ekran Görüntüsü.

Mobil Hizmetler Ekranında; Uygulama Hizmetleri yönetimi ve Notification Hubs işlemleri yapılabilmektedir. Şekil 7.6: Mobil Hizmetleri Ekran Görüntüsü.



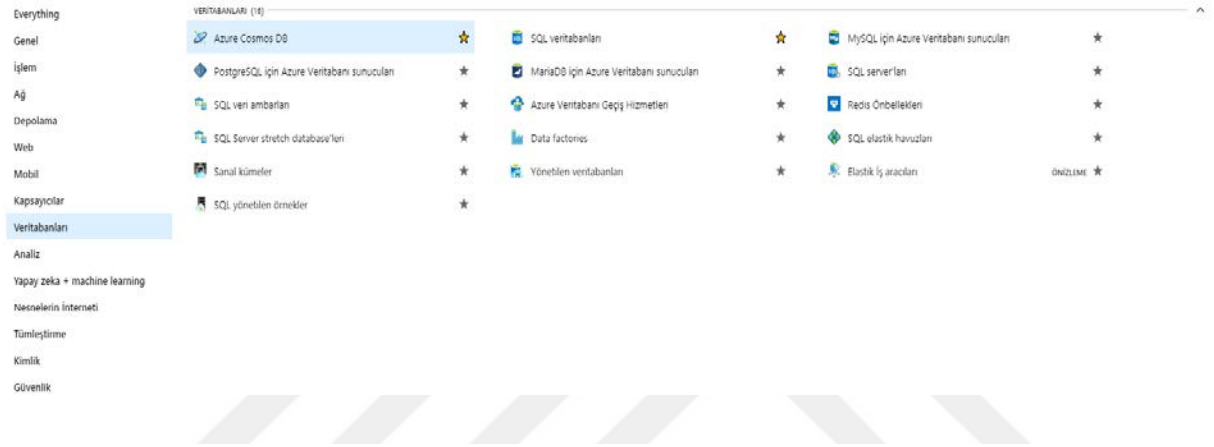
Şekil 7.6: Mobil Hizmetleri Ekran Görüntüsü.

Kapsayıcılar Hizmetleri ekranında; kapsayıcı hizmetleri (kullanım dışı), kapsayıcı kayıt defteri, uygulama hizmetleri, kapsayıcı örnekleri, batch hesapları, kubernetes hizmetleri, service fabric kümeleri gibi hizmetler bulunmaktadır. Şekil 7.7: Kapsayıcılar Hizmetleri Ekran Görüntüsü.



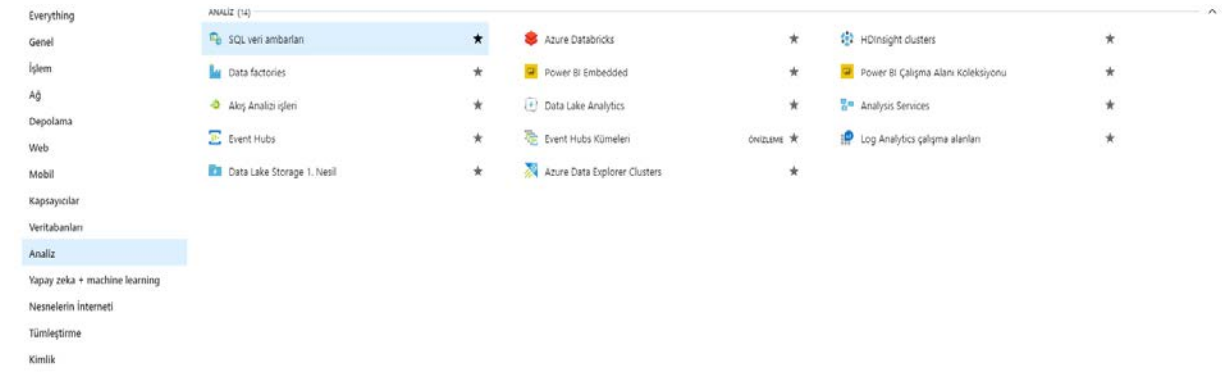
Şekil 7.7: Kapsayıcılar Hizmetleri Ekran Görüntüsü.

Veritabanları Hizmetler Bölümünde; sunucuların çalışmasını ve kurgulanması işlemlerinin yapıldığı ekranlardır. Bu ekranları hizmetlerin ve verilerin kurgularının oluşumu için önem arz etmektedir. Bundan dolayı SQL ve MySQL gibi temel veri tabanları yönetim şablonlarının hizmetlerinin yapıldığı ekrandır. Bu kısımda Azure Cosmos DB, PostgreSQL için azure veri tabanı sunucuları, SQL veri ambarlarıi SQL Server Stretch databaseleri, sanal kümeler, SQL yönetim örnekleri, SQL veri Tabanları, Maria DB için Azure Veritabını sunucunları, Azure veritabanı geçiş hizmetleri, data factoroes, yönetim veritabanları, SQL serverları, redis önbellekleri, elastik iş araçlarının iş ve işlemlerinin tamamı bu ekranda yapılmaktadır. Şekil 7.8: Veritabanları Hizmetleri Ekran Görüntüsü.



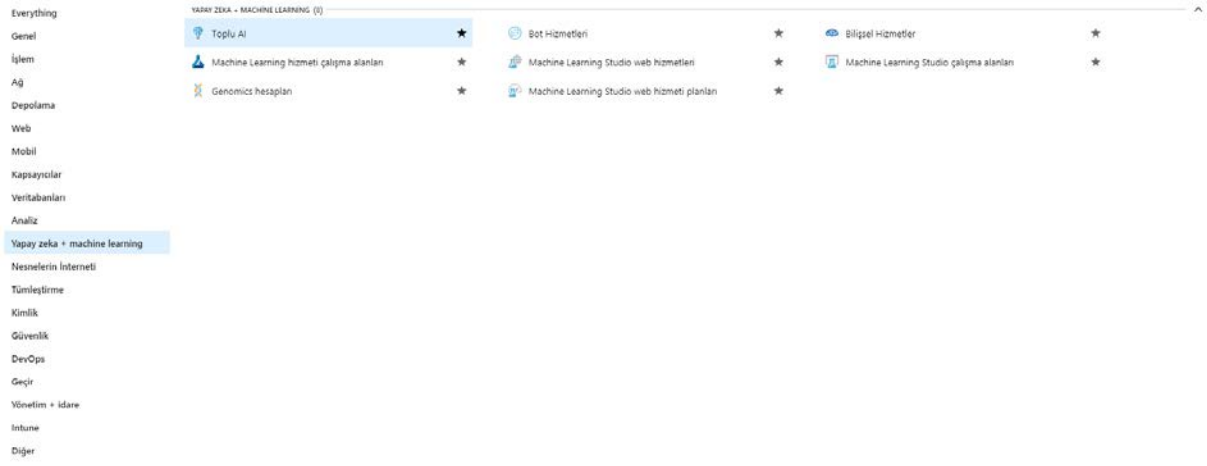
Şekil 7.8: Veritabanları Hizmetleri Ekran Görüntüsü.

Analizler ekranında; sanal sunucuların ve VM'lerinin analizlerinin yapıldığı ve işlemlerin yük kapasiteleri ile ilgili bilgilendirmelerin yapıldığı ekranlarıdır. SQL veri ambaları, Data factories, Akış Analiz İşlemleri, Event Hubs, data lake storage 1. Nesil, Azure databricks, power BI Embedded, data leke analyticks, event hubs,azure data explorer clusters, HDInsinght clusters, power BI çalışma alanı koleksiyonu, analysis services ve log analytics çalışama alanları gibi işlemlerin yürütüldüğü ekrandır. Şekil 7.9: Analiz Hizmetleri Ekran Görüntüsü.



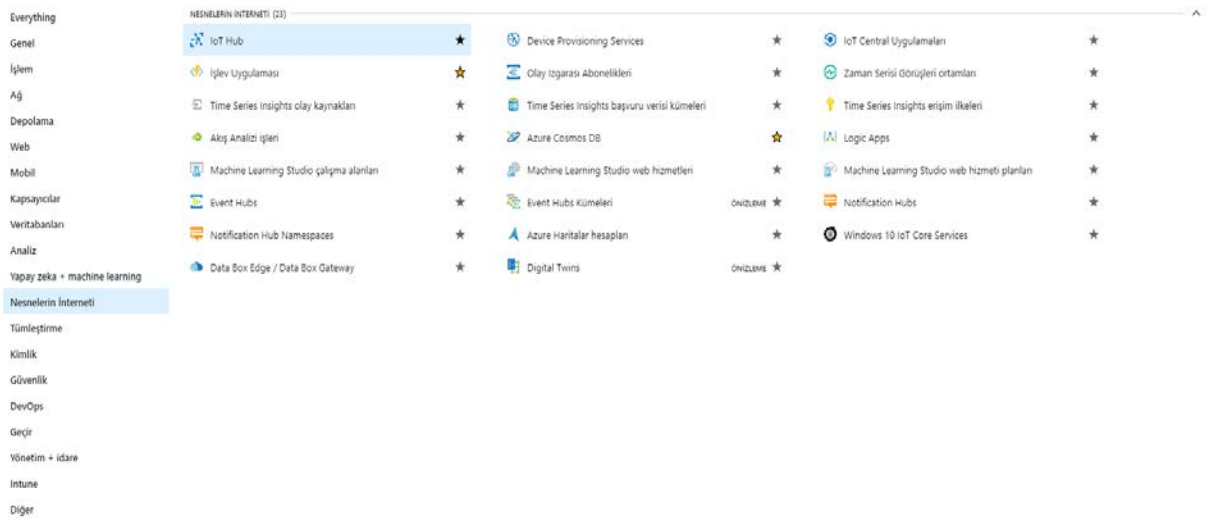
Şekil 7.9: Analiz Hizmetleri Ekran Görüntüsü.

Yapay Zeka + Machine Learning ekranında; Toplu alım, machine learning hizmeti çalışma alanları, genomics hesapları, bot hizmetleri, machine learning studio web hizmetleri, machine learning studio web hizmetleri planları, bileşen hzimetletler, machine studio çalışma alanları gibi araçlarla toplu işlerin yapılmasını kolaylaştırıcı araçlar kullanıcılara sunulmuştur. Şekil 7.10: Yapay Zeka + Machine Learning Hizmetleri Ekran Görüntüsü.



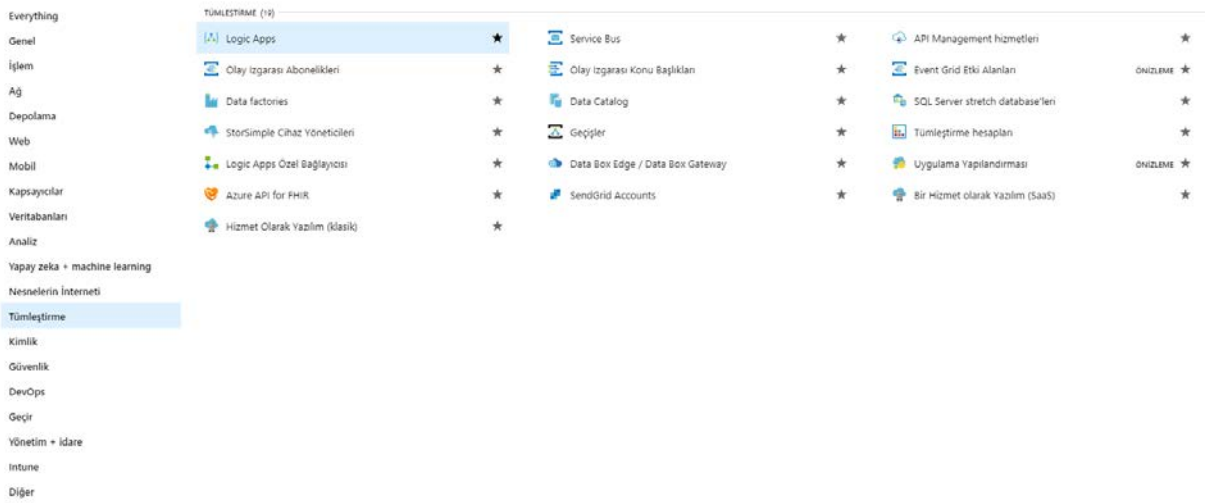
Şekil 7.10: Yapay Zeka + Machine Learning Hizmetleri Ekran Görüntüsü.

Nesnelerin İnterneti ekranında; akış analizlerinin izlenmesi ve işlerinin takip edilmesi ile Time Series Insights Olay Kaynaklarının analizlerinin yapıldığı ekrandır. Bu ekranda IoT Hub, İşlev Uygulaması, Machine Learning Studio Çalışma Alanları, Event Hubs, Notification Hub Namespaces, Data Box Edge/Data Box Gateway, Device Provisioning Services, Olay Izgara Abonelikleri, Time Series Insights Başvuru Verisi Kümeleri, Azure Cosmos DB, Machine Learning Studio Web Hizmetleri, Event Hubs Kümeleri, Azure Haritalar Hesapları, Digital Twins, IoT Central Uygulamaları, Zaman Serisi Görüşleri Ortamları, Time Series Insights Erişim İlkeleri, Logic App, Mechine Learning Studio Web Hizmetleri Planları, Notification Hubs, Windows 10 IoT Core Services gibi araçlar vardır bu ekranda. Şekil 7.11:Nesnelerin İnterneti Hizmetleri Ekran Görüntüsü.



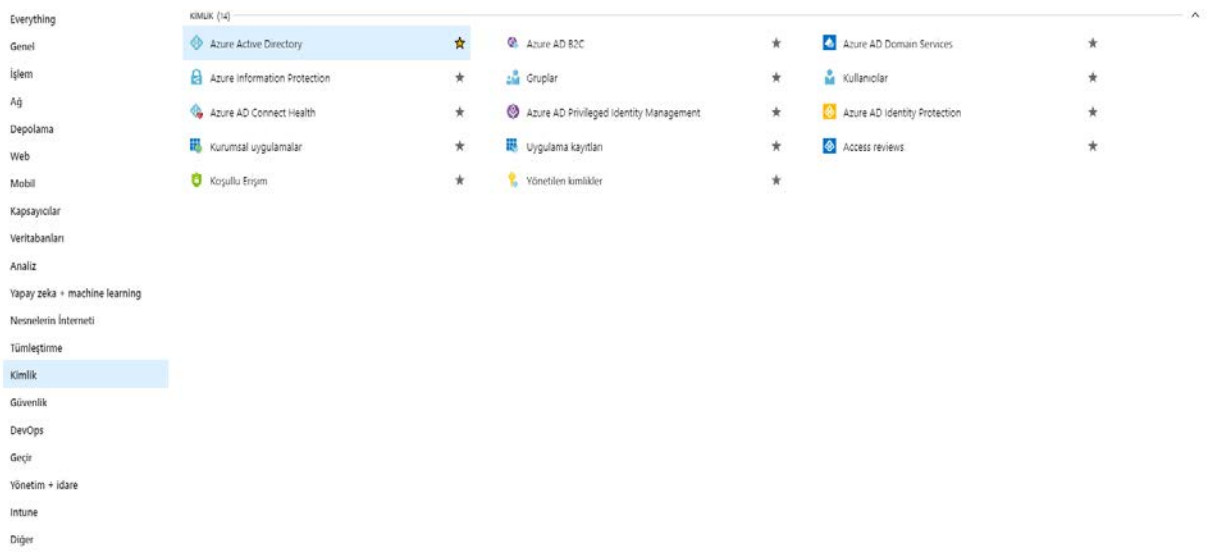
Şekil 7.11: Nesnelerin İnterneti Hizmetleri Ekran Görüntüsü.

Tümleştirme ekranında; bulut hizmetlerinin yazılım ve uygulama yapılandırması gibi işlemlerin yürütüldüğü ekrandır. Hizmet Olarak Yazılım (SaaS) sanallaştırma işlemlerinin ve VM sanallaştırma protokollerinin bu ekran aracılığı ile yapılmaktadır. Bu ekranda; Logic App, Olay Izgarası Abonelikleri, Data Faktories, StorSimple Cihaz Yöneticileri, Logic API for FHIR, Hizmet Olarak Yazılım (klasik), Service Bus, Olay Izgarası Konu Başlıkları, Data Catalog, Geçişler, Data Box Edge / Data Box Gateway, Send Grid Accounds, API Manegement Hizmetleri, Event Grid Etki Alanları, SQL Server Strethc Database'leri, Tümleştirme Hesapları, Uygulama Yapılandırmas, Bir Hizmet Olarak Yazılım (SaaS) gibi araçlar vardır. Şekil 7.12: Tümleştirme Hizmetleri Ekran Görüntüsü.



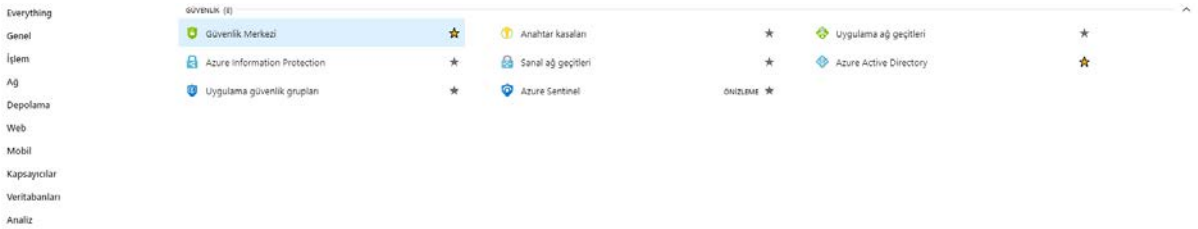
Şekil 7.12: Tümleştirme Hizmetleri Ekran Görüntüsü.

Kimlik Hizmetlerinde; domain sistemlerinin olmazsa olmaz yalımı olan Active Directory ile kullanıcılar tanımlara ve yetkilendirme işlemlerinin yapılması, kullanıcı gruplarının kimlik ve log kayıtlarının takibi, Azure Active Directory Azure Informaiton Protection, Azure AD Connect Health, Kurumsal Uygulamalar, Koşullu Erişim, Azure AD B2C, Gruplar, Azure AD Privilaged Identity Management, Uygulama Kayıtları, Yönetilen Kimlikler, Azure AD Domain Services, Kullanıcılar, Azure ADIdentity Protection, Acces Revievs gibi önemli uygulamaları barındırmaktadır. Şekil 7.13: Kimlik Hizmetleri Ekran Görüntüsü.



Şekil 7.13: Kimlik Hizmetleri Ekran Görüntüsü.

Güvenlik Hizmetlerinde; sanal sunucular ve host edilen bütün sitelerin güvenlik mekanizmlarının oluşumu yönetimi izlenimi gibi iş ve işlemlerin yapıldığı ekrandır. Güvenlik Merkezi, Azure Information Protection, Uygulama Güvenlik Grupları, Anahtar Kasaları, Azure Centinal, Sanal Ağ Geçitleri, Uygulama Ağ Geçitileri, Azure Active Directory gibi uygulamalarda bu hizmetler ekranında bulunmaktadır. Şekil 7.14: Güvenlik Hizmetleri Ekran Görüntüsü.



Şekil 7.14: Güvenlik Hizmetleri Ekran Görüntüsü.

Azure sunduğu uygulamalar ve yönetimde ki kolaylılar sayesinde VM kontrolleri ve denetimlerinde diğer bulut bilişim sistemlerinin arayüzlerine nazaran daha kolay görünüm sergilenmektedir. Yukarıda sıraladığımız hizmetlerin yanında;

DevOps Hizmetler

- DevOps Projects
- DevTest Labs
- Azure DevOps Organizations
- API Managament Hizmetleri
- Application Insight
- Lab Services

Geçir Hizmetler

- Geçir Projeleri
- Recovery Services Kasaları
- Azure Veritabanı Gçeiş Hizmetleri
- Maliyet Yönetimi + Faturalandırma
- Data Box
- Data Box Edge / Data Box Gateway

Yönetim ve İdare Hizmetler

- Danışman,
- İlke,
- Blueprinter'ler
- Tanılama Ayarları
- Çözüm
- Konuk Atamaları
- Geçiş Projeleri
- Managed Desktop
- Recovery Services Kasaları
- Kullanıcı Gizliliği
- Etkinlik Günlüğü
- Uyarılar

- Scheduler İş Kolaksiyonları
- Ağ İzleyicisi
- Ücretsiz Hizmetler
- Hizmet Kataloğu Yönetilen Uygulaması Tanımları
- Maliyet Yönetimi ve Faturalandırma
- İzleyici
- Ölçümler
- Log Analytics Çalışma Alanları
- Otomasyon Hesapları
- Application Insightes
- İşlem Günlüğü
- Yönetilen Uygulamalar

Intune Hizmeletler

- Intune
- Eğitim İçin Intune
- Cihazlar
- Exchange Erişim
- Yazılım Güncelleştirmeleri
- Koşullu Erişim
- Intune Uygulama Koruması
- İstemci Uygulamaları
- Cihaz Yapılandırması
- Excange Şirket İçi Erişim
- Sorun Giderme
- Microsoft Intune
- eKitaplar
- Cihaz Kaydı
- Cihaz Uyumluluğu
- Security Baselines

Diğer Hizmetler

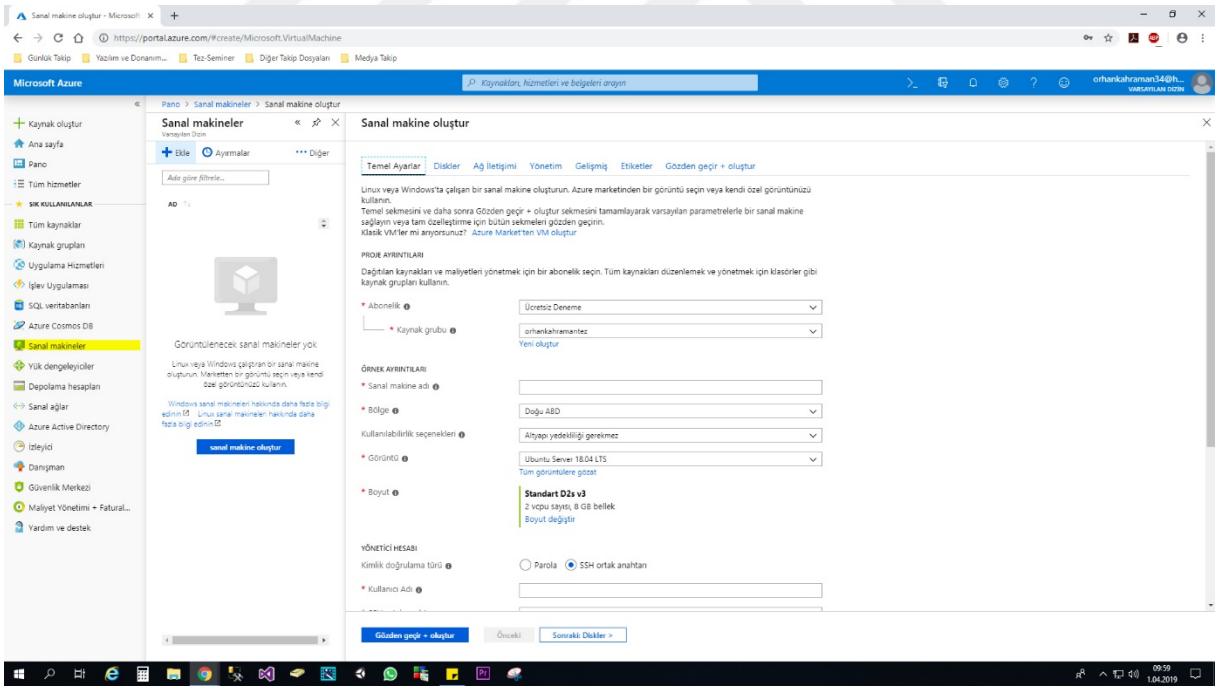
- AppDynamics
- Bing Maps API For Enterprise

- CloudMonix
- Crypteron
- Eğitim
- Kaynak Gezgini
- Mailjet Email Service
- Nuu:bit CND
- Raygun
- SparkPost
- The Identity Hub
- Aspera Server On Demond
- Classic Dev Services
- Contend Moderator
- Customer Luckbox for Microsoft Azure
- Hive Steaming
- Kiracı Durumu
- MyCloudiT-Azure Desktop Hosting
- PokitDok Platform
- RevAPM CDN
- Spatial Anchors Accounts
- Tümleştirme Hizmeti Ortamları
- Azure Iot Hub Securty
- CloudAMQP
- Controllers
- Deep Security SaaS
- İşlev Uygulamaları
- LiveArena Broadcast
- MyGet – Hosted NuGet, NPM, Brower and Vsix
- RavenHQ
- Signiant Flight
- Stackify
- Web Application Frewall policies

8. MİCROSOFT AZURE PLATFORMUNDA SANAL SUNUCU VE SQL VERİ TABANI KURULUMU

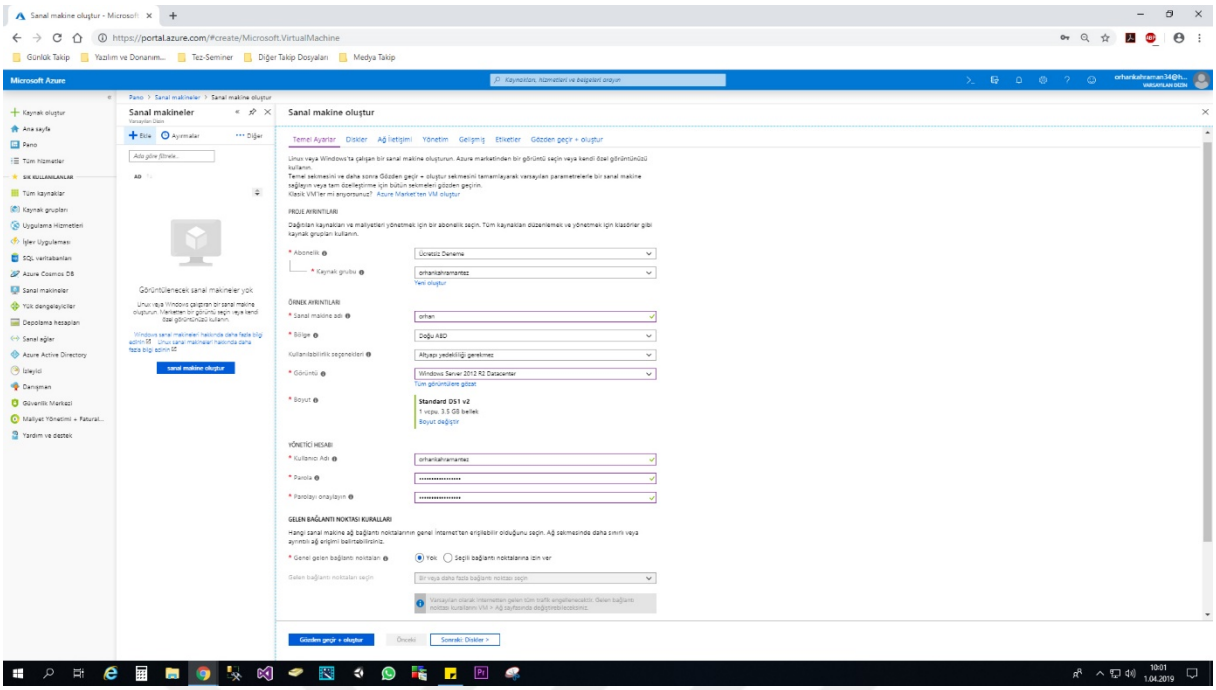
Bulut bilişimin kullanıcılar sunduğu en büyük kolaylık kesinlikle Sanal Sunucu ve onlara bağlı veritabanları oluşumunda sağladığı kolaylıklardır denilebilir. Fiziksel bir sunucunun kurulumu ve onlarla yapılacak olan veritabanı bağlantılarının ve kurulumlarının sadece deneyimli teknik personelle yapılabilir olması, maliyetlerin bunlara oranlara daha fazla çıkması gibi etmenlerden dolayı bulut bilişim büyük ayrıcalıklarla kullanıcılara sunulmaktadır. Sanal makine işletim sistemlerinin gelişimlerinin kolaylaştırmak, program dönüşümlerine yardımcı olmak, ve bu programları farklı işletim sistemleri üzerinde çalışabilmesine izin verebilmektedir[39]. Sanallaştırma, mevcut fiziksel bir donanımı mantıksal parçalara ayırarak sanal makinalar (Virtual Machine – VM) oluşturmak suretiyle birden fazla makine olarak kullanılmasını sağlamaktadır[40]. Microsoft Azure platformunda sanal sunucu kurulumunu ekran resimleri ile aşağıda örneklendirilmiştir.

- Azure ortamında Ana Sayfa- Sanal Makinalar- Ekle bölmesine gelerek oradan yeni bir sanal makine eklenir. Şekil 8.1: Azure Sanal Makine Oluşumunda 1. Adım

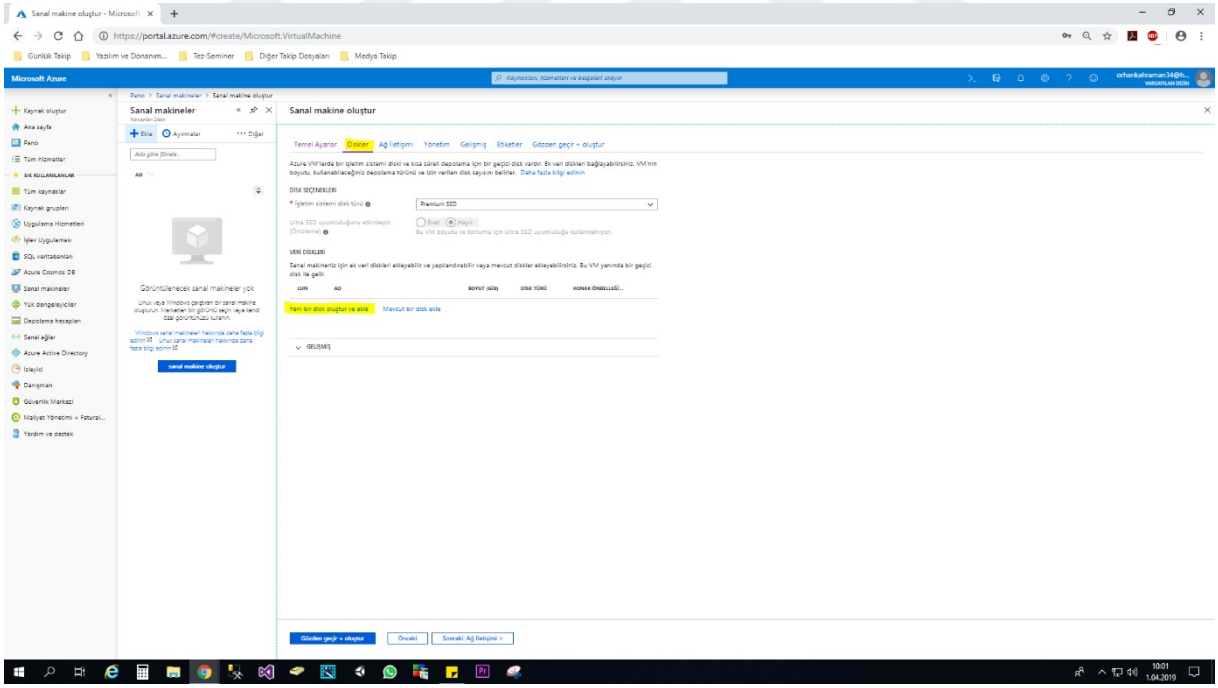


Şekil 8.1: Azure Sanal Makine Oluşumunda 1. Adım

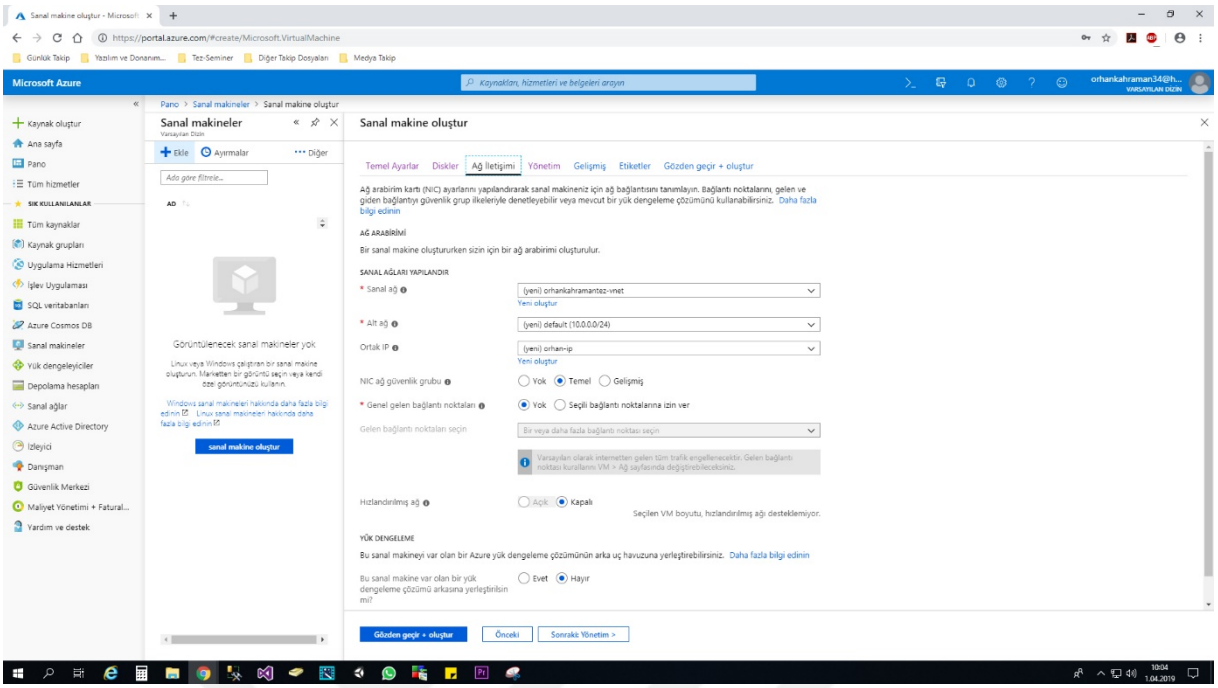
- Sanal Makine Oluşturma Ekranında; 7 ayrı ekran kullanıcılar karşısına çıkmaktadır. Temel Ayarlar Bölmesinde; Proje Ayrıntılarının girilmesi (sanal makine adı, kullanıcılar bölgesi, yedek alınıp alınmayacağı, hangi işletim sunucu yapısının kullanılacağı, sunucunun boyutunun ne olacağı, kimlik doğrulama mekanizmalarının parola ile mi yaksa SHH ortak anahtarıyla ile mi yapılacağı, kullanıcı adı ve SSH ortak anahtarının belirlenmesi gibi işlemlerin yapıldığı ortamdır). *Diskler* bölümünde ayrıntılı olarak VM'lerinde iki çeşit disk vardır. İşletim sistemi diski ve kısa süreli depola diski olarak adlandırılırlar[42]. İşletim sistemi disklerinde izin verilen disk türleri SSD ve HDD olarak belirlenmiştir. Bunlara bağlı olarak veri disklerinin de eklenmesi ve yapılandırılması gibi işlemlerinde yapılabildiği ekrandır. *Ağ İletişimi* Bölümünde ise Ağ Arabirim Kartı (NIC) ayarlarının yapılandırılması için ağ bağlantılarının tanımlaması işlemlerinin yapıldığı; Sanal Ağ, Alt Ağ, Ortak İp, NIC ağ güvenlik grubu, gelen genel bağlantı noktaları, yük dengeleme gibi işlemler ekranıdır. *Yönetim* bölümünde; VM izleme ve yönetimleri gibi iş ve işlemlerin yapıldığı ekrandır. Önyükleme tanılamaları, işletim sistemi konuk tanılaması, tanılama depolama hesabı, otomatik kapama ve yedekleme gibi işlemler ekranıdır. Sanal makine uzantıları, cloud-init ortamlarında ek yapılandırma ve uygulamaların eklendiği ekrandır. Etiketler ekranında bir ya da birden fazla kaynak grubuna aynı etiketle kaynak gruplarını çeşitleştirmek ya da ayrıştırmak için kullanılan bir kolaylık ekranıdır. Son olarak *"Gözden Geçir + Oluştur"* ekranında ise son gözden geçirme ayrıntıları vardır. Sanal sunucun oluşumu yapılan ayarlamalar oluşturulan işletim sistemleri ve ağ arabirimlerinin ayarlarının gözden geçirilip oluşumun son noktasıdır. Bu ekrandan sonra sanal sunucu oluşur ve uzak masaüstü bağlantısı aracı oluşturulan sanal sunucunun barındığı ip adres ayarlarından oluşan bağlantı modülü indirilir. Çalışımı sonrasında da normal bir makinaya bağlantı gerçekleştirilmişçesine artık sunucuya müdahale edilebilir. Yukarıda ki bütün adımlara ilişkin ekran görüntüleri sıralanmıştır. Şekil 8.2-3-4-5-6-7-8: Azure Sanal Makine Oluşumunun ekran görüntüleri verilmiştir.



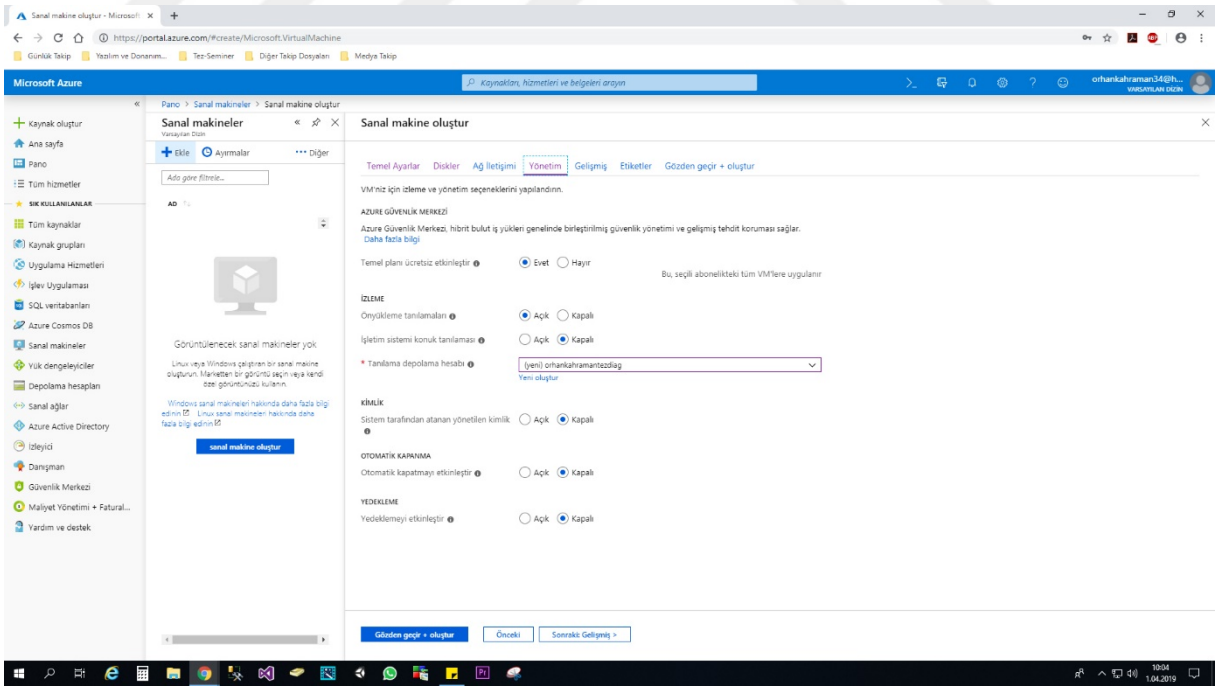
Şekil 8.2: Azure Sanal Makine Oluşumunda 2. Adım



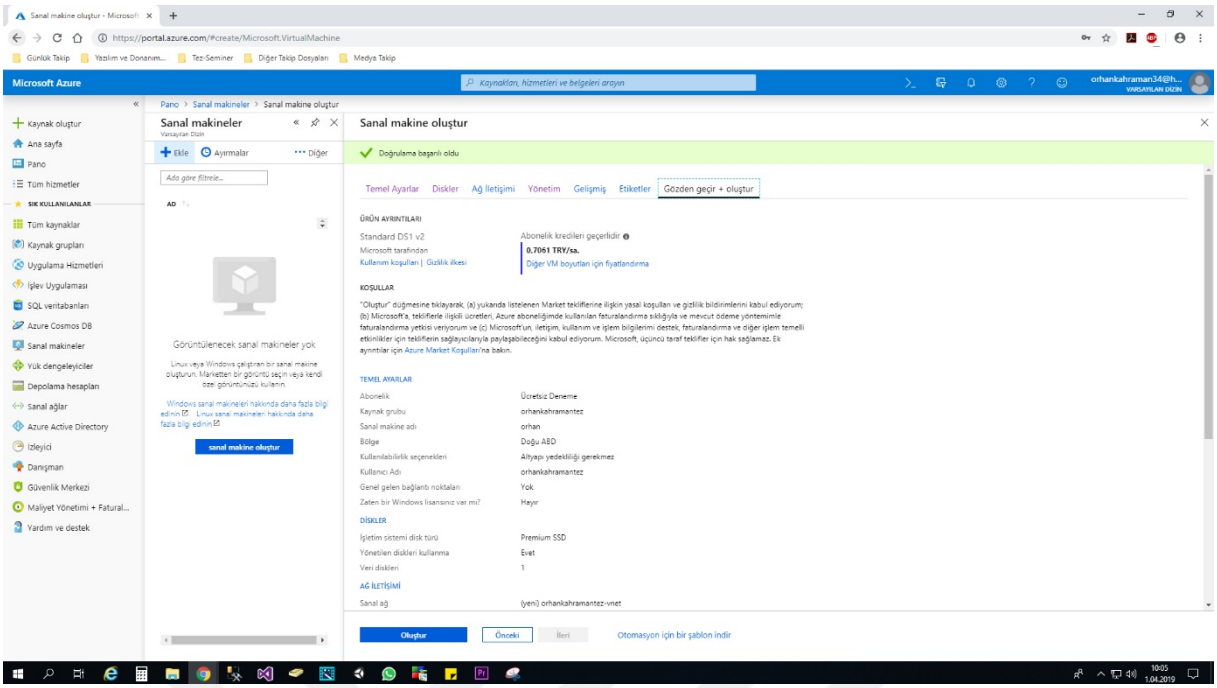
Şekil 8.3: Azure Sanal Makine Oluşumunda 3. Adım



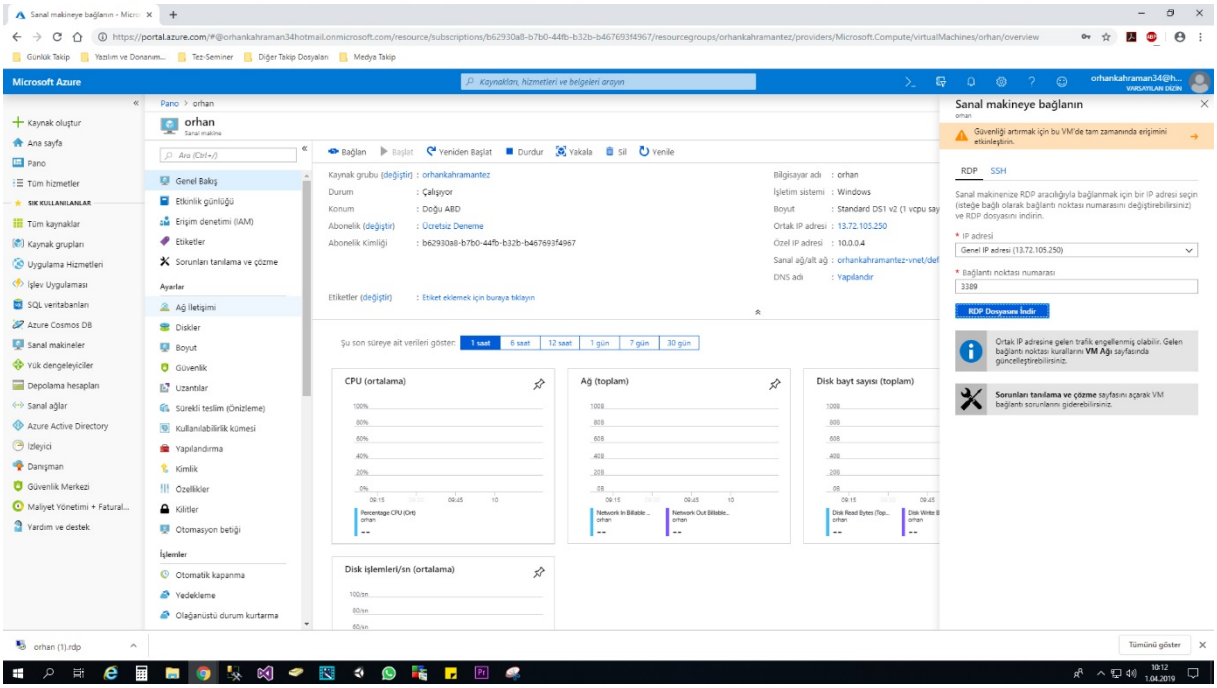
Şekil 8.4: Azure Sanal Makine Oluşumunda 4. Adım



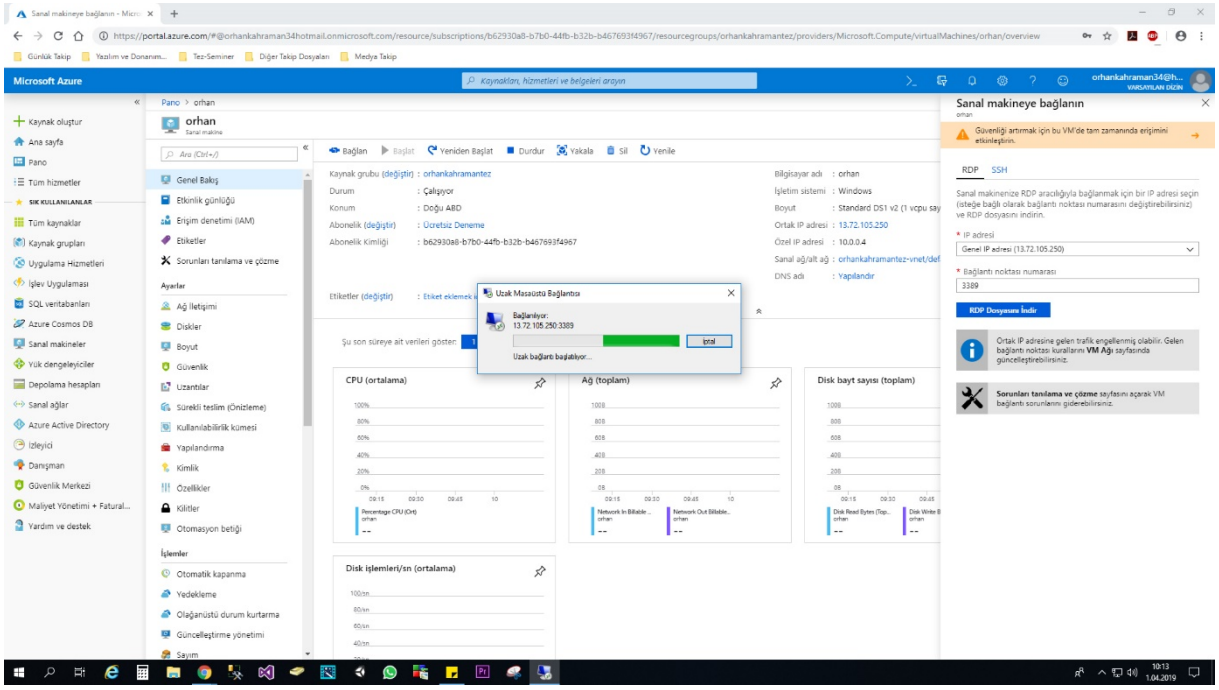
Şekil 8. 5: Azure Sanal Makine Oluşumunda 5. Adım



Şekil 8.6: Azure Sanal Makine Oluşumunda 6. Adım



Şekil 8.7: Azure Sanal Makine Oluşumunda 7. Adım

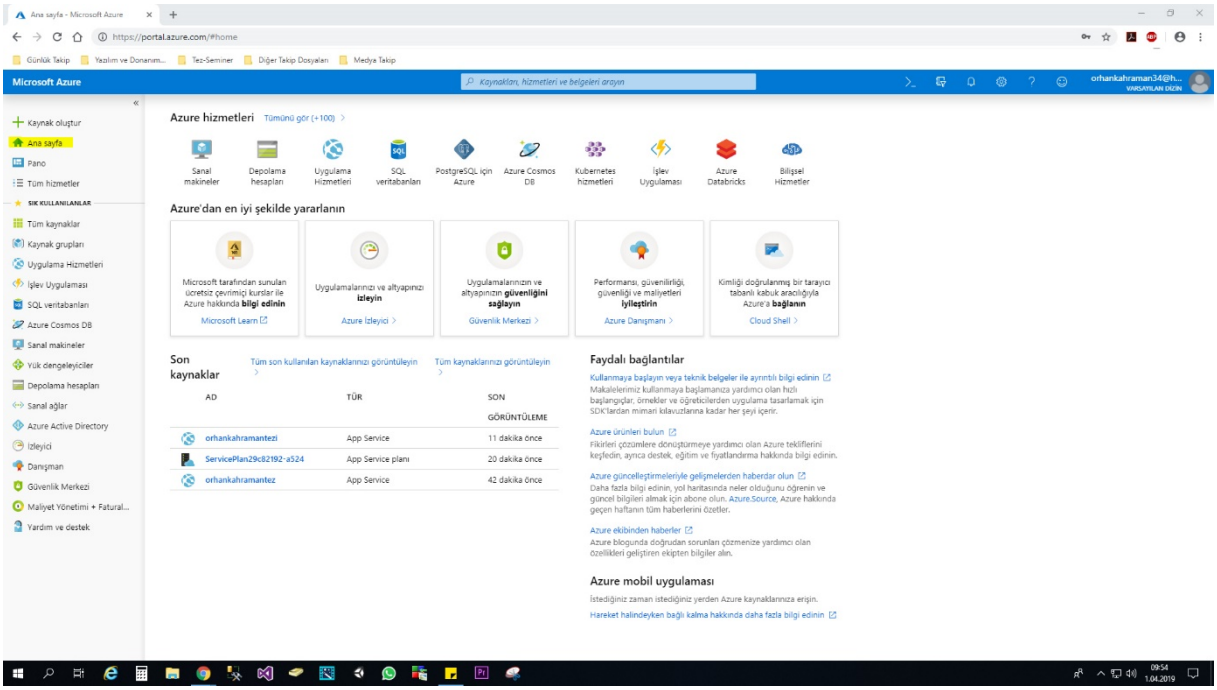


Şekil 8.8: Azure Sanal Makine Oluşumunda 8. Adım

Sanal sunucu kurulumu yapıldıktan sonra veritabanı kurulumu yapılası gerekmektedir. Veritabanlarının oluşumu ve kurgu işlemleri 4 ana başlık altında oluşturulmaktadır. Normal SQL kurulumundan çok daha basite indirgenmiştir. *Temel Ayarlar* kısmında Proje Ayrıntıları, Veritabanı ayrıntıları (veritabanı adı, sunucu(….@database.windows.net uzantılı olması gerekmektedir ayrıca sunucu yöneticisi oturum açma bilgileri, parola gibi değerlerin girilmesi gerekmektedir.)), SQL elastik havuzu(sabit bir bütçede birden fazla veritabanı kullanımına olanak sağlar) kullanımı istemi seçeneği, işlem ve depolama (işlemler için SQL veritabanı için en uygun katman ve performans seçeneği) gibi işlemlerin yapıldığı alandır. Bir sonra ki aşamada ise *Ek Ayarlar* kısmı kullanıcının karşısına çıkmaktadır. Burada kullanıcının varsa daha önceden oluşturduğu veritabanı bunların sanal sunucuya aktarım işlemleri yapılabilmektedir. Ayrıca gelişmiş veri güvenliği seçenekleri ile saldırılara karşı bir önlemde alınması gibi işlemleri kullanıcıya ücretler dahilinde sunar. Son olarak sanal sunucu oluşumunda da bahsi geçen Etiketleme ve Gözden Geçir + Oluştur sekmesinde de son işlemlerin ön izlemeleri yapılarak kurulum sonlandırılır.

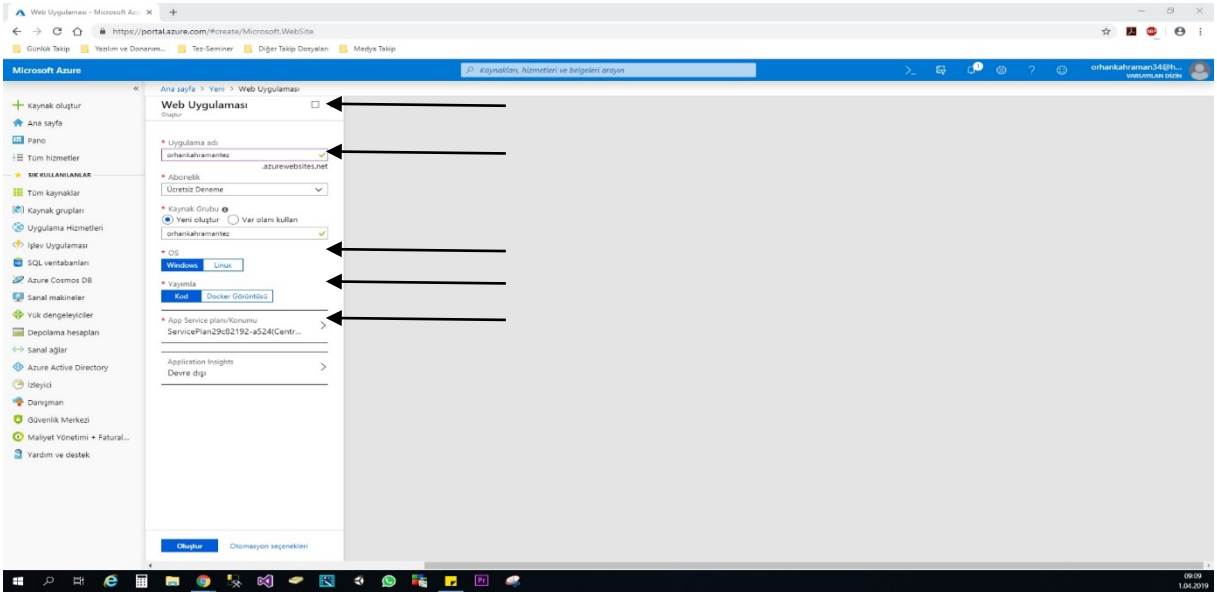
9. MİCROSOFT AZURE PLATFORMUNDA ÖRNEK BİR WEB SİTESİ KURULUMU

Microsoft Azure Platformunda üyelik işlemlerin yapılmasından sonra kolaylıkla web siteleri oluşumu yapılabilmektedir. Ayrıca hazır olan scripter(WordPress, Jomla, DasBlog, BlogEngine.NET) gibi şablonlardan da yararlanılabilir. Adım adım Microsoft Azure Platformunda bir web sitesi nasıl yapılır ve yayınlanır aşağıda gösterilmiştir.



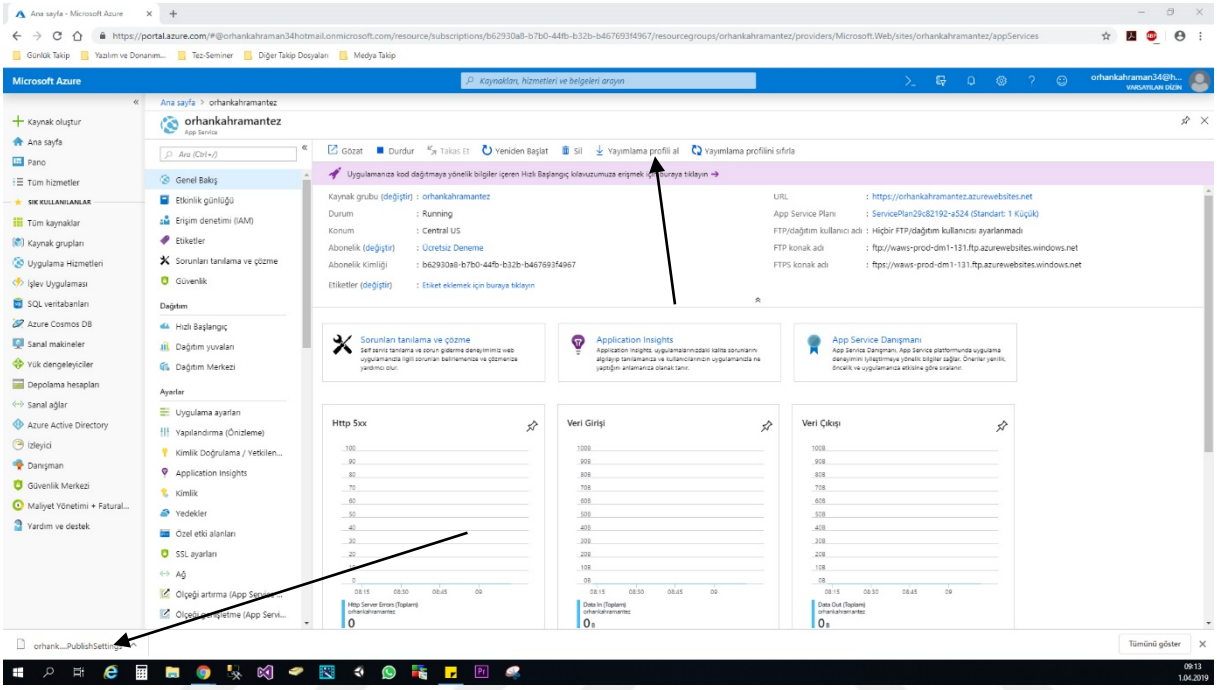
Şekil 9.1: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

Birinci adımda portala giriş yapmak gerekmektedir. Sol taraftan +Kaynak Oluştur Simgesine tıklayıp gelen ekranda Web App uygulamasına giriş yapılması gerekmektedir.



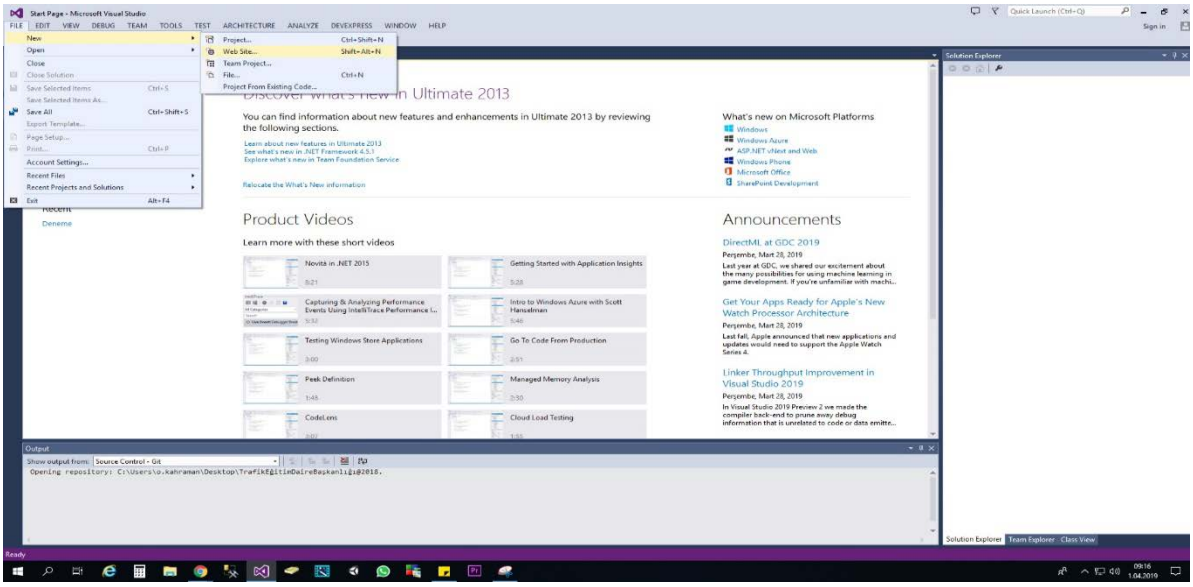
Şekil 9.2: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

İkinci adımda domain ismini vermek gerekmektedir. Ardından hangi host(Linux yada windows) tabanını kullanacaklarını seçip bir diğer adıma geçmek gerekmektedir. Ancak bilinmesi gerekir ki ilk verilecek domain ismi …..azurewebsitesi.net olarak görülecektedir. Bunun nedeni yeni yapılacak olan sitenin tam aktif edilene kadar gizli tutulmasıdır. Kullanıcılar tüm veri girişlerinden sonra web sitesine verilmek istenen ismi görebileceklerdir.



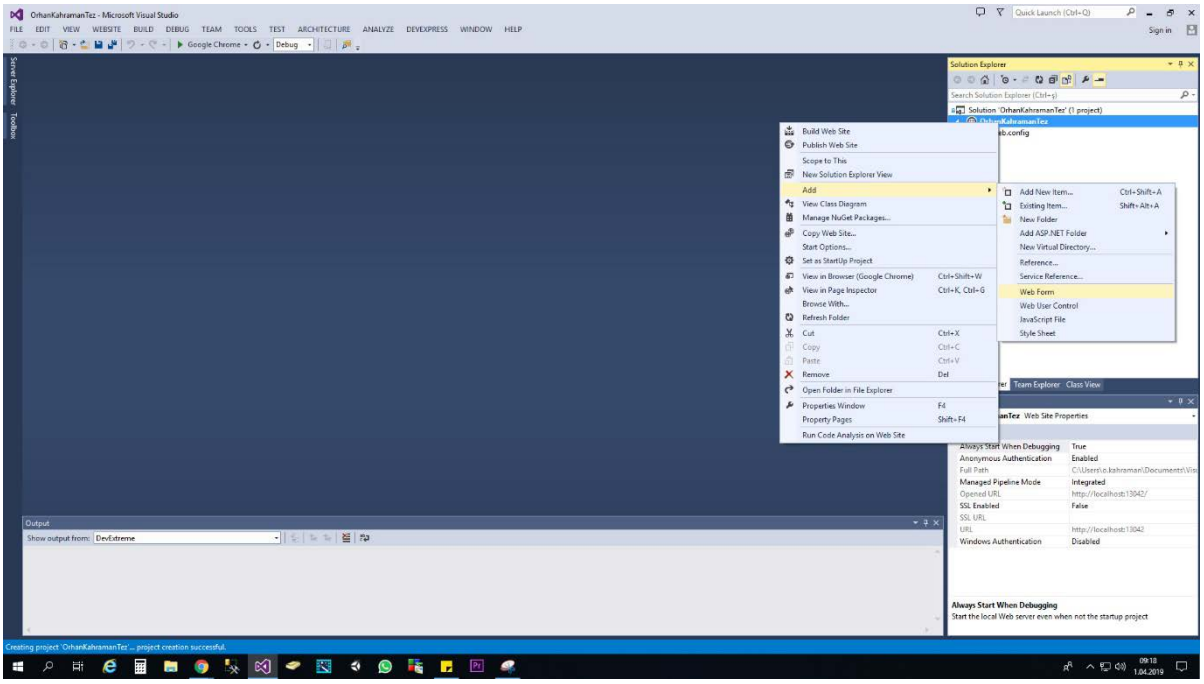
Şekil 9.3: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

Üçüncü adımda sanal sunucular üstünde bir yer açılmış oldu. Burada isimlendirdiğimiz domain artık *orhankahramantez.azurewebsitesi.net* olarak tamamlanmıştır. Ardından FTP bağlantılarına ait olan dosya Yayımlama Profilini Al sekmesinde oluşturulmuştur. Bu dosyayı indirmek gerekmektedir. Bu dosya Visual Studio tarafından hazırlayacağımız web sitesinin host edilmesi için gerekmektedir.



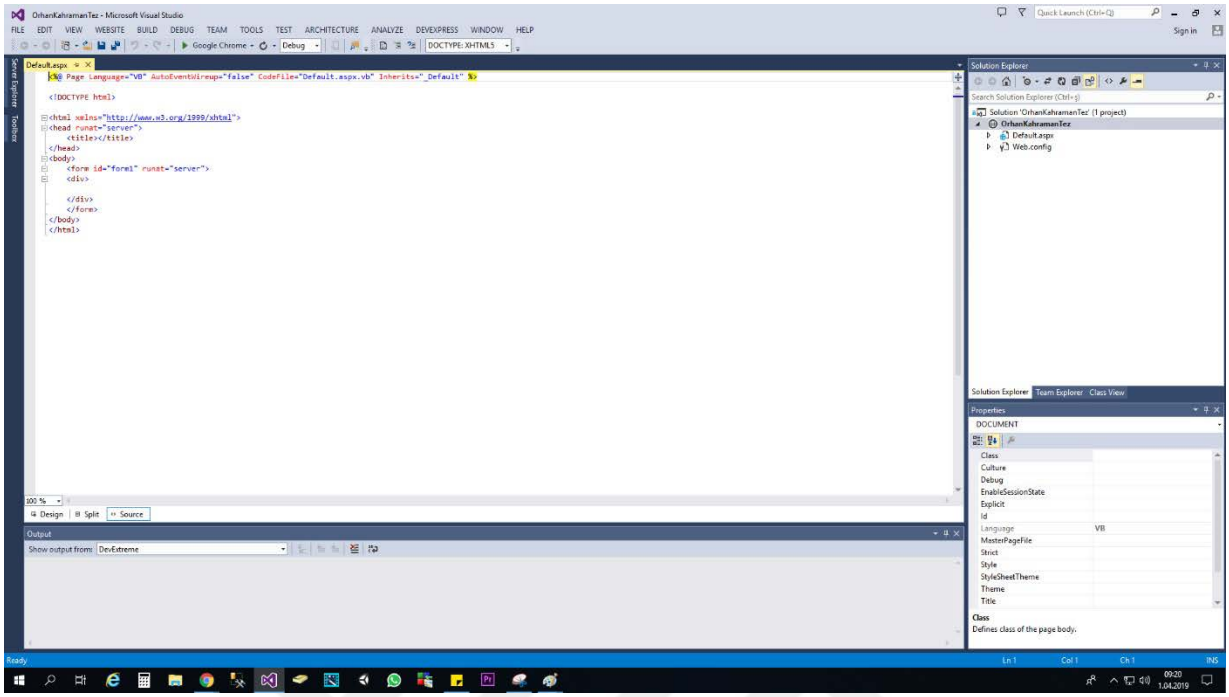
Şekil 9.4: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

Dördüncü adımda Visual Studio ortamında File-New-Web Site ekranlarından yeni oluşturacağımız projenin hangi kaynak yazılımında oluşumu yapılacaksa o seçilir. Örneğimiz de ASP.NET Empty Web Site bölümünden ilerliyoruz. İlerleme sonrasında karşımıza çıkan ekranın Solution Explorer bölümünde ismini verdiğimiz web class'ını sağ tıklayıp Add-Web Form eklemesi yaparak Web Sayfamızın ilk görünüm sayfasını oluşturuyoruz.



Şekil 9.5: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

Beşinci adımda oluşturulan Default.aspx dosyasının kaynak kod yazımına başlayıp ilk ekran sayfasının tasarımını yapıyoruz**.**



Şekil 9.6: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

Altıncı adımda tarım ve eklemelerini tüm ekran fonksiyonlarını çıkardığımız alan olarak son halini veriyoruz. Ardından da yayınlama için Azure ortamına host edilecektir. Yaptığımız sitenin ilk defaul sayfasının kaynak kodları ile birlikte ekran resmi aşağıda verilmiştir.

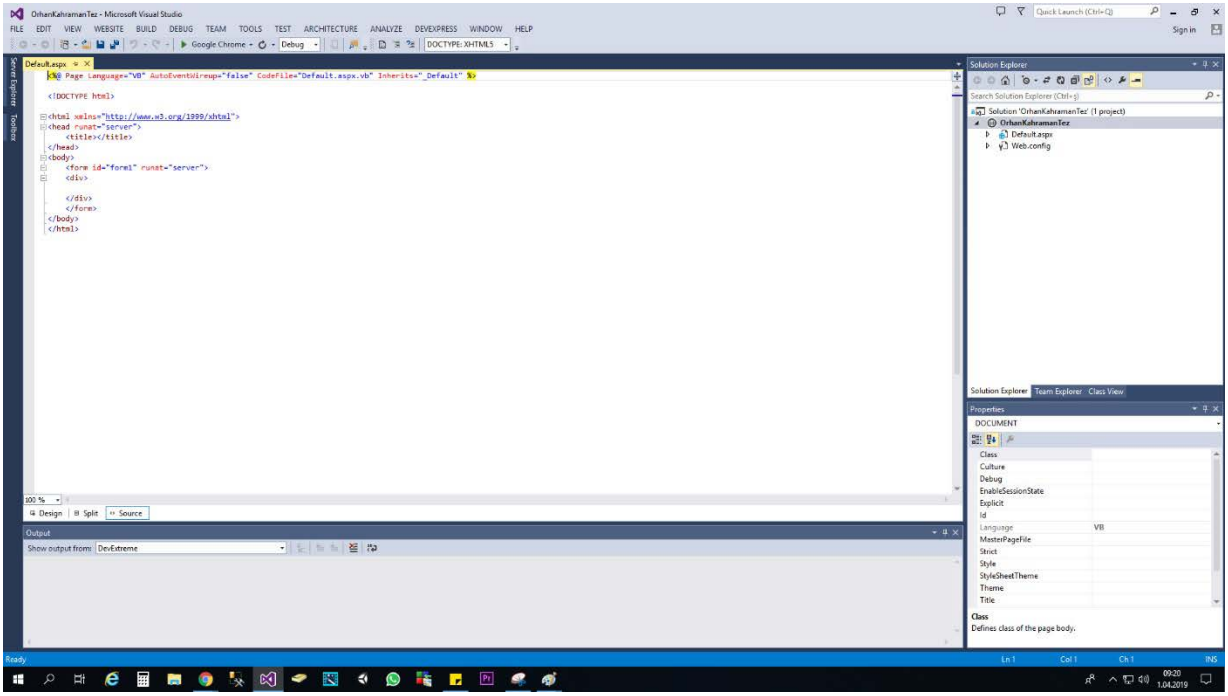
<%@ Page Language="VB" AutoEventWireup="false" CodeFile="Default.aspx.vb" Inherits="_Default" %>

<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
    <title></title>
</head>
<body>
    <form id="form1" runat="server">

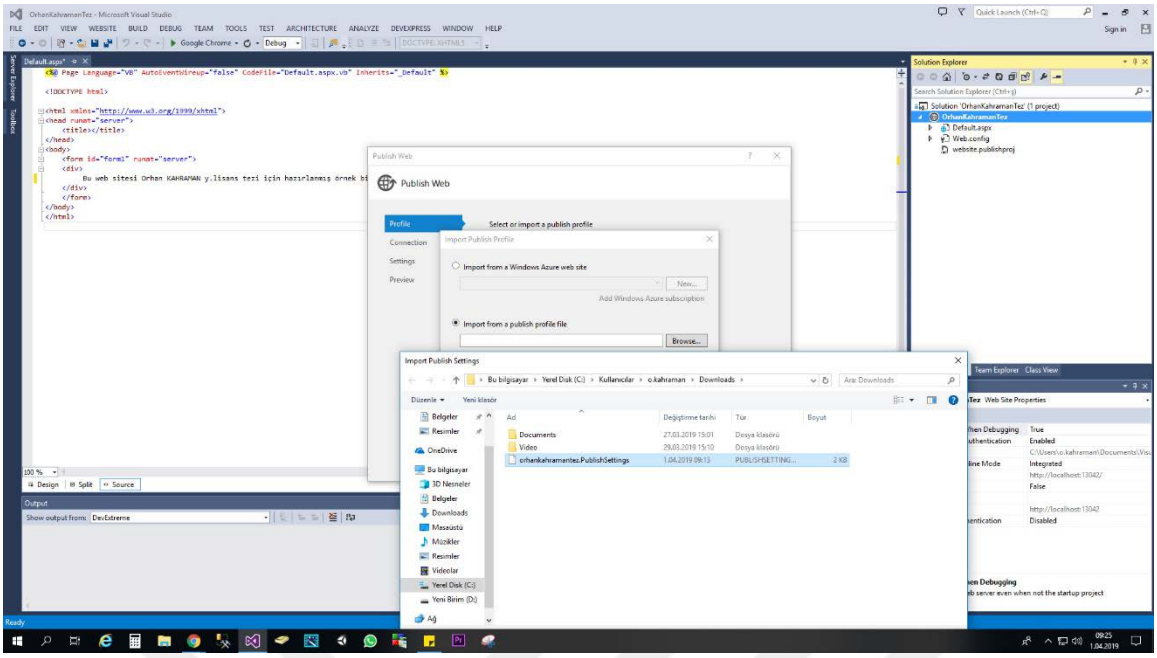
        Bu web sitesi Orhan KAHRAMAN y.lisans tezi için hazırlanmış örnek bir çalışmadır.

```
    </div>
    </form>
</body>
</html>
```



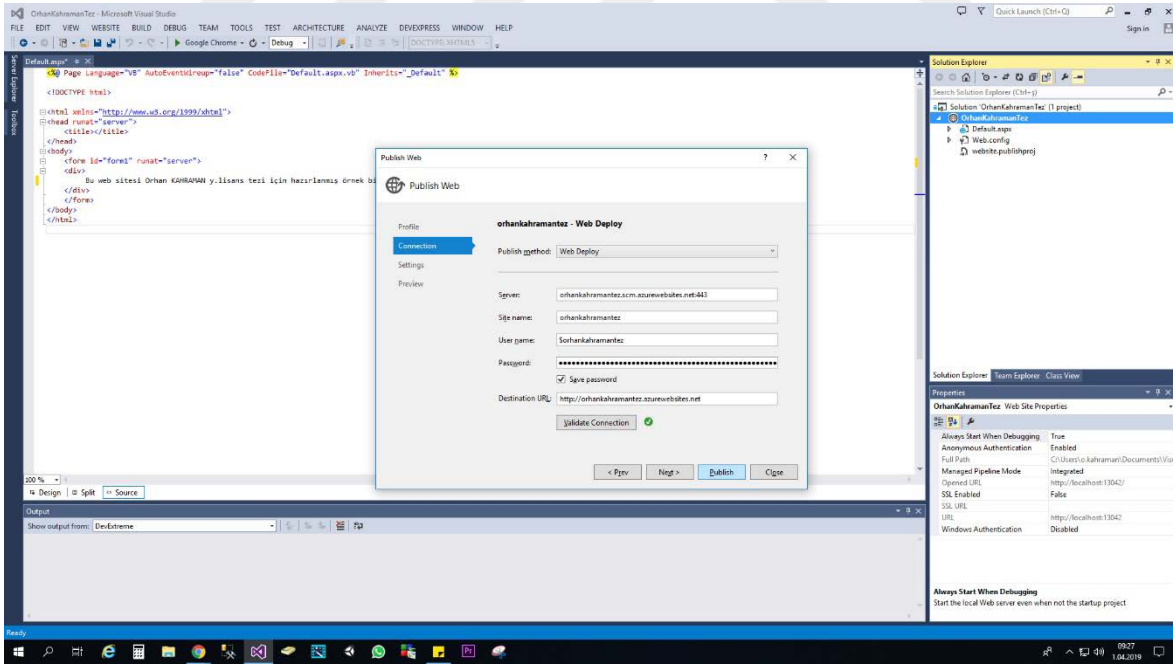
Şekil 9.7: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

Artık web sitemiz yayınlanmaya hazır konuma gelmiştir. Bu adımda Visual Studio programında Solition Exlorer ekranından web form(orhankahramanTez)'e sağ klik yaparak Publis Web Site diyerek bir sonra ki adıma geçiyoruz.



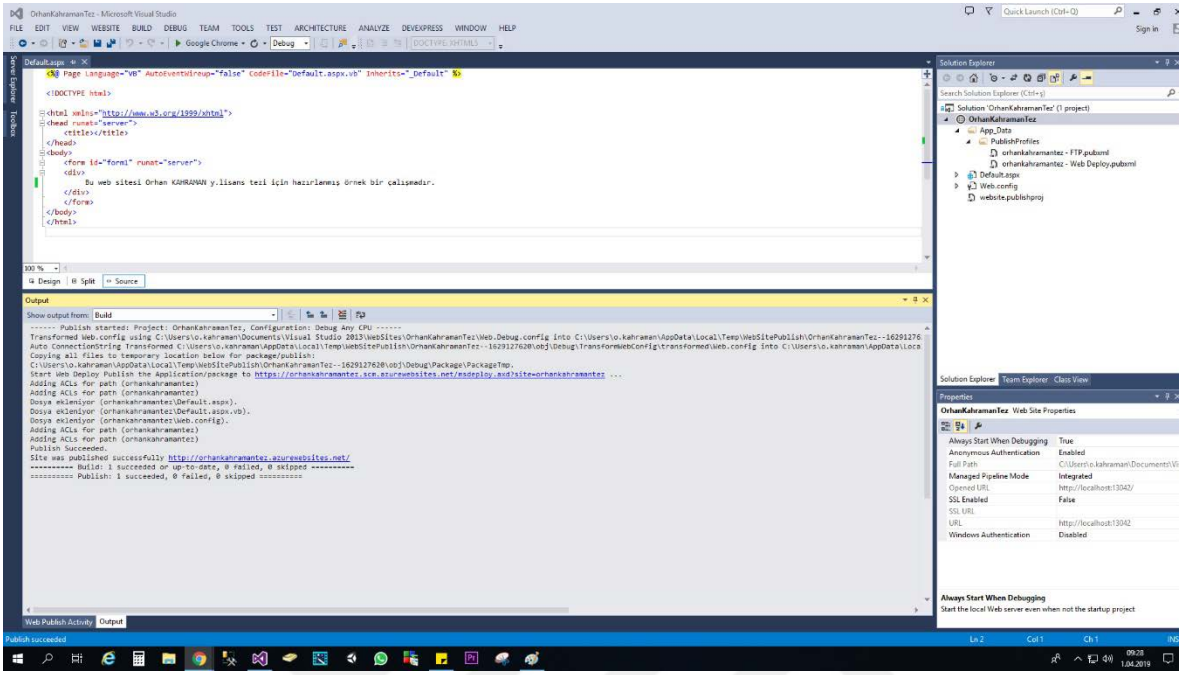
Şekil 9.8: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

Bir sonra ki adımda daha önceden Azure ortamında indirdiğimiz FTP dosyasını import... sekmesinden yol olarak gösteriyoruz.



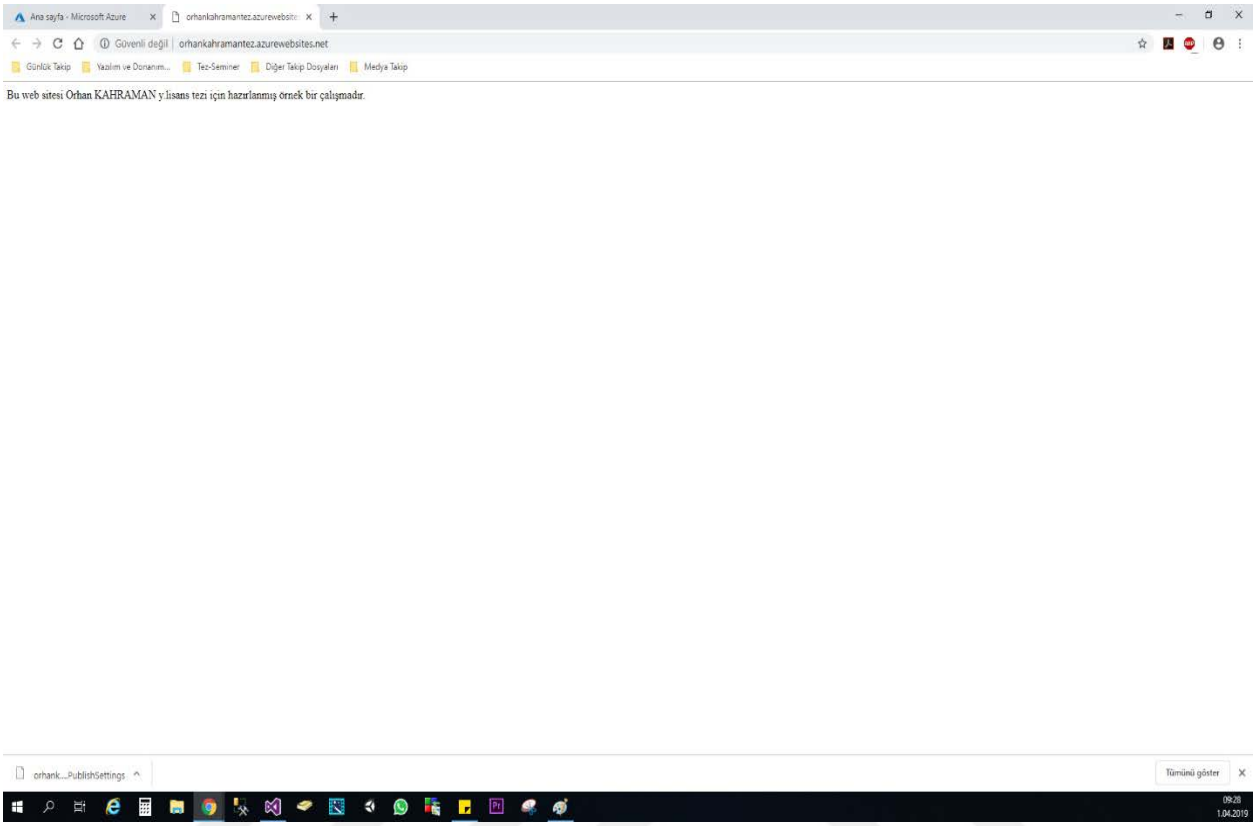
Şekil 9.9: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

Bir sonraki adımda ise otomatik olarak import edilen FTP dosyaları Validate Connection seçeneği ile kontrolünü sağlıyoruz.



Şekil 9.10: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

Dosyaları host etme işlemi burada başlamaktadır. Publish seçeneği tıklandıktan sonra host edilen dosyalar Visual Studio Ekranında görülecektir.



Şekil 9.11: Microsoft Azure Web Sitesi Kurulumu Ekran Görüntüsü

Bu işlemlerden sorna artık web sitemiz yayınlanmış olacaktır. Yükeleme işlemleri sonrasında otomatikmen web sitemiz açılacaktır.

10. SONUÇ VE ÖNERİLER

Bilgisayar ve internetin yaygınlaşmasıyla birlikte teknolojik gelişmeler hızlıca ilerlemektedir. Bilgisayar donanımlarının gelişmesi, iş ve işlemlerin hızlıca yapılmasına olanak sağladı ve işlem hacimleri TB(terabayt) düzeylerine ulaşmıştır. Dolayısıyla bilgisayarlar insanların yaşamlarının bir parçası haline gelmiştir.

Zaman ilerledikçe 2000'li yıllardan sonra bilişim hız ivmesini arttırmıştır. Dünyanın en büyük veri merkezlerinin temelleri bu zaman dilimlerinde atılmaya başlanmış ve rekabet ile iyileşmeler ve kullanıcı dostu arayüzleri sunmuşlardır. Tüm yaşantımıza yön verecek olan veri merkezleri kurumlarıyla tekstilden eğitime, otomotivden enerji sektörüne, evlerimizden işyerlerine kadar hizmet sağlayıcıları kullanılmaya başlanmıştır.

Ticari iş ve işletmeciler arge faaliyetlerini önemsek zorundadırlar. Eğer çalışmalarında güncelliklerini yitirirlerse piyasalardan değer kaybetmeleri kaçınılmazdır. Bu kapsamda bilişim sektörü günümüze kadar hızlı bir arge ivmesi yakalamıştır. Dolayısıyla bu gelişmelerden geride kalan kurum ve kuruluşların günümüz ve sonrasına ulaşmaları da zordur.

Bilgisayar donanımlarının ve yazılımlarının hızlı ilerleyişiyle beraber internet kullanımı da o kadar artmıştır. Bununla beraber sanallaştırma teknolojilerinin ortaya çıkmasıyla daha düşük ücret girdilerinde daha verimli bir iş yapabilme olanağı doğmuştur. Bu sayede hem maddi hem de esnek kullanılabilme gibi avantajlar kullanıcılara sunulmuştur.

İnternet teknolojisinin artması ve kullanımların tüm insanlar tarafından kabul görmesiyle birlikte, kurum ve kuruluşlar hizmetlerini müşterilerine kolay sunmak için veri ve kullanıcı bilgilerini internet ortamına taşımışlardır. Bunun sonucunda bilgilerin depolanması ve depolanan bilgilerin korunması gibi önemli güvenlik endişelerini ortaya çıkmıştır. Bunlarla başa çıkmanın kurum ve kuruluşlar için sorun oluşundan daha da önemli olanı kullanıcıların bilinçlendirilmesi, kullanılan yazılım ve donanımların lisanslı ve güvenilir olması, kullanıcı name ve password kullanımlarında güvenli (harf, rakam, noktalama işaretleri vb.) karma yapıları kullanımlarına teşvikleri ön plana çıkmaktadır.

Datalar hem kullanıcılar için hem de hizmet sağlayıcıları için önem arz etmektedir. Önemli olan her türlü bilgi çalınmaya, saldırılara maruz kalmaya gebedir. Bundan dolayı bir bilgiyi korumanın yoluda hukuksal düzlemden geçmektedir. Hukukun korumadığı bir düzenin açık saldırganları da çoktur. Ülkemizde hizmete sunulan hizmet sağlayıcıları kullanıcıların veri

kayıplarından kaynaklanabilecek sorun ve riskleri kabul etmemektedirler. Veri gizliliği ve ihlal edilemezliliği Türkiye hariç neredeyse bütün ülkelerde kabul edilmiş yasalarla korunmaktadır. ABD, İsveç, Avusturalya ve AB Ülkeleri hizmet sağlayıcı kurum ve kuruluşların kullanıcı bilgilerini korumalarına yönelim sorumluluklar yüklemişlerdir. Herhangi bir veri kaybında hizmet sağlayıcıları teminatlara maruz kalmaktadırlar ve kullanıcının veri kayıplarının önüne geçmek için mümkün olduğunca hizmet sağlayıcılarının aleyhlerine cezai yaptırımlar uygulamaktadırlar. Türkiye hukuk kurallarında ne yazık ki kullanıcıların veri kayıplarında ya da verilerine saldırılarında hizmet sağlayıcılarına yaptırım veya cazai işlem ön görülmemektedir. Bütün sorumluluk kullanıcılara yüklenmektedir. Genel anlamda hizmet sağlayıcıları yurt dışı kaynaklardan sağlandığında kullanıcılar itiraz etseler dahi yerel mahkemeler destek olamadıkları için ne yazık ki kullanıcı aleyhine sonuçlar çıkmaktadır.

Bulut bilişimin ortaya çıkmasıyla birlikte şirketlerde sınırlı olan nitelikli personel, veri merkezi donanımları, bakım maliyetleri gibi sorunların önüne geçmek daha kolay olmuştur. Kurum ve kuruluşlar bu yönde yapabilecekleri sınırlı olan yatırımlarının ekonomik olarak daha minimize düzeye indirmektedir. Ayrıca kurum içerinde sistem odalarının oluşturulması, güç kaynakları, jeneratörlerin bulundurulması, bunların güvenlik önlemlerinin alınması, yangın ve sel gibi afetlerin önlemlerinin alınması, dış kaynaklardan nitelikli eleman istihdamı gibi iş ve işlemleri önüne geçmektedir. Bulut bilişim teknolojisi hizmetleri sayesinde kurumlar ihtiyaçları doğrultusunda kaynak kiralımı yaparak büyük tasarruf ve kolaylıklardan faydalanabilmektedirler.

Dünyanın her yerinde günümüzde internet kullanımı mevcuttur. Kimi ülkelerde internet kullanıcı oranları %99'leri bulurken Türkiye'de bu oran, Türkiye İstatistik Kurumu verilerine göre 2013 ile 2017 yılları arasında internet erişimine sahip olan firma sayısı %95.2'yi, web sayfası sahiplik oranı ise %65.5 olarak görülmüştür. Hane halkının internet kullanım oranı %49.1'den %80.7'e yükselmiş ve Bilgisayar kullanım oranları da 97.2'ye yükselmiştir[43,44]. Bu yükselmeye paralel olarak internet bant genişlikleri de artmıştır. Yapılan araştırmalar da internet üzerinden sanal alışveriş olanaklarının artmasıyla birlikte kurum ve kuruluşların yanında kişilerde bu kolaylıklardan hızlıca yararlanmaktadırlar.

Akıllı mobil telefon kullanımı günümüzde kullanımı çok yaygın bir araçtır. Dünya geneli 2018 Ocak ayı toplam nüfus 7.593 milyar olarak raporlanmış ve 4.021 milyar insan internet kullanıcısı, 3.196 milyar aktif sosyal medya kullanıcısı, 5.135 milyar cep telefonu kullanıcısı, 2.958 milyar aktif akıllı cep telefonu kullanıcı oranları verilmiştir[45]. Bu raporda Türkiye'de ki kullanım oranları ise 82 milyon nüfus oranının 54.3 milyonunun aktif internet kullanıcı

olduğu ve mobil internet kullanıcı sayısının da 51.5 milyon olduğu araştırmalar sonucunda elde edilmiştir.

2009 yılından itibaren bu hızlı gelişimin Türkiye'de 3G teknolojisinin kullanımı sayesinde olmuştur. 3G teknolojisi mobil kullanıcılar için dönüm noktası olmuştur. Ancak kullanım ihtiyaçlarına tam anlamıyla hizmet veremeyen 3G teknolojisin yerini kısa süre sonra yani 2016 yıllında 4,5G teknolojisine bıraktı. Bu kullanıcılar için veri kullanımını neredeyse 2 katına hatta 3 katına çıkarma olanağı sağladı. Kullanıcıların bu ilgisi BT yatırımlarının artmasına ve bulut tabanlı verilere erişim gerekliliğini doğuran olumlu sonuçlardan olmuştur. Ulaştırma Denizcilik ve Haberleşme Bakanlığının 2020 yılının başlarına kadar 5G teknolojisinin Türkiye'ye getirileceğinin hedeflemiştir. Bunun sayesinde Türkiye'de erge çalışmalarının hızlanması ve alt yapı hızlandırma çalışmalarının süratle ilerleyeceği öngörülmektedir.

Türkiye'de bilişim pazarının büyüklüğü 116.9 milyar TL, Türkiye merkezli üretici donanımsal olarak 1.6 milyar TL, Türkiye merkezli üretim yazılım olarak 1.9 milyar TL, Türkiye merkezli üretici hizmet olarak 397 milyon TL rakamlarıyla çok büyük yol almıştır. Ayrıca Türkiye'de bilişim pazarı büyüklüğü aşağıda detaylandırılmıştır[46].

- Sistem entegratörü = 8.1 Milyar TL
- Hizmet Sağlayıcı = 5.9 Milyar TL
- Uluslararası Merkezli Üreticinin Türkiye Temsilcilerini = 8.5 Milyar TL
- Dağıtıcı = 27.1 Milyar TL
- Telekom Şirketi =48.8 Milyar TL
- Ağ Donanımı = 1.4 Milyar TL
- Masaüstü Bilgisayar OEM = 2.3 Milyar TL
- Mobil Telefon Dağıtıcısı =12.4 Milyar TL
- Tablet ve Taşınabilir Bilgisayar Geliri =2.5 Milyar TL
- Telekomünikasyon Altyapı Donanımı = 996 Milyon TL
- Görüntü ve Ses Sistemleri =1 Milyar TL
- İş Uygulamaları – Yazılım =597 Milyon TL
- Sanallaştırma Yazılımları = 76 Milyon TL
- Güvenlik Yazılımı = 740 Milyon TL
- Sektörel Yazılım = 2.3 Milyar TL
- Çağrı Merkezi Geliri = 1.5 Milyar TL
- İnternet Hizmeti = 5.4 Milyar TL

- Donanım İhracatı = 998 Milyon TL
- Yazılım İhracatı = 528 Milyon TL
- Hizmet İhracatı = 451 Milyon TL

10. Kalkınma planı olan 2014-2018 yıllarını kapsayan zaman diliminde BT Pazarlarının paylarında artış hedeflenmektedir. Bu Pazar payı %23 olarak lanse edilmiştir. Pazar payının diğer gelişmekte olan ülkeler sıralamasının üstünde olduğu ancak yetişkin beyin gücünün dışarıya kaçmasından dolayıda istenilen seviyelere gelmenin zor olduğu görülmektedir. Bunun önüne geçmek için son zamanlarda yazılım firmalarına arge için destek ödemelerinin verildiği, üniversitelerin teknoloji merkezlerine önem verdiği de çalışmalar arasında olumlu bir çizgi grafiğini çizmektedir.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) önderliğinde bilişim alanında arge çalışmalarına katkı ve maddi destek sağlamaya yönelik çalışmalar 2010'lu yıllardan sonra hız kazanmıştır. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) iş birliği ile bilişim alanlarında işler yapan kurum kuruluş ve kişilerin bir araya gelerek projlerini tanıtmalarına, gerekli olan açık desteklerin alınmasına, varsa teknolojilerin ortak çatılarda ilerleyişlerine öncülük etmektedir.

Dünyanın ilk yazılım şirketlerinden olan Microsoft yazılımlarının muadillerini üretmek, kendi yazılımlarımızla dünyada söz sahibi olmak için Pardus işletim sistemi ortaya çıkarılmıştır. Açık kaynak yazılıma sahip olan bu işletim sisteminin gelişimi ile uluslararası alanda kendimize ait yazılımlarımızla Microsoft gibi şirketlere milyarlarca dolar gibi değerlerinde ülke içinde kalması amaçlanmıştır. Pardus işletim sistemin yapılabilirliği sayesinde türk yazılımcılar savunma sanayisinde gelişmeler sağlamışlardır. Tüm dünyada kullanılan tekel yazılımların güvenliği olumsuz yönde etkilediği, savunma ve saldırı bilgilerinin yazılım sahiplenin eline geçtiği bilinmektedir. Bunun önüne geçmek için İHA (İnsansız Hava Araçları), Siha (İnsansız Silahlandırılmış Hava Araçları), helikopter, uçak, tank gibi savunma sistemlerinin yerli ve milli imkanlarla yapılması önem arz etmektedir.

Türkiye'de bulunan teknoloji ve internet servis sağlayıcıları artık bulut teknolojilerini kendi bünyelerinde oluşturmaya ve kullanıcılara sunmaya başlamışlarıdır. 2018 yılı verilerine bakıldığında Türk Telekom internet ve mobil servis sağlayıcısı olan firma bu konuda diğer firmalardan önde giderek kendi alt yapısıyla bulut çözümleri sunmaktadır. Türkiye'de faaliyet gösteren Vodafone ve Turkcell gibi firmalarda bulut teknolojisi mantığında depolama hizmetleri sunmaktadırlar. Kullanıcılarının verilerine (kişiler, takvim, fotoğraflar ve

videolarına) mesafe ve cihaz farkı olmadan kullanıcıların erişimine olanaklar sağlamaktadırlar. Ancak ülkemizde her ne kadar gayret gösterilse de bu teknolojilerin üretilmesine Google(Google Drive) ve Microsoft(Windows Azure ve Microsoft Office) gibi sektörün büyük şirketlerine ulaşmamız daha çok zaman isteyecek gibi görünmektedir.

Bu tez çalışmasında bulut bilişimin küresel gelişimi ve Türkiye'de ki kullanım ve üretimlerine değinilerek farkındalık hedeflenmiştir. Bu doğrultuda tez kapsamında teknik bilgiler verilmiştir. Dünyada ve Türkiye'de ki yapılan çalışmalara değinilmiş ve bunların örneklemler üzerinde teknik bilgileri verilmiştir. Bulut teknolojileri alanlarında yapılan çalışmalar ve yatırımların son yıllarda daha da fazla üzerinde durulduğu görülmüştür. Bu kapsamda oluşan sorun ve problemleri azaltmak, bulut bilişim teknolojilerinin güven içinde kullanımını sağlamak, sürdürülebilir bir yapı ortaya koymak için gerekli bir takım önlemlerin alınması gerekmektedir.

- Türkiye'de bulut bilişim sistemlerinin kullanımlarının daha güvenli olması için, ABD, Çin, Japonya, AB Ülkeleri gibi ülkelerle iş birliği sağlamak, bunların bu tür iş ve işlemlerin güvenlik ve hak ihlalleri için yaptığı yasaların kapsayıcılığına Türkiye'yi de eklemek gerekmektedir.
- Hizmet sağlayıcılarına sorumluluklar yüklenmelidir. Üst düzey kimlik doğrulama ya da haberleşme protokollerinde iyileştirmeler sağlamak adına yapılmalıdır.
- Kullanıcıların bu platformlarda daha güvenilir kullanımlar sağlayabilmeleri adına arayüzlerinde kullanıcı dostu çalışmalar yapmaları gerekmektedir.
- Bulut bilişim sektörlerinde hizmet veren sağlayıcıların denetlenmeleri kesinlikle gerekmektedir. Denetimsiz bir bilişim yapısı sonu olmayan zararlar doğurabilir.
- Hizmet sağlayıcıların veri güvenliği için Uluslararası geçerliliği olan algoritmalar kullanması ve bunu kullanıcılarına zorunlu sunması gerekmektedir. Şu an kullanıcılara ayrı fiyatlandırmalarla sağlanmaktadır.
- Hizmet sağlayıcılarına sertifika zorunluğu getirilmelidir. Dolayısıyla kullanıcılar devlet kontrolünde olan bir mimari oluşumu kullanmaları daha güven sağlayacaktır.
- Hizmet sağlayıcılarının ülkemizde olanlarının uluslararası hizmet veren diğer firmalarla ortaklık ve bilgi alışverişi yapmaları gerekmektedir. Gelişim ve ileri mimari için çok önem arz etmektedir.
- Üniversiteler bünyesinde hizmet sağlayıcıları eğitimleri verilmeli, kullanıcı ve üretici bilgilendirmeleri yapılmalıdır. Hatta şirketlere eğitimler verilmelidir.

- Veri merkezlerinin ülkemizden tüm dünyaya dağıtılması gibi hedefler olmalıdır. Devlet kurum ve kuruluşların burada yatırımlarına olağan bir teşvik sağlamalıdır.
- Yerli ve milli becerilerle yapılacak olan bütün yatırım kaynaklarına devlet kesinlikle ve kesinlikle yer, enerji, personel vb. destekler vermelidir.
- İnternet hız problemlerinin önüne geçmek için geniş bant internet hatlarının çekilmesi ve 5G teknolojisi alt yapısının hızlanması gibi işlemlerin yapılası gerekmektedir.
- En önemlisi e-Devlet gibi platformlara yatırım yapılmalı ve kullanıcıların zaman ve mekan tasarruflarına olanak sağlayıcı arge çalışmaları ortaya konmalıdır.

Bulut tabanlı sanallaştırma işlemlerinde ciddi olarak yatırımların yapılması gerekmektedir. Sanallaştırma teknolojilerinde bir donanımı birden fazla parçalara ayırma prensibi kullanıcıların kendi kullanımları kadar kullanım yapma olanaklarına olanak sağlamaktadır. Zaman ve donanım konusunda bu şekilde iş ve işlemlerin Türkiye gibi küresel anlamda büyüme hedefi olan ülkelerin üzerinde durması gerek bir olay olarak karşımıza çıkmaktadır.

Çalışmada saldırı tespit sistemlerine değinilmiştir. Saldırı tespit sistemlerinin gelişim, kullanımı ve hizmet sağlayıcılarının kullanıcılara yönelik saldırıları engellemelerine yönelik çalışmalar dünya genelinde artmaktadır. Gelişen teknikler saldırılara karşı koyma açısından önem taşımaktadır. Bilinmelidir ki saldırganlarda o derece taktik geliştirmektedirler. Türkiye saldırı tespit sistem yazılım ve donanımlarını tam olarak üretememektedir. Bu sebeple saldırılara karşı koruyucu önlemleri almakta gecikebilmektedir. Siber yazılım ve uygulama firmaları genel anlamda sizi korumayı hedeflemezler çünkü amaçları para kazanmaktır. Saldırıları bazen kendileri yaparlar ki kullanıcılara kendilerine bağımlı hale getirmek isterler. Ayrıca saldırılardan korunan veri tabanlarının erişim hakkında devletler saldırı tespit sistemlerini satan firmalarla paylaşmak zorundadırlar. Türkiye'nin en kısa zamanda saldırı tespit cihaz ve yazılımlarını üretmesi ve kendisini savunacak duruma gelmesi gerekmektedir. Çözüm ise gerekirse dünyanın her yerinden nitelikli eleman teminine gitmelidir. Yetişmiş beyinlerden kendini dünyanın en büyük üretici devletleriyle rekabet edecek seviyeye getirmelidir.

Bulut sistemler üzerinde bir tane Web sitesi, sanal makine kurulumu ve sanal sunucu üzerinden birer tane uygulama kurulumu gerçekleştirdik. Windows Azure platformunda kurulumunu yaptığımız ve PaaS hizmetlerinde donanım ve yazılım sanallaştırma platformunda gerçekleştirdik. Burada ücretsiz deneme sürümünde *orhankahramantez* adında bir kaynak grubu oluşumu yapıldı. Sunucu adı orhan, Bölge Doğu ABD, İşletim Sistemi Windows Server

2012 R2 Datacenter, Boyut 1vcpu, 3.5 GB bellek, kullanıcı adı *orhankahramantez* olarak ayarlamalar yapıldı. Disk yapılandırma işlemlerinde Disk türü Premium SSD ve boyut olarak 1023 GİB disk yapılandırması yapıldı. Sanal ağlar yapılandırma işlemlerinde NIC ağ güvenlik grubundan yararlanılarak ayarlamaların Azure ortamında otomatik yapılması sağlandı. Yük denge havuzunun gerek olmadığı ve yapacağımız işlemlerin sınırlı olmasından dolayı kapalı tutulmuştur. Bu şekilde yaptığımız çalışmamızda sanal sunucunun yapılandırılması işlemleri yapılmıştır. Bağlantı dosyası kurumu sağlanmış ve diğer fiziksel sunuculardan daha verimli bir performans sağladığını tespit etmiş bulunmaktayız.

Sanal makine kurulumundan sonra SQL veri tabanı oluşumu gerçekleştirdik. Yaptığımız örnek veritabanı ve eklemelerde bulunduğumuz dosyalara sorunsuzca ve hızlıca erişim sağlanmıştır. SQL veritabanı kurulumundan sonra web sitesi kurulumu gerçekleştirdik. Windows Azure portalında yaptığımız web sitesi kurulumunda *orhankahramantez.azurewebsites.net/* domain ile host edilmiştir. Windows masaüstü ve mobil cihazlar üzerinden testler yapılmıştır.

Windows Azure ortamında sanallaştırma, SQL hizmetleri, hosting hizmetleri, hazır şablon kullanımları gibi birçok özelliklerde kullanıcılarına hizmet vermektedir. Kullanıcılar kendi veritabanlarını oluşturabilir, sanallaştırma teknolojisi sayesinde istediği boyutta VM kurulumu yapabilir ve kiralayabilirler. Ayrıca şirketlerin veri merkezi kurma, personel çalıştırma, güvenlik önlemlerinde profesyonel destek alma vb. iş ve işlemlerinde kolaylıklar sağlamaktadır. Yaptığımız çalışmada bu özellikler ve işlevleri test edilmiştir.

Bulut bilişim ve Microsoft Azure ortamında yapmış olduğumuz çalışma ile bulut teknolojisi mimarisi üzerinden Azure ortamında geliştirilen uygulamanın, yazılım katmanıyla kullanıcılara aktarılması işlemlerini yaptık. Bulut bilişim teknolojisinin kullanımı sayesinde işlemlerin daha pratik ve maliyetsiz yapılabildiğini çalışmalarımızda test etmiş bulunmaktayız. Ayrıca verilen yüksek maliyetlerde ki yazılım ücretlerinde da kolaylıkları sunduklarını test ettik.

Yapılan çalışmada Türkiye'de bulut bilişim ve alt yapı çalışmaları incelenmiş ve sektörün en büyük sistem bulut hizmet sağlayıcılarından olan Microsoft Azure ile Türk kullanıcılar lehine ve aleyhine veriler çıkarılmıştır. Yetişmiş nitelikli iş gücüne değer verilmediği, ücret politikalarının gelişmiş ülkelere nazaran çok düşük olması, alt yapı hizmetlerinin çalışmalar için yeteli olmaması vs. gibi birçok etken gelişmiş olan ülkelere beyin göçünü arttırmaktadır. Ülkemizde yerli hizmet sağlayan bulut bilişimin kuruluşları kullanıcılar için çok büyük etki yaratmamaktadır. Hem kullanım hem de mali yönden büyük uluslu şirketlerin kullanıcılara

sunduğu hizmetler ilgi görmektedir. Sebep olarak güvenlik kaygısı, yazılım ve donanım üretiminin ne yazık ki ülkemizde çok teknik olarak yapılamayışındandır. Türkiye'nin bu sektörlere yatırım yapması, yetişmiş beyinlerin göçünü engelleyecek politikalar hedeflemesi, alt yapı ve üst yapı destelerini hızlandırması, ulusal ve uluslararası hukuksal normlarını düzenlemesi ve bunları yürürlüğe acilen sokması gerekmektedir. Yeni hizmet sağlamaya yönelik yapılan çalışmalara gerekirse kamu kurumlarından destekler verilmesi, güvenlik zafiyetlerini ortadan kaldıracak siber güvenlik yazılımları temininde destekler sağlaması gibi firmaların gelişimine katkılar sunulmalıdır.

Bulut bilişim nükleer çalışmalardan radar cihazlarına, medikal cihazlardan günlük kullanılan muhasebe programlarına kadar hizmet sağlayabilen bir yazılım hizmetidir. Çalışmada AB, ABD, Japonya gibi ülkelerin çeşitli teşviklerle yazılım ve donanım üreticilerine büyük mali destekler verdikleri görülmüştür. Türkiye'de bulut bilişim hizmet sektörünün gelişmesi ve hizmetlerin uluslararası boyuta taşınması kolay değildir. Çünkü büyük sermaye ve birikime sahip yazılım şirketlerinin ARGE çalışmalarına milyonlarca dolar ayırması, nitelikli elaman sayılarının çokluğu, geçmişten gelen bilgi birikimleri hafife alınamaz bir olgudur. Ancak aşağıda sıraladığımız çalışmalar planlı bir şekilde yapılırsa ekonomik olarak büyük olan sektörden bir pay alabiliriz.

- Alt yapı ve üst yapı çalışmalarının gelişmiş ülkelere göre tasarlayıp yenilenmesi çalışmalarının hızlanması
- İnternet bant genişlikleri hızlandırılması
- Yetişmiş yazılımcıların yurt dışından geri gelmeleri sağlanması
- Siber güvenlik tehlikelerine karşı yurt dışından alınan yazılımların yurt içinde muadilleri yazılmalıdır. Güvenlik zafiyetlerini en aza indirmeye yönelik çalışmaların yapılması
- Hukuksal normların en kısa zamanda diğer ülkeler hukuk normlarına ters düşmeyecek şekilde düzenlemesi çalışmalarının yapılması
- Yatırımcılara mali destek sağlanması
- Sanayi ve Teknoloji Bakanlı ile Bilgi Teknolojileri ve İletişim Kurumu Başkanlıklarının yazılım geliştiren şirketlere yurt dışında eğitimlerini sağlayıcı destekler planlamalarının yapılması
- Gereken yurtiçi ve yurtdışı reklam tanıtımların yapılması

Yukarıda çalışmamızda Türkiye'de bulut bilişim sektörünün Google, Amazon, Windows gibi büyük hacimli firmalarla yarışabilmesi için gerekli maddeler sıralanmıştır. Bu maddelerin

sonuçlanmasında hedef siber saldırılara karşı yerli yazılım ve donanımlarla karşılık verebilmek, dünyada yazılımında söz sahibi olabilmek ve son zamanların en prestijli sektörü bulut teknolojisi hizmet sağlayıcıların arasına girebileceği hedeflenmektedir.

KAYNAKLAR

[1] J. Moar, “Wearables:smart chic or smart hype?” Juniper Research Ltd., 2014.

[2] Bulut Bilisim Hizmet Modelleri http://tr.wikipedia.org/wiki/Bulut_bilişim

[3] Furht, B.,Escalante, A., 2010, Handbook of Cloud Computing, Springer, New York, ABD

[4] Ahmet Albayrak 2015, Bilgisayar Ağlarında Güvenlik Politikaları ve Bulut Bilişim

[5] Marshall D., Beaver S. S., McCarty J. W., 2009, VMware ESX: Essentials in the Virtual Data Center, CRC press.

[6] Bourguiba M. ve El Korbi I. (2014), Improving Network I/O Virtualization for Cloud Computing, IEEE Transactions On Parallel And Distributed Systems, (Cilt 25, Sayı 3, Sf.673-681), Mart 2014.

[7] Peng L. ve Mohammed T. (2008), Integration of Virtualization Technology into Network Security Laboratory, Frontiers in Education Conference (FIE), (Cilt 38, Sf. 7-12), Ekim 2008.

[8] Laadan O. ve Nieh J. (2010), Operating System Virtualization : Practice and Experience, In Proceedings of the 3rd Annual Haifa Experimental Systems Conference (SYSTOR '10), (Cilt 17, Sf. 12), 2010.

[9] M. Çalışkan Sanallaştırma Teknolojilerinin Saldırı Tespit Ve Önleme Sistemlerinin Performansı Üzerine Etkisi, haziran 2014

[10] Finn A., Lownds P., Luescher M. ve Flynn D. (2012), Windows Server 2012 Hyper-V Installation and Configuration Guide. Sybex, Indiana, Mart 2013.

[11].VMWare ESX and VMWare ESXi, http://www.vmware.com/files/pdf/VMware-ESX-and- VMware-ESXi-DS-EN.pdf , son erişim: Mayıs 2015.

[12]. VirtualBox, https://www.virtualbox.org, son erişim: Mayıs 2015.

[13]. Powers S., Readers’ Choice Awards 2014, 2 Aralık 2014, http://www.linuxjournal.com/rc2014?page=16, son erişim: Haziran 2015.

[14]. Barham P., Dragovic B., Fraser K., Hand S., Harris T., Ho A., Neugebauer R., Pratt I., Warfield A., 2003, Xen and the art of virtualization, ACM SIGOPS Operating Systems Review, 37, 5, 164-177.

[15]. Bellard F., 2005, "QEMU, a fast and portable dynamic translator". USENIX.

[16]. Kirch J., Eylül 2007, Virtual machine security guidelines. The center for Internet Security, http://www.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf.

[17]. Teneyuca D.,2011, Internet cloud security: The illusion of inclusion, Information Security Technical Report, doi:10.1016/j.istr.2011.08.005.

[18]. Öğretmen F.D. Temmuz 2015, güvenli bulut bilişim için saldırı tespit sistemleri ,s.32,

[19]. Kumar, A., Kumar, V., Singh, P., & Kumar, A., 2012, A Novel approach: Security measures and Concerns of Cloud Computing. International Journal of Computer Technology and Applications, 3(3), 1008 -1014.

[20]. Scarfone K., ve Mell P., 2007, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94 (SP800-94), National Institute of Standards and Technology, Gaithersburg.

[21]. Marinova-Boncheva V., 2007, A short survey of intrusion detection systems, Problems of Engineering Cybernetics and Robotics, 58, 23–30.

[22]. Trusted Computing Group, http://www.trustedcomputinggroup.org/, son erişim : Haziran 2015.

[23]. Kong J., 2010, Protecting the confidentiality of virtual machines against untrusted host, International Symposium on Intelligence Information Processing and Trusted Computing (IPTC), Çin, 364.

[24]. Kong J., 2011, AdjointVM: a new intrusion detection model for cloud computing, Energy Procedia, 13, 7902-7911.

[25]. M. Çalışkan Sanallaştırma Teknolojilerinin Saldırı Tespit Ve Önleme Sistemlerinin Performansı Üzerine Etkisi, haziran 2014

[26]. Columbus L., 2014, Predicting The Future Of Cloud Service Providers, http://www.forbes.com/sites/louiscolumbus/2015/04/05/predicting-the-future-ofcloud-service-providers/, Forbes, son erişim: Haziran 2015.

[27]. Farcasescu M.R., 2012, Trust Model Engines in Cloud Computing, 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 465-470.

[28]. Oktay, U., Aydın, M. A., Sahingoz, O. K. Kasım 2013. A circular chain intrusion detection for cloud computing based on improved AdjointVM approach. Computational Intelligence and Informatics (CINTI), 2013 IEEE 14th International Symposium, IEEE, 201-206.

[29]. Intel Virtualization Technology for Directed I/O Architecture Specification Rev. 1.3, 2011, Intel Corporation.

[30]. D.G. Martinez, E.A. Rua, and D.A.R. Silva, "Secure Crypto-Biometric System for Cloud Computing," Securing Services on the Cloud (IWSSC), 2011 1st International Workshop, Milan, İtalya, 6-8 Eylül 2011, pp. 38-45.

[31]. OSSEC Log Management with Elasticsearch, Kasım 2013 http://vichargrave.com/ossec-log-management-with-elasticsearch/, son erişim: Haziran 2015.

[32]. Kibana, https://www.elastic.co/products/kibana, son erişim: Haziran 2015.

[33]. ElasticSearch, https://www.elastic.co/products/elasticsearch, son erişim: Haziran 2015.

[34]. Logstash, https://www.elastic.co/products/logstash, son erişim: Haziran 2015.

[35]. Scarfone K., ve Mell P. (2007), Guide to Intrusion Detection and Prevention Systems (IDPS), NIST (SP800-94-97) National Institute of Standards and Technology, Gaithersburg, Şubat 2007.

[36]. Microsoft Sanal Makine Kurulumu, http://ezgican.net/windows-azure-ile-sanal-makine-kurulumu/, son erişim: Mart 2019.

[37]. Öğretmen F.D. Temmuz 2015, güvenli bulut bilişim için saldırı tespit sistemleri , s.82-84,

[38]. Xentop, https://twiki.cern.ch/twiki/bin/view/Sandbox/JanMichaelSandbox,

son erişim: Mart 2019.

[39] Popek G.J. ve Goldberg R.P. (1973), Formal Requirements For Virtualizable Third Generation Architecture, Proceedings of the fourth ACM symposium on Operating system principles (SOSP '73), (Sf. 121),1973.

[40] Sugerman J., Ganesh V. ve Beng-Hong L. (2001), Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor, Proceedings of the 2001 USENIX Annual Technical Conference, (Sf. 1-4), 2001.

[41]. Çalışkan M. Haziran 2014, sanallaştırma teknolojilerinin saldırı tespit ve önleme sistemlerinin performansı üzerine etkisi, s.24-24

[42].MicrosoftAzure Disk Bilgisi, https://portal.azure.com/#create/Microsoft.VirtualMachine, son erişim: Nisan 2019

[43]. türkiyede internet erişim oranları, https://www.cnnturk.com/bilim-teknoloji/turkiyede-internete-erisim-orani-yuzde-80i-gecti?page=1 son erişim: nisan 2019

[44]. kobi istatistikleri (tüik), http://www.kobi.org.tr/index.php/tanimi/stats son erişim: nisan 2019

[45]. Dünya ve Türkiyede internet kullnıcı oranları, https://vergialgi.net/ekonomi-maliye/digital-in-2018-raporunda-dunyada-e-turkiye-de-durum son erişim nisan 2019

[46]. 2018 türkiye bilişim Pazar , Gartner Forecast Research Document 2018 Nisan, TÜBİSAD, Deloitte, BT Haber "İlk 500 Bilişim Şirketi Araştırması 2017" , https://www.karel.com.tr/blog/2018-turkiye-bilisim-pazari son erişim: nisan 2019