TÜRTEP

YÖNETİM-BİLİŞİM SİSTEMLERİ
YÜKSEK LİSANS PROGRAMI

TYBS-621 PROGRAMLAMA DİLLERİ
DÖNEM ÖDEVİ

BULUT PROGRAMLAMA
(CLOUD COMPUTİNG)

HAZIRLAYAN

Berkay Uğuralp ŞAHİN

18421025700

DANIŞMAN

Prof. Dr. Tolga GÜYER

MAYIS 2021

1. GİRİŞ

Çalışmaya öncelikle NIST"in yani Amerikan Ulusal Teknoloji ve Standartlar Enstitüsünün Bulut Bilişim tanımını vermekle başlayayım. Bulut bilişim istek üzerine rahat ulaşılabilir, kullanılmaya hazır, yapılandırılabilen bilgisayar kaynaklarının paylaşıldığı havuza ağ bağlantısı sağlama modelidir.

Teknolojinin hızlı bir şekilde ilerlemesi şirketler arası rekabet boyutunu da değiştirmiştir. İşletmelerin rekabet gücü ve avantajı elde etmeleri, buna bağlı olarak kârlılıklarını arttırıp, ekonomik büyüme ve piyasa değer artışı sağlamaları için yatırım yaptıkları bilişim teknolojilerinden elde edecekleri faydayı maksimum düzeyde tutmaları gerekmektedir. Bu bağlamda yapılan yatırımların işletmelere yeterince faydalı olup olmadığı ve bilişim teknolojisi kaynaklarının ne ölçüde verimli kullanıldığı sorgulanır hale gelmiştir. İşletmelerin bu sorgulaması başka bir alternatif çözüm yolunu gündeme getiriyor: Bilişim teknolojilerine büyük tutarlarda finansal kaynak ayırıp, yatırım yapmak ve bu bilişim teknolojilerini yüksek maliyetlerle işletmek yerine söz konusu bu bilişim hizmetlerini merkezi bir servis sağlayıcıdan satın alma seçeneği. Bu alternatif çözümün temelinde, bilişim teknolojileri için büyük yatırımlar yapmak yerine; "bilişim teknolojilerini elektrik, su ve doğalgaz gibi bir hizmet olarak satın alma ve bu hizmetten internet aracılığıyla yararlanma fikri" yer almaktadır. Bu alternatif çözüm yolu, bulut bilişim (cloud computing) adıyla ortaya çıkmış ve ekonomik yaşamda ve bilişim dünyasında büyük değişiklikleri beraberinde getirmiştir.

Günümüz şirketlerin sahip olduğu bilgi çokluğunun yanı sıra bu bilgileri saklayabilmesi de oldukça güçtür. Bilişim dünyası günümüzde gelişim, değişim, dönüşüm geçirmekte. Cloud Computing /Bulut Bilişim konsepti hızla bilişim endüstrisinde yayılmaya devam ediyor. Bilişim teknolojilerinin makro düzeyde ülke ekonomilerinde, mikro düzeyde de işletmelerde öneminin giderek artması, bilişim tabanlı endüstrilerin Dünya ticaretinden aldıkları payların sürekli artması ve bilişim tabanlı endüstrilerin büyüme hızları bilişim teknolojilerinin iş dünyasında stratejik bir öneme sahip olduğunu göstermektedir. Buluttaki bilgisayar yazılımlarına bir tıkla ulaşabilmeleri firmaları bilişim alt yapısı kurmaktan ve yönetmekten kurtulma becerisi karşı konulmaz hale gelmiştir. Bulut Bilişim" e geçiş yaparken tüm bulut modelleri ve servisleri göz önüne alınarak buluta geçiş senaryoları hazırlanmalı, oluşabilecek bulut ekonomisine bakılmalı ve altyapıdaki değişim ve dönüşüm ile birlikte şirketin iş yapış modelindeki değişim ve dönüşüm mutlaka dikkate alınmalı, bulut stratejisi oluşturulmalıdır. Bu geçişi yaparken servis kontratlarında diğer konularla birlikte şifreleme – cryptography ve encryption- konularına dikkat edilmesi gerektiğine inanıyorum. Bulut Bilişim başlıklı bu çalışmamızda bundan sonraki bölümlerde sırasıyla bilişim teknolojileri, bulut bilişim kavramsal olarak tüm yönleriyle incelenecektir.

3. BİR BİLGİ AĞI OLARAK BULUT BİLİŞİM

Bilgisayarlar arasında bilgi paylaşımı ağ (network) ile gerçekleştirilmekte, bilgi paylaşımını gerçekleştiren ağları yöneten bilgisayar "sunucu" (server), ağ üzerinde bulunan ve sunucuya bağlı olan bilgisayarlar ise "kullanıcı" (client) olarak adlandırabiliriz.

3.1. Bulut BiliĢim Tanımı ve Özellikleri

Bulut Bilişim (Cloud Computing), "gelişmiş bulut ve servis modelleri ile iş hayatında yaşanan problemleri oldukça ucuz ve hızlı bir şekilde çözebilecek bir teknoloji" olarak ifade edilmektedir

Bulut bilişim bilgi ağında bulut terimi, bilgi ağında paylaşılan dosyaların yer aldığı konumu ifade etmektedir. Bulut bilişimi "akıllı mobil cihaz, tablet veya bilgisayar kullanılarak bir yazılım ve depolama unsuruna gereksinim duyulmaksızın internet aracılığıyla diğer sunuculara erişilerek hizmet alma modeli" olarak ifade edebiliriz.

2. BULUT HİZMET SAĞLAYICI

Endüstri 4.0, Nesnelerin İnterneti ve büyük veri gibi kavramlarının ortaya çıkışı birçok sektörü etkilemiştir. Kurumlar kendi özel bulut hesaplama sistemini kurabileceği gibi, başka bir kamusal bulut hesaplama sisteminden hizmet alabilir ya da hem kendi özel bulut sistemlerinin hem de halka açık kamusal bulut sistemlerinin sunduğu hizmetlerden yararlanacak biçimde bir melez bulut yapısı oluşturabilir. Teknolojideki bu değişim, şirketlerin verileri saklaması, gizlilik, hızlı erişim gibi birçok ihtiyacı da doğurmuştur. Şirketler verilerinin güvenli bir şekilde saklanıp, hızlı bir şekilde erişebilmek için aktif olarak bulut hizmet sistemlerini kullanmaktadırlar.

Bulut hizmet; Bilgisayarlar arasında bilgi paylaşımı ağ (network) ile gerçekleştirilmekte, bilgi paylaşımını gerçekleştiren ağları yöneten bilgisayar "sunucu" (server), ağ üzerinde bulunan ve sunucuya bağlı olan bilgisayarlar ise "kullanıcı" (client) olarak adlandırılmaktadır. Sunucunun başka bir ülke veya kıtada olduğu halde sanal bir platform aracılığı ile kullanılabilir. Bunun için en önemli şart İnternet ağının aktif bir şekilde kullanılabiliyor olması gerekir. Bulut hizmet kullanan şirketler maliyet, zaman, veri saklamada sınıflandırma ve gizlilik gibi birçok özellikten yararlanbilinir. Hem bu avantajlardan dolayı hem de teknolojide konumundan dolayı şirketler, sektörel pazarda yaşamlarını devam ettirebilmeleri için bulut hizmetleri kullanması gerekmektedir.
Bulut servisi modellilerin

- *SaaS* – Bulut yazılımı

Servisi sağlayanın yazılımı bulut altyapısı üzerinde çalışır ve tüketicideki çeşitli cihazlardan web tarayıcısı gibi thin client ara yüzüyle ulaşılır. Tüketici sadece kullanıcıya özel yazılımın yapısal ayarlarını sınırlı olarak değiştirebilir.

Son kullanıcıların bilhassa veri depolama hizmeti almak ve verilerine her an her yerden ulaşabilmek adına kullandıkları hizmet olarak yazılım (*"Software as a Service"*, SaaS) programlarına örnek olarak GoogleDrive , SkyDrive, Dropbox , box verilebilir. Bulut bilişim yazılım servis modeli bir yazılım hizmeti olup, bu modelde merkezi bir kurulumdan birden fazla kullanıcının cihazına, herhangi bir kurulum yapılmasına gerek olmadan uç kullanıcılara internete bağlı herhangi bir cihazdan erişim hizmeti verilmektedir.
Bu modelde kullanıcılar uygulamalara, web tarayıcıları gibi hafif ara yüzler aracılığı ile çeşitli cihazlardan erişilebilme imkânına sahip olup; kullanıcıya özgü uygulama ayarları dışında altyapıdaki bileşenleri yönetme veya denetleme imkânına sahip değildir. Bulut bilişim yazılım servis modelinde servis sağlayıcılarına ve sağladıkları servis hizmetlerine Microsoft Office 365, Oracle, Google Apps, Workday, HP Cloud Services, Salesforce ve Amazon Web Services örnek olarak gösterilebilir.

- *PaaS* – Bulut Platformu

Tüketici servis sağlayıcı tarafından sunulan yazılım dilleri ve araçlarını kullanarak bulut altyapısı üzerinde kendi yazılımlarını geliştirebilir ve sadece kendi geliştirdiği yazılımlara ve yazılımın barındırılması için gerekli çevre birimleri üzerinde kontrol ve yönetime sahiptir. PaaS (*Platform as a Service*), şeklinde kullanılan teknolojilerin bazıları şöyle sıralanabilir: Google App Engine, Engine Yard, Force.com, Heroku, VMware, Amazon Web Services , Windows Azure. Bunlar arasında Google markasının her alanda isminin popüler olmasından dolayı da öne çıktığı düşünülen Google App Engine, yazılımcılar için açık kaynak imkanı sunan Java ve yanı sıra modüler program geliştirmeye olanak tanıyan Python programlama dillerine direkt olarak destek vermekte ve bazı eklentiler ile daha birçok dili desteklemektedir. Bulut bilişim platform servis modelinde müşteri işletmeler tarafından geliştirilen veya temin edilen uygulamalar, servis sağlayıcının sunduğu bulut altyapısı üzerine yerleştirilmekte ve müşteri işletme konumundaki kullanıcıların bu uygulamalar dışında bulut bilişim platform servis modelinin altyapısını meydana getiren unsurlar üzerinde herhangi bir müdahale imkânı bulunmamaktadır
Bulut bilişim platform servis modelinde kullanıcıya, programlama dilleri ve servis sağlayıcının verdiği araçları kullanarak oluşturulmuş ya da edinilmiş olan uygulamaları bulut altyapısına konuşlandırma yeteneği sağlanmaktadır.
Bulut bilişim platform servis modelinde servis sağlayıcılarına ve sağladıkları servis hizmetlerine AWS ElasticBeanstalk, cloudControl, Apprenda, CloudFoundry, Engine Yard, Google App Engine, Heroku, Mendix, Nodejitsu, Tsuru, OpenShift, OrangeScape, Windows Azure ve Jelastic örnek olarak gösterilebilir.

- *IaaS* – Bulut alt yapısı

Dağıtık ortamda paylaşılan havuzdaki kaynaklar, sanallaştırma veya iş çizelgeleme ile birleştirilebilmektedir. Hizmet olarak altyapı (*"Infrastructure as a Service"*, IaaS) şeklinde görülebilen sanallaştırma, genellikle fiziksel kaynaklar gibi davranan ve yazılım bileşenleri tarafından gerçeklenen mantıksal kaynak kümelerinin oluşturulmasıdır. Böylece, kullanıcılar tüm bulut altyapısını fiziksel olarak algılamaya ihtiyaç duymadan kullandıkları uygulamalarla ilişkili sunucu servisleri ile etkileşimde olur. Tüketiciye depolama, ağ ve diğer ana bilgisayar kaynaklarına erişmesi ve işletim sistemi dahil yazılımları geliştirip çalıştırabilmesi sağlanır. Tüketicinin bulut altyapısı üzerinde yine yönetim ve kontrolü yoktur, ama işletim sistemi, depolama, kullanılan yazılımlar üzerinde yönetim ve kontrole sahiptir ve firewall, yük eşleyiciler gibi ağ parçalarını seçme hakkı vardır. Altyapı hizmeti anlamına gelen bu hizmeti kullanıcı, kendi bilgisayarlarında istediği yer ve zamanda kullanarak, uygulamalara ve yazılımlara erişip kullanmak için modelin altyapı bileşenlerinden yararlanır. Bulut bilişim altyapı servis modelinde, kullanıcının gereksinim duyduğu temel bilişim unsurları kullanıcı tarafından yapılandırılabilmekte ve bu temel unsurlar üzerinde gereksinim duyulan işletim sistemi ve diğer uygulamaları yine kullanıcının kendisi kurabilmektedir. Kullanıcı konumundaki müşteri işletmenin altyapı üzerinde denetim ve müdahale hakkı olmamasına rağmen, işletim sistemi düzeyinde sisteme müdahale etme hakkına sahip olup Firewall gibi bazı bilişim ağı unsurlarını denetleyip yönetebilmektedir. Bulut bilişim altyapı servis modelinde servis sağlayıcılarına ve sağladıkları servis hizmetlerine Amazon EC2, HP Cloud, Google Compute Engine, Rackspace Open Cloud, SAVVIS, SingleHop ve iLand örnek olarak gösterilebilir.

- Cloud as a service – Servis olarak Bulut

Tüketiciye ticari ürünler, servisler ve çözümler internet üzerinden gerçek zamanda sağlanır. Bulut servisine daha yakından bakacak olursak;

- Tüm servis modellerini kapsar.
- Bir market için diğer standart olarak hazırlanmış paylaşılan bir servistir.
- Anahtar teslim modelidir, yani tüketici, sunulan servise sahip olmaya, yönetmeye veya kaynakları anlamaya ihtiyaç duymadan servise erişebilir.
- Altyapı göz önüne alındığında "tıkla ve satın al" yöntemiyle bulut depolama, bulut sunucuları ve bulut yazılımı alınıp self-servis olarak işletilebilir.
- İhtiyaç anında çabuk ölçeklenebilir.
- Tüketiciler ölçeklenebilir servisle ne kadar kullanıyorlarsa o kadarını öderler.
- Yetkili kullanıcılar tarafından İnternet üzerinden erişilebilir.
- Servis sağlayıcı müşterisini kullanıcı ara yüzü seçiminde serbest bırakır.
- Servisleri birbirine bağlamak ve entegre edebilmek, hızla web servislerinin ve API‟ lerinin hazırlanabilmesini sağlamak modern bulut servisinin ana elemanıdır.

Bulut hizmet kullanımı yönünden üç katmandan oluşur. Şirketlerin ihtiyaçlarına göre bir veya birden fazla katmanda çalışabilmektedirler. Bu üç katman SaaS (yazılım servisi), PaaS (platform hizmeti) ve IaaS (sunucu altyapı hizmeti) olmak üzere üç hizmet modeli olarak geçmektedir.

Bulut hizmet katmanının en altında IaaS katmanı yer almaktadır. Bu katmanda işlemler, depolama, ağ ve diğer temel bilgi işleme kaynakları standart hizmetler olarak bütün ağa sunulmaktadır. Oluşturulan bu katmanda kullanıcılara bilişim teknolojileri altyapısı sağlamaktadır. Katmanda gerekli araç ve gerece servis sağlayıcı sahiptir ve kullanıcıya da sanallaştırmış olarak bu altyapıyı kullanma imkânı verilmektedir. Orta katmanda hizmet olarak PaaS katmanı yer almaktadır. Bu katmanda temel işlemlerden ziyade daha çok geliştirme, test etme, yazılımların dağıtımı, barındırma hizmeti, birleştirilmiş geliştirme ortamındaki uygulamaların bakımı için soyutlamalar ve hizmetler yer almaktadır.

3. 3. Bulut Bilişim Dağıtım Modelleri

Bulut bilişimde, sunucuların bulunduğu lokasyon ve bu sunuculara erişim sağlayan kullanıcılara göre farklı dağıtım modelleri vardır. Dört farklı model olarak sınıflandırılan bulut bilişim dağıtım modelleri aşağıdaki alt başlıklarda açıklanmıştır.

3. 3. 1. Kamu Bulutu (Public Cloud)

"Bir servis sağlayıcının internet üzerinden erişime açık olacak şekilde uygulama, sunucu veya depolama gibi hizmetleri ölçeklenebilir ve esnek biçimde, ücretli veya ücretsiz olarak sunması" olarak tanımlanan kamu bulutu modeli; donanım, uygulama ve bant genişliği gibi kurulum ücretlerinin servis sağlayıcı tarafından karşılanmasından dolayı kullanıcıları için kurulumu kolay ve düşük maliyetli bir ortam sağlamaktadır

3. 3. 2. Özel Bulut (Private Cloud)

Özel bulut bilişim dağıtım modelinden yalnızca belirli bir kurum faydalanabilmektedir. Özel bulut bilişim dağıtım modelinde, modelin altyapısı kurum içerisinde veya dışında konumlandırılabilir. Özel bulut modeli, bulut bilişimin sağladığı bütün faydaları beraberinde getirirken; önemli bir risk olan bilgi güvenliği konusunda, modelin dışarıdan kullanıcılara kapalı olması nedeniyle sorun yaşanmamaktadır. Özel bulut bilişim dağıtım modelinde, planlama, ölçeklendirme ve güvenlik ile ilgili konular kurum içerisinde çözülmektedir.

3. 3. 3. Topluluk Bulutu (Community Cloud)

Topluluk bulutu modelinde, ortak faaliyette bulunan kurumlar ve belirli kuruluşlar modelin bilişim alt yapısını paylaşmakta; modelin tüm üyeleri sistemin verilerine ve uygulamalarına erişebilmektedir. Bu bulut modelinde kurumlar altyapılarında oluşan benzer türdeki ihtiyaçlarını ve maliyeti paylaşarak ölçeklerini artırabilmektedir.

3. 3. 4. Melez Bulut (Hybrid Cloud)

Karma bulut olarak da ifade edilen melez bulut modelinde, kamu bulutu ve özel bulutun birlikte kullanılması söz konusudur. Melez bulut, ihtiyaç ve önceliklere göre bilgi işlemin bir kısmının kamu bulutu, bir kısmının da özel bulut olarak alındığı; gizlilik ve/veya işlem güvenlik düzeyinin çok önemli olmadığı durumlardaki uygulamalar için kamu bulutunun, gizlilik ve/veya işlem güvenlik düzeyinin önem arz ettiği durumlardaki uygulamalar için de özel bulutun kullanıldığı bulut bilişim dağıtım modelidir.

4. Bulut Hesaplamada Güvenlik

Bu bölümde, bulut hesaplama ortamlarında güvenlik unsurunun önemi vurgulanarak kullanılan güvenlik teknolojileri belirtilmektedir. Ayrıca, bulut hesaplamadaki temel güvenlik ve mahremiyet gereksinimleraktarılmakta ve bulut hesaplama güvenliği, buluttaki 3 temel aktörün (sistem, uygulama geliştirici, kullanıcı) bakış açılarından incelenmektedir.

4.1 Bulut Hesaplamada Güvenlik Teknolojileri

Bulut hesaplamada öne çıkan güvenlik unsurlarını sıralayabilmek adına, öncelikle, kullanılan güvenlik teknolojilerinin sunduğu servisleri araştırmak uygundur. AWS, ölçeklenebilir bir bulut hesaplama platformunu yüksek erişilebilirlik olanaklarıyla sunmaktadır.

AWS, servis sağlama sürecinde gerekli politikalar tanımlayarak kapsamlı bir kontrol ortamı sağlamaya çalışmaktadır. Bu noktada sertifikasyon amacıyla Federal Bilgi Güvenliği Yönetim Eylemi (FISMA), hükümet büro müşterileri ile uyumluluk, Sağlık Sigortası Taşınabilirlik ve Hesaplanabilirlik Eylemi (HIPPA) tarafından belirlenen sağlık alanında uygulama geliştirenler için uyumluluk gibi güvenlik ve mahremiyet kuralları arz etmektedir. AWS'de kullanıcıların servisler üzerinde kimliklerinin belirlenmesi amacıyla, kullanıcı kimlikleri, parolalar ve Kerberos sistemi kullanılmaktadır. Amazon Esnek Hesaplama Bulutu (EC2), AWS'nin merkezi bölümünü oluşturmaktadır. Amazon EC2, bulut üzerinde tekrar boyutlandırılabilir hesaplama kapasitesi sağlayan bir web servisidir ve uygulama geliştiriciler için web bazlı hesaplamayı daha kolay hale getirebilmek için tasarlanmıştır. Bu amaçla, bir kullanıcı, örnek olarak oluşturduğu bir sanal makineyi Amazon Makine Görüntüsü üzerinde başlatabilir. Amazon EC2 güvenlik sistemleri, kullanıcının seçimi doğrultusunda çalışmakta olan örneklerini gruplara ayırma izni verir. Web servisleri arayüzünü kullanarak hangi grubun diğer hangi gruplarla iletişim içerisinde olduğu belirtilebilir ve internet üzerindeki hangi IP altağlarının bu gruplara erişebileceği tanımlanabilir. Böylece dinamik bir ortamda bahsedilen sanal makine örnekleri üzerinde erişim denetimi sağlanabilir.

IBM SmartCloud Resilience, işletmelerin daha planlı ve yönetilebilir sistemler oluşturabilmesi amacıyla servisler sunmaktadır. Güvenlik açısından sunulan servislerden IBM SmartCloud Manager

Backup, hassas verinin korunmasına yardımcı olan uygun maliyetli bir yedekleme çözümüdür. IBM SmartCloud Archive, arşivlenen veriyi indeksleme, araştırma, edinme ve depolamayı düşük ücretli şekilde sağlama amacı güden bulut tabanlı bir veri arşivleme çözümüdür. IBM SmartCloud Virtualized Server Recovery, kapsamlı sunucu kurtarma çözüm yaklaşımı ile kullanıcının altyapısının kurtarılabilirlik açısından güvenilirliğini arttırır ve kurtarma zamanını azaltmaya çalışır.

Bulut hesaplamada sunulan diğer bazı güvenlik mekanizmalarına örnek olarak şunlar da sıralanabilir: Öncelikli kimlik yönetim desteği sunabilen Cyber-Ark yazılım teknolojisi; güvenlik risk değerlendirmesi yapabilen ve bulut sunucularını iç ve dış saldırılara karşı korumak üzere kullanılabilen Cloud Passage ateş duvarı; hesaplama iletişimini gözetleyebilen ve tehditleri daraltarak bütünüyle güvenlik sağlayıp verimliliği arttırmaya çalışan Lieberman Software teknolojisi, Microsoft'un sağlam bulut için kullandığı Azure ürünü, güvenlik de dahil genel bir bulut çözüm teknolojisi olarak Google App Engine.

4.2 Bulut Güvenliğinde Öne Çıkan Kavramlar

Bulut hesaplamanın birçok avantajı bulunmasının yanı sıra servislerde karşılaşılan bazı olası sorunlar göze çarpmaktadır. Bu sorunların başlıcaları, yerel veya bölgesel düzenlemelere uyumlu olma, erişim yetkisine sahip olunmayan alanlarda onay alınması gerekliliği, denetim açısından bazı ek karmaşıklıklar getirmesi, bulutun doğasına uygun olarak onarım ihtiyacı ve bulut servislerinde algılanabilecek güven eksiklikleri olarak sayılabilir.

Bulut bakış açısıyla lokasyonu ele alırsak, bilginin farklı noktalarda bulunabileceği bir sistemden bahsedildiği görülmektedir. Farklı noktalarda bulunan bilgi değişik bileşenler tarafından yönetilebilmekte, farklı coğrafi konumlarda bulunan sunucular üzerinde depolanmaktadır. Dolayısıyla veri ile ilgili uyumluluk gereksinimleri için küresel yasalara göre uzlaşmak zor olabilir ve bu durumda veriye sahip olma kısıtları, sektöre bağlı kısıtlar, ulusal veya eyalet bazındaki kısıtlar göz önüne alınmaktadır.

Küreselleşmenin hakim olduğu günümüzde, mahremiyet için geleneksel çatıların sunduğu yaklaşımlar tekrar gözden geçirilmektedir. Bağlam, farklı veriler üzerinde değişik mahremiyet, güvenlik ve gizlilik gereksinimleri doğmasında önemli bir argümandır. Bulut servisi eğer kişisel bilgileri ele almaktaysa mahremiyet hesaba katılmalıdır. Bulut servisleri halka ait bilgiyi işliyorsa düşük bir mahremiyet tehdidi öngörülebilir. Buna karşın, kişinin bulunduğu yere, tercihlere, sosyal ağlara ve bu gibi dinamik bilgilere göre kişiselleştirilen bulut servisleri için yüksek bir mahremiyet tehdidi öngörülebilir. Kişisel bilgilerin yanı sıra kurumsal bilgilerin ve ticari sırların da ağ üzerinde paylaşımı dikkate alındığında gizlilik de önemsenmelidir.

Güvenilir bulut hesaplama mimarisi, bulut sistemini, sisteme zarar verebilecek ihlallerden ve ataklardan korumaya yönelik tasarlanan bir güvenlik yapısı içerecek biçimdedir. Güvenilir bir bulut hesaplama sistemi, bilgiyi yetkisiz erişime karşı korumak, güçlü kimlik doğrulama sağlamak, çalınma veya kaybolmaya maruz kalabilecek cihazlar üzerinde duran hassas veriyi koruma amacıyla şifrelemek ve donanım/yazılım mekanizmaları ile uyumluluk sağlamak gibi güvenlik mekanizmaları sunmakla yükümlüdür. Güvenilir Hesaplama Tabanı ("Trusted Computing Base", TCB), bilgisayar sistemi içindeki koruma mekanizmalarının bileşimidir; bir güvenlik politikasını yerine getirerek donanım, yazılım ve gömülü aygıt yazılımının güvenilirliğini sağlar. TCB bileşenleri, bulut hesaplama sisteminin güvenlik politikasını yürütmekle yükümlüdür. Güvenilir Platform Modülü ("Trusted Platform Module", TPM), hesaplama için donanım tabanlı güven sağlayan bir standarttır. TPM, bilgisayar içerisine üretim esnasında eklenen bir bileşen de olabilmektedir. Bilgisayar üzerinde bulunan bir donanım elemanı olması vasıtasıyla kullanıcı ile birlikte cihazın da kimlik doğrulamasının yapılması için kullanılır. Bir kullanıcı birden fazla servise tek oturum açma ("Single Sign On", SSO) ile bağlanabilme hakkına sahipken yine de cihaz için kimlik doğrulama yapar. Bu yaklaşımla sadece bulut tarafından bilinen cihazlar/kullanıcılar uygulamaları kullanabilir ve buluttaki veriye erişebilir. Bu özelliklerinin yanında TPM, depoladığı kriptografik anahtarlar yardımıyla, donanım ve yazılım ayarlarının değiştirilmediğini doğrular. TPM bileşenlerinin bulut içerisinde çalıştırılması amacıyla, güvenilir bir sunucu üzerinde bulunan her sanal makine için TPM bileşenlerinin yazılım örneklerini sağlayan sanal bir TPM (vTPM) meydana getirilir ve ilgili vTPM için uygun spesifikasyonlar oluşturulur.

Bulut hesaplama sağlayıcılarının birçoğu, güvenli bir bağlantı üzerinden kimlik doğrulama ve güvenli veri transferi gerçekleştirmesine rağmen, verinin şifreli saklanmasıyla ilgilenmemektedir. Dolayısıyla hassas verinin bulut üzerinde şifreli olarak bulunması kullanıcı tarafına bırakılan bir görev olarak görülebilir. Bulut üzerinde şifreli veri ile beraber şifreleme anahtarlarının da tutulması uygun bir yaklaşım değildir. Kullanıcıların kendi bilgisayarlarında yaptıkları şifreleme ile ilgilenmeleri zaman alıcı bir süreç olduğundan buluta veriler depolanmadan önce kullanıcı ile bulut arasında bir çözüm sunulmaya çalışılmaktadır. CipherCloud Encryption Gateway, kullanıcı bulut uygulamalarına hassas veriyi aktarmadan önce şifreleme yapar ve ihtiyaç duyulduğunda deşifrelenmiş halini son kullanıcıya sunar. Böylece bulut uygulamalarında herhangi bir değişime ihtiyaç duyulmadığı ve servis sağlayıcının hassas veriye erişemediği bir yapı elde edilmektedir.

Bulut hesaplama güvenliği, bulut içindeki kullanıcıların ve servis sunucuların verilerinin / uygulamalarının güvenliği, bulut hesaplama ile ilişkili kullanılan altyapının güvenliği için kullanılan yöntemler, kurallar ve teknolojiler ile ilişkilidir. Bulut güvenliğini sağlamaya yönelik gereksinimler, bulut altyapısında varsayılan olarak tanımlanmış sistem güvenliği mekanizmaları, kullanıcıların ve servis sağlayıcıların aralarındaki sözleşmeleri doğrultusunda anlaşılan veri erişimi kontrol mekanizmaları, servis seviyesinde erişim anlaşmaları, ayrıca kullanılan servisin sunduğu ek güvenlik işlevleri ile birlikte sağlanır. Bu kapsamda, bulut güvenliği gereksinimlerinin başlıcaları veri gizliliği, veri bütünlüğü, kimlik doğrulama olup bunların yanı sıra kimlik yönetimi, fiziksel ve kişisel güvenlik, erişilebilirlik, uygulama servisinin güvenliği, mahremiyet ve kanuna uygun unsurlar ek olarak öne çıkmaktadır.

4.3 Bulut Hesaplama Güvenliğine Farklı Açılardan Bakış

Bu kısımda bulut hesaplama sisteminde rol üstlenen bileşenlerin bulut hesaplama güvenliğine bakış açıları ele alınacaktır. Bu bağlamda, bulut yapılarındaki kullanım senaryolarında görev alan birimler, bulut mimarisi, BT yöneticisi, sistem yöneticisi, altyapı ve servis sağlayıcı, üçüncü parti güvenlik danışmanı, servis geliştirici, hizmet satıcı ve son kullanıcı gibi çeşitlendirilebilir. Ancak, bu çalışmada birimlerin 3 temel eylemci figürü üzerinde ele alınması planlanmıştır: sistem, uygulama geliştirici ve kullanıcı. Bu 3 temel bileşen, altyapı ve fiziksel destek bakımından bir bütün olarak kullanılan bulut sistemi, BT yöneticiliği, servis sunumu, danışmanlık, hizmet satışı, uygulama ve yazılım geliştirme bakımından aynı tarafta görülebilen bütün birimleri temsil etmesi adına uygulama geliştirici, hizmet alan kurumları ya da son kullanıcıları temsil etmesi adına kullanıcı ifadeleriyle anlatılmış, bulut hesaplama sisteminin içinde yer alan bu temel birimlerin bulut hesaplama güvenliğine kendi açılarından baktıkları durumda etkileşim içinde oldukları eylemleri ve dolayısıyla buluttaki kendileriyle ilişkili güvenlik görüş açılarını aktarmaktadır.

Bulut sisteminde farklı kullanıcıların perspektifinden görülen öncelikli güvenlik unsurları ele alınmıştır; elbette ki sisteme ilgili birim tarafından bakıldığında bakış açısına girdiği düşünülen güvenlikle ilişkili özellikler daha da arttırılabilir. Her ne kadar en dar açıya sahip olan son kullanıcı güvenlikle ilişkili en az unsur içinde yer alıyormuş gibi görünse de kişisel olarak güvenlikten en fazla manevi zararı görebilecek olan da yine odur.

Sistem bakış açısından güvenlik: Sistem her bileşenini bilip güvenli biçimde yönetmek ister ve hiçbir bileşenine gizlilik unsurları açısından zarar gelmesini istemez. Dağıtık ortamdaki tüm kaynakları korumaya çalışan sistem, servislerini uygulama sunucularında barındırır ve sistem tasarımcılarının veya uygulama geliştiricilerin bu web servisleri aracılığıyla son kullanıcılara yönelik ek uygulama yazmalarını da destekler. Bu yolda güvenlik unsuru sistemin ayrılmaz bir parçası niteliğinde olmalıdır. Özel, kamusal veya melez tipte oluşuna göre güvenlik gereksinimlerinin değişebileceği bulut sistemi, altyapısal bir güvenlik desteği sunmak yükümlülüğündedir. Sistemin güvenlik bakış açısında öncelikli görülen unsurlardan birisi güvenli sanallaştırmadır. Farklı sistem bileşenlerini ortamdaki son kullanıcılara platformdan bağımsız bir büyük veri merkezi ve içeriğindeki erişilebilir kaynaklar halinde sunan yapılanmanın ağ güvenliği açısından dikkatle ve uygun konfigürasyonla düzenlenmesi ihtiyaçtır. Çeşitli işlemci merkezleri veya son kullanıcı tarafından erişim için veri depolama merkezlerinde saklanan verilerin fiziksel güvenliği yine önemli ihtiyaçlardandır. Ayrıca, sistemde güvenlik hizmetinin ölçeklenebilir olması beklenmektedir; dolayısıyla fiziksel kaynaklar, sunulan servisler, hizmet sağlayıcılar ve hizmet alıcılar arttıkça yani sistem bileşenleri çoğaldıkça güvenlik seviyesinin

düşmemesi sağlanmalıdır. Buna ek olarak, hizmet alıcıların farklı fiziksel platformlardan sisteme dahil olmaları durumunda da temel güvenlik altyapısından uygun ölçüde yararlanmaları desteklenmelidir.

Sistemin, ağ kaynaklarına yönelik ataklara karşı korunma mekanizmalarıyla donatılmış olması öncelikli bir başka yükümlülük olarak görülebilir. Bulut hesaplama yapısı içinde yer alan donanımlara veya yazılımlara yönelik hizmet engelleme ("denial of service", DoS) saldırıları, virüs yayma, fiziksel zarar verme ve ağa veya iletişime yönelik olası başka ataklara karşı savunma mekanizmaları bulunması ihtiyaçtır.

Sistemin en temel güvenlik gereksinimleri açısından veri gizliliği, veri bütünlüğü ve kimlik doğrulama sunabilmesi istenir. Ayrıca, veriye her an her yerden erişilebilirlik, kişisel verilere yönelik mahremiyet hakkı, hesap ve kimlik yönetimi gibi gereksinimler de desteklenebilmelidir. Sistem perspektifinden bulut hesaplama güvenliğiyle ilişkili görülebilen unsurlar daha da arttırılabilir. Sisteme katılan cihazlara kimlik numarası benzeri özellik atanması ve dolayısıyla kurumsal donanımlara yönelik kimlik yönetim desteği sunulabilmesi, ayrıca üçüncü parti güvenlik sertifikasyon hizmetleri için kriptografik anahtar oluşturma ve dağıtma sisteminin desteklenmesi ve dolayısıyla sertifika yönetiminin sağlanabilmesi bunlara örnektir.

Uygulama geliştirici bakış açısından güvenlik: Uygulama geliştirici güvenlik bakış açısına göre, bulut üzerindeki uygulama/yazılım, kullanıcıların ihtiyaç duyduğu görevleri gerçekleştirirken gerekli ek güvenlik kıstaslarını da sağlar. Bu noktada kullanılan yazılımlar izlenerek meydana gelebilecek güvenlik tehditlerinden de korunmaya çalışılmaktadır. Güvenlik sözleşmeleri, yazılım lisanslarındaki özellikleri andırmakla beraber dış kaynak kullanma kontratları gibi kullanılacak altyapıdaki yazılımdan başka donanımsal ve veriye özgü maddeleri de içerebilmektedir. Güvenlik ve uyumluluğun ön planda olduğu kontratlar, bölge bazında uygulanabilir kanunlar da göz önüne alınarak oluşturulmaktadır. Hizmet seviyesi anlaşma ("Service Level Agreement", SLA) maddeleri baz alındığında altın, gümüş, bronz ve platin gibi servis kullanım olanakları kategorize edilmekte, kontratlar buna göre düzenlenmektedir. "Microsoft SQL Azure Service Level Agreement" bilgilerini örnek olarak aldığımızda zamana bağlı (aylık, yıllık vs.) kontrat düzenlemeleri de görülebilmektedir. Bulut hesaplama ortamında veri erişim kontrolü için geliştiriciler, kullanıcılara sağladığı verinin güvenilirliği için denetim politikaları tanımlar. Bu noktada hem servis sağlayıcıları hem de kullanıcılar tarafından meydana gelebilecek gizlilik, bütünlük ve güvenilirlik ile ilgili suçlamaların ortadan kaldırılmasına çalışılmaktadır. Bu amaçla ilgili erişim yetkisine sahip olmayan kişilerin veya kurumların, okumak, yazmak veya güncellemek istedikleri ilgili verilere, çalıştırmak istedikleri ilgili uygulamalara erişimleri kısıtlanmaktadır. Ayrıca veri veya uygulamanın silinmesi aşamasında ilgili kaynağın sürekli olarak başkaları tarafından erişilemeyecek şekilde silinmiş olması gibi durumların da kontrolünün sağlanması önemlidir.

Sürdürülebilirlik amacıyla yedekleme ve kurtarma kontrollerinin devamlılığının sağlanması gerekmektedir. Çoğu güvenlik ihlallerinin veri yedeklemesine dayalı olduğu düşünüldüğünde veri yedeklemesi üzerinde fiziksel ve mantıksal kontrollerin yapılmasının önemi anlaşılmaktadır. Bu noktada özellikle fiziksel olarak yedeklenmiş verilerin hangi mekanizmalar yardımıyla yaşam döngüsünün devam ettirileceğinin üzerinde durulması önemli bir husus olarak göze çarpmaktadır. Bulut üzerinde güvenlik testleri yapılırken, uygulama geliştiricinin bulut çözümünü kendi şirketinden veya diğer bir bulut sağlayıcısından aldığından bağımsız olarak test senaryoları geliştirmesi öngörülmektedir. Uygulamalar üzerinde yapılacak testlerin uygulamanın sınırları ile belirlenmesi gerekmekle beraber bulut sınırlarının da önemsenebileceği güvenlik testleri yapılması düşünüldüğünde ağ altyapısının hesaba katıldığı durumlar meydana gelebilmektedir. Dolayısıyla beyaz-kutu veya kara-kutu test stratejilerinden hangisine uygun testler geliştirileceği uygulamaya ve bulutun altyapısına göre değişebilmektedir.

Risk değerlendirmesi, uygulama geliştiricilerin, ayrıcalıklı kullanıcı erişimi, verinin bulunduğu konum, verinin değerliliğine göre ayrımı, veri kurtarma, uygunsuz veya yasal olmayan aktivitelerin araştırılması, uzun dönemde veri yaşayabilirliği gibi noktalarda optimum çözümler getirebilmek amacıyla yoğun analizler yaptıkları bir alandır.

Uygulama geliştiricinin de sunabileceği ek bir ihtiyaç olarak görülen güvenli ücret ödeme sistemi ise, kullanıcıların "kullandığın kadar öde" modeline uygun yaptığı ücret ödemelerinde kredi kartı bilgileri gibi hassas bilgilerinin korunmasına olanak sağlandığı bir tasarımla oluşturulmalıdır.

Kullanıcı bakış açısından güvenlik: Son kullanıcının güvenlik bakış açısı dar ele alınmıştır, çünkü kullanıcılar genel olarak güvenlik detaylarını önemsememektedir. Buluttan yararlanan son kullanıcı arka tarafı pek bilmez ve görmek de istemez, kendisine altyapı açısından güvenli bir sistem ve servis açısından güvenilir bir uygulama/yazılım sunulmasını ister. Tabii ki kullanıcıya düşen en önemli görev güvenlik bilincine vakıf olmaktır. Bilinçli bir kullanıcı olarak sadece verilerine veya kendi mahremiyetine zarar vermemek adına değil aynı zamanda sisteme de olası tehdit sunmamak adına zararlı uygulamaları kullanmaktan kaçınmalı ve kendisi için verimli olabilecek güvenlik sözleşmelerini ele alıp bunlara uygun hareket etmeye çalışmalıdır. Ayrıca, sisteme erişim için kullandığı dizüstü bilgisayar, akıllı telefon gibi cihazların zararlı kod veya uygunsuz veri barındırmadığını takip etmesi anlamlı olacaktır. Sonuçta, bulut içinde kendisiyle ilişkili bir güvenlik sorunu olduğunda son kullanıcı maddi külfet yaşamasa dahi durumdan en fazla manevi zararı büyük ihtimalle yine kendisi görecektir.

Bu açıklamalar doğrultusunda kullandığımız bulut bilişimlerin ortak özeliklerini sıralayacak olursak:

- Büyük ölçeklilik
- Homojenlik
- Sanallık
- Esneklik
- Düşük maliyet
- Dağıtıklık
- Servis odaklılık
- İleri güvenlik

5.Bulut Bilişimin Avantaj ve Dezavantajları

Bu avatajları aşağıdaki gibi örneklendirilebiliriz:

- Güvenlik alanında tüm şehirler kameralarla izlenerek güvenlik çemberine alınabilmektedir.
- Alışveriş alanında online alışveriş siteleri aracılığıyla istenilen ürüne internet ortamında ulaşılabilmekte ve ödemesi yapılabilmektedir.
- Bankacılık alanında belli bir mekâna bağlı olmaksızın her türlü parasal hareket internet üzerinden ya da ATM'lerden banka kartlarıyla yapılabilmektedir.
- Gazetecilik alanında online olarak gazetelere, dergilere ve makalelere ulaşılabilmektedir.
- Eğitim alanında bilgiler bellekler aracılığıyla saklanmakta, online düzenlenen sınavlar ve uzaktan eğitim yöntemleri kullanılmaktadır.
- Sağlık alanında hasta veri tabanına ve bilgi bankasına sadece tek bir kimlik numarasıyla ulaşılabilmektedir.
- Ulaşım alanında online bilet alımı ve takibi yapılabilmektedir.
- Sosyal medya alanında aynı anda birçok kişiyle iletişime geçilebilmektedir.
- Telekomünikasyon alanında akıllı mobil telefonlarla bir bilgisayarın yapabileceği işler mobil işletim sistemleri aracılığıyla gerçekleştirilebilmektedir.

"Bilişim teknolojilerinin dış kaynak kullanımı yoluyla; süreçleri geliştirmeyi, verimliliği artırmayı ve işletme faaliyetlerini daha cazip, daha kısa zamanda ve daha düşük maliyetle yenileştirmeyi" hedefleyen bulut bilişim bilgi ağı, kullanıcılarına pek çok kolaylık ve fayda sağlamaktadır.

1. Maliyet Yönetiminde Etkinlik ve Verimlilik: Bulut bilişim, sağladığı imkanlar ile başta işletmeler olmak üzere kullanıcılarının bilişim teknolojilerine yapacakları sermaye yatırım tutarlarını azaltarak, bilişim teknolojisiyle ilgili sabit maliyetleri düşürmektedir. Bulut bilişim servis modellerinin sunduğu bilgi ağı ortamı sayesinde işletmeler, veri merkezi kurulum maliyetlerinde ve bilişim ile ilgili diğer sabit maliyetlerde tasarruf sağlayacak ve tasarruf edilen sermaye yatırım tutarlarını diğer iş süreçlerinin kalitesini arttırmaya ayırabileceklerdir. Bulut bilişime geçişle beraber donanıma ayrılacak sermaye yatırım bütçesinde, sunucu yazılımı lisansı maliyetlerinde, yıllık bakım maliyetlerinde ve veri depolamanın yol açacağı ek maliyetlerde tasarruf sağlanabilecektir.

2. Esneklik: Bulut bilişim bilgi ağında maliyetlerin düşük düzeylerde olması ve sistemin artan ya da azalan iş hacmine anında karşılık verebilmesi işletmelere esnek bir yapıda organizasyon kurma imkânı sunmaktadır. İşletmeler bulut bilişim ile birlikte yeni teknolojilere ve servislere otomatik olarak ulaşabilecek ve bu sayede iş süreçleri yeniden yapılanırken daha fazla seçenek söz konusu olacaktır.

3. Kullanılabilirlik ve Sürdürülebilirlik: Bulut bilişim bilgi ağında hizmet sağlayıcı şirketler teknolojik olarak en gelişmiş düzeyde ve kapasitede donanım ve bant genişliği sunarak kullanıcı ihtiyaçları karşılanmaktadır. Bulut bilişim bilgi ağında, hizmet sağlayıcı şirketler sistem kesintilerine ve aşırı yüklenmeye karşı gerekli tedbirleri almakta ve ek sistemleri devreye sokabilmektedir.

4. Yaygın Ağ Erişimi ve Neredeyse Sınırsız Depolama Kapasitesi: Benzer olmayan unsurlardan oluşan istemciler (telefon, bilgisayar, tablet vb. cihazlar) aracılığı ile servis sağlayıcının sunmuş olduğu hizmetlere, kullanıcı bulunduğu her yerden bulut bilişim bilgi ağı üzerinden erişebilir kapasitededir. Bulut bilişim bilgi ağındaki bulutları depolama kapasitesi yüzlerce pet bayttır. 1 pet baytın bin terabayta eşdeğer olduğunu dikkate alırsak neredeyse sınırsız bir kapasite söz konusudur. Bulut bilişimde bulut depolama sistemi, kullanıcıların verilerini bir diske depolayarak istedikleri yerden istedikleri zaman erişmelerini sağlamaktadır.

5. Ölçümlenebilir Servis: Bulut bilişim sistemleri, kaynakların kapasitelerini ölçümleyerek otomatik olarak kontrol ve optimize edebilmektedirler. Bu bağlamda kaynak kullanımı izlenebilmekte, kontrol edilebilmekte ve raporlanabilmektedir. Kaynak kullanımına bağlı olarak kapasitede artan talebe bağlı olarak gerekli önlemler alınabilmektedir.

Bir bilgi ağı olarak bulut bilişimin yukarıda belirtilen avantajlarının yanı sıra bazı dezavantajları da söz konusudur. Bulut bilişime özgü dezavantajlar aşağıdaki üç başlıkta ifade edilmiştir:

1. Güvenlik ve Gizlilik Konusu: Bulut bilişim bilgi ağında, en önemli risk konusu güvenlik ve gizliliktir. Bulut bilişim bilgi ağında kullanıcı ve servis sağlayıcı arasında paylaşılan özel ve gizli verilerin, bulut bilişim bilgi ağı içindeki diğer kullanıcılardan nasıl korunacağı konusu önemli bir dezavantaj doğurmaktadır.

2. Performans Düşüklüğü Olasılığı: Bulut bilişim bilgi ağında, hizmet sağlayıcı şirketlerden uzak mesafede bulunan ve yoğun işlem odaklı ve veri yoğun uygulamalarla çalışan organizasyonlar, zaman zaman bilgi ağında gecikmeler yaşayabilmektedir. Bu durum kullanıcı konumundaki işletmelerin faaliyetlerini olumsuz etkilemektedir.

3. Yasal Uygulamalardaki Farklılık: Bulut bilişim bilgi ağı kullanıcısı bir işletmenin, bulut bilişim servis sağlayıcısından farklı bir ülkede bulunması durumunda; bulut bilişim servis sağlayıcısının bulunduğu ülkenin mevzuatı geçerli yasal uygulamalar olacağından bu ülkede depolanan verilerin gizliliği tehlikeye girebilmektedir.

6. Değişim ve Dönüşüm

6.1. Alt yapı dönüşümü

Tüm yeni teknoloji uygulamaları gibi test ortamında bulut bilişim uygulamasına geçmek doğru bir yöntemdir. Bu çalışanlarınıza diğer kritik işleri aksatmadan bulutu tanıma fırsatı verecektir. Bazı şirketler buluta geçişlerine bulut fonksiyonlarını test etmek için bulutta bir geliştirme ortamı hazırlayarak başlıyorlar işe. Bazılarıysa var olan sanal ortamlarına self-servis yöntemiyle bulut ortamını ekliyorlar. Bu çözümde hem geleneksel yapınızı hem de bulut ortamını yönetmeniz gerekecek, bunu sağlayabilmek için elinizdeki araçların her iki ortamı da desteklemesi gerektiğini unutmayın. Dünyada birçok kuruluş halka açık-kamu bulutu-public cloud sağlayıcılarından özel bulut servisi alarak karma bulut kullanıyorlar. Bu karma yaklaşım servis yönetimini de içerdiğinden birçok problem baştan bertaraf edilebilir. Sonuç olarak halk-kamu bulutu sunan tedarikçi seçimini yaparken servis yönetimini sizin kuruluşunuza kadar genişletebileni seçmenizi öneririm.

6.2. Süreç ve organizasyonel dönüşüm

Seneler boyunca birçok IT kuruluşu ITIL gibi IT disiplinlerinde başarılı süreçleri elden geçirdi ve geliştirdi. Olay ve problem yönetimi, değişim ve yapılandırma yönetimi, erişim kontrolü ve uygunluk yönetimi sadece birkaç örnek. Yine de süreçlerinizi Bulut ortamına uyum sağlayabilmeleri için elden geçirip kodifiye etmeniz gerekebilir. Örneğin değişim yönetimi süreçleri değişim isteklerinin ilgili müdür tarafından onaylanmasını da içerir. Eğer bu onay birçok organizasyonda olduğu gibi el ile yürütülüyorsa istekleri zamanında gerçekleştirmenizi engelleyecek darboğaz oluşması doğaldır. Kendi konumdan, bilgi işlemden örnek vereyim; Bir bilgi işlem müdürünün "yeni sunucuyu birkaç dakikada devreye alabilirim, ama hazırladığım dokümanın imzalanması aylar sürebilir" sözü sanırım yeter derecede açık. Bazı değişim isteklerini ön-onay mekanizmasından geçirmek, gecikmelerin önüne geçebilir. Bilgi işlem örneğine dönecek olursak, standart bir sunucu kuruluşu süreçlerini ön-onay mekanizmasından geçirmek beklemeyi engelleyecek ve sunucudan daha çabuk verim alınacaktır. Servis yönetimiyle birçok IT organizasyonu bulutta süreç yönetimini basitleştirerek teknolojiden faydalanabilecektir. Örneğin büyük sayıdaki kaynakların içinde hızlı hareket eden, hızla tedarik edilen, yayılan ve hızla emekli olan bulut ortamını destekleyerek yapılandırma yönetiminde ilerlemeler kaydedilebilir. Servis odaklılık IT" nin organizasyonel yapısını bulut ortamını daha iyi yöneten ve destekler duruma getirir.

6.3. Servis dönüşümü

Bulut Bilişim, çalışanların kendi servislerini kendilerinin istemesini sağlar. Self-servis iş ihtiyaçlarının karşılanma çevikliğini artırır. Ek olarak servisin maliyetini düşürür. Self-servis çalışabilmek için hazır verilen kaynakların kullanıcılar, çalışanlar tarafından anlaşılır olması gerekir. Çalışanlar Bilgi İşlem alt yapısını umursamazlar, onlar için önemli olan onlar tarafından anlaşılır servislerin istedikleri anda önlerinde olmasıdır. Örneğin bir alışveriş sitesi için işlemci kapasite ihtiyacı değil de 1000 kullanıcıya aynı anda servis verilmesi onlar için daha önemlidir.

Standardizasyon, servis isteklerini ve yönetimini kolaylaştıracak dolayısıyla IT masraflarını düşürecektir. Business service management (BSM) IT organizasyonlarına daha servis odaklı olabilmeleri için yardımcı olur. Sonuç olarak, IT servisleri işi odaklı olur ve artarak verimli hale gelirler. Servis istek otomasyonu becerileri, örneğin; çalışanların katalog üzerinden ihtiyaçları olan servisleri istemelerini kolaylaştırır. Erişim ve kimlik yönetimi ise sadece yetkili kişilerin bu servisleri almasını sağlar ve erişim düzeyi organizasyondaki role göre kontrol edilir.

6.4. Kültürel dönüşümü

Geçmişte bazı IT organizasyonları kurumsal ya da bütçe tahditleri nedeniyle engellenmiş ve sonuç olarak iş isteklerini karşılamakta yavaş kalmıştır. Bunun tersine Bulut bilişim çevikliği sağlar. IT servis isteğine dakikalar içinde cevap verir. Bu sadece IT kültüründe değil aynı zamanda iş kültüründe de önemli bir değişimdir. Servis isteğine bulut tarafından sağlanan hızlı cevapla, çalışanlar değişen iş koşullarına daha çevik ayak uydurabilirler. Bu çeviklik yeni iş olanaklarına göre büyümeyi düşük maliyetle sağlar. IT servis maliyetini bir katalog halinde kullanıcılarına sunarsa, çalışanlar kullanım öncesi maliyetler hakkında bilgi sahibi olarak seçimlerini ve bütçelerini ona göre yapabilirler. Ülkemizde bu uygulamayı ne derecede başarırız bilemiyorum. Genelde şirketlerde kararlar IT ve üst yönetim tarafından alınıyor. Kullanıcılar pek işin içine dahil edilmiyor. Karar alındıktan sonra uygulama aşamasında kullanıcılar devreye alınıyor. Çünkü bizde IT departmanları şirketin tüm süreçlerini gözleri kapalı bilirler, bilmek zorundadırlar. Belki bulut bilişimle ülkemizde de Bilgi işlem yönetimi ve iş süreçleri yönetimi (business process management) böylece ayrılmış olurlar. Bulut bilişim ölçümü desteklediğinden IT" nin güvenilir, transparan fiyatlama modeli oluşturmasını sağlar. Bu model fiziksel kaynakların kullanımından, yazılım maliyetinden servislerde artışın, maksimum/minimum kullanım maliyetine kadar her şeyi kapsar. IT bu kültürel değişimin sürücüsü olmak durumundadır. Bulut mesajlarını etkin bir şekilde çalışanlara iletmek elzemdir. Servis isteklerini gecikmesiz yerine getirmek ve kullanıcıların beklentilerini karşılamak için ölçümleme yapmak servis kalitesini artıracaktır.

7. Planlama

Bulut Bilişime geçiş yaparken planlama her geçişte olduğu gibi ön planda olmalıdır.

• Öncelikle Bulut stratejisini belirlemek gerekir. Sonrasında var olan altyapı ve süreçler gözden geçirilir ve değerlendirme yapılır.
• Tasarım safhasında ise blueprint-proje planı hazırlanır, kaynaklar, süreçler ve hedef netleştirilir, görev tanımları yapılır.
• Sonrasında pilot uygulama ve uygulama ile süreçlerin gözden geçirilip sorunların çözülmesi gerekir.
• Geçiş planı son defa gözden geçirilir, veri ile değerlendirmesi yapılır. Sistem geçişi için gerekli son hazırlıklar yapıldıktan sonra, önce sistem geçişi sonra veri geçişi sağlanır. Ama iş burada bitmez..
• Sonrasında ölçümler yapılır ve izlenir. Dokümantasyon kesinlikle unutulmamalıdır.

8. Bulut Bilişimin etkileyeceği sektörler

Bu araştırmanın sonucuna göre; bulut bilişimin telekom sektörü dışında medya, devlet, eğitim ve sağlık gibi sektörlere büyük etkisi olacak. Ülkemizde de aşağı yukarı aynı sıralamanın takip edileceği kanısındayım. Önce altyapıları bulut bilişim için nerdeyse hazır olan telekom sektörünün sonra sosyal medya ve sosyal ağlardaki gelişmeler neticesinde medya‟ nın buluta geçiş yapacağına, onu belediyeler gibi devlet kuruluşlarının takip edeceğine inanıyorum.

Bulut bilişimin gücüne bir başka örnek Animoto‟dan geliyor. Animoto müşterilerinin Facebook üzerinden fotoğraf ve müzik yüklemelerine izin veren ve paylaşımını sağlayan bir video sunumu hazırlamış olan bir şirket. Geçen sene başında günde yaklaşık 5,000 kişi kullanırken Nisan ayında 3 gün içinde 750,000 kişi kaydoluyor ve bir saatte 25,000 kişi yazılımı deniyor. Bu isteğe cevap verebilmek için şirket sunucularını 100‟e katlamak durumuyla baş başa kalınıyor. Bu hem sunucuların kurulması ve sonrasında da yönetim becerisini gerektiriyor. Bunun yerine hali hazırda birlikte çalıştıkları RightScale – bulut servisleri veren bir firma- yazılımlarını Bulut‟a göre ayarlıyor ve Amazon‟un servislerini kullanmaya başlıyorlar. Böylece sunucular yerine saati 10cent‟e Amazon‟dan servisi alıyorlar ve bazı depolama masrafları ile bant genişliğine para ödeyerek çok daha ucuza müşterilerini memnun edecek çözümü çok kısa sürede buluyorlar.

İlaç endüstrisi bulut bilişimi kullanma gücüyle ilgili çok güzel örnekler vermiş durumda. Bir ilaç şirketindeki bilim adamları Amazon‟un bulut servislerini kullanarak veri analizleri ve hastalıkların nasıl tedavi edilmesi gerektiği ile ilgili harcadıkları zamanı azaltmışlardır. Büyük veri setlerinin analizini 140 günden 6 güne indirmeyi bulut servislerini kullanarak başarmışlardır.

New York Times ise sadece kredi kartı ile aldığı Amazon‟dan EC2 ve S3 servisleri ile 4TB veri içeren 15 milyon civarındaki haberi scan edip pdf dosyası olarak online dağıtım için hazırlamıştır.
Nasdaq ise geçmiş hisse senedi ve tahvil bilgilerini kendi veritabanında tutmak yerine bir kredi kartıyla aldığı Amazon servisiyle Amazon bulutunda tutmaktadır-IaaS. Böylece eldeki eski verileri satarak da kar amacı sağlanmıştır.

9. Bulut Stratejisi

Yaklaşık son 30 yıldır, IT stratejisi milyonlarca liralık yeni teknoloji donanım ve yazılımı kullanma üzerine kurulmuştu. Pahallı yazılım paketleri kullanan büyük yeni sistemler kurulur ya da sıfırdan oluşturulurdu. Bu zahmetin başarı oranı ve yatırımın geri dönüşü - ROI – nazikçe söylemek gerekirse mütevazi olurdu. Artık bu stratejiler miatlarını doldurdular. Bugün artık iş isteklerine cevap verebilecek tutarlıkta değiller.

Artık sürekli değişen bir dünyada yaşıyoruz. Şirketler kompleks ve değişen problemlere standart yazılım paketleri ile çözüm arıyorlar. Şirketler bu yaklaşımla katı, aynı zamanda rakiplerinde olan IT sistem eşyalarına kendilerini kilitliyorlar. Böylece şirketin kendi iş durumunun gelişen ihtiyaçları değil, büyük yazlım evleri sistem değişikliklerinin kontrolünü ellerinde tutmuş oluyorlar.

Bulut Bilişim iyi ve kötü yanlarıyla doğru servislerin, doğru ihtiyaçların ve servis bazlı yönlendirme ile odağın, dikkatin iş üzerinde olmasını sağlar. Siyah ya da beyaz, herkese açık ya da özel, herkesin doğrusu kendi işinin stratejine göre farklı olacaktır. Dolayısıyla ortada herkes için tek doğru yoktur. Bu sebeple Bulut bilişime geçişte tüm seçenekler iyi değerlendirilmelidir.

Sonuç

Bulut sistemlerinin güçlü yönleri olarak düşük maliyet, erişim kolaylığı, kullanım kolaylığı, yüksek güvenlik standartları, veri aktarımı, veri saklama ve yedekleme kolaylığı faktörlerini; bulut sistemlerinin zayıf yönleri olarak çevrimiçi çalışma zorunluluğu, uygulamadaki kısıtlar, veri gizliliği, veri güvenliği ve performans faktörlerinin tespitti önemlidir.

Güçlü ve zayıf yönleri belirten bu iç faktörlerin yanında fırsat ve tehditleri gösteren dış faktörler de şu şekildedir: verilere gerçek zamanlı erişim, entegre uygulamalar, mobil uygulamalarda kullanım ve hareket esnekliği fırsat faktörlerini; sistemin çevrimdışı çalışmaması, güvenlik ihlalleri, sözleşme kaynaklı sorunlar ve yasal engeller ise tehdit faktörlerini göstermektedir.

İşletme yönetimleri, bilişim teknolojilerini; kendilerine rekabet avantajı ve üstünlüğü sunacak, belirsizlik ortamında gerek işletme varlığını sürdürme, gerekse de karar alma ve planlama konularında önemli bir stratejik araç olarak değerlendirmektedir. Birçok işletme bilgisayar kullanımının yaygınlaşmasıyla birlikte bilgi toplama, analiz ve raporlama faaliyetlerinde bilişim teknolojilerinden yararlanmaktadır. İşletmelere maliyet yönetiminde etkinlik sağlayan, maliyetlerin verimli bir şekilde yönetilmesine katkıda bulunan, kullanılabilir ve sürdürülebilir bir bilgi ağı ortamı sunan, yaygın ağ erişimi ve neredeyse sınırsız depolama kapasitesi ile bulut bilişim teknolojisi temel işletme fonksiyonlarına alternatif çözümler getirerek işletmelere birçok avantaj sunmaktadır. Bulut bilişim uygulamalarının temel bir işletme fonksiyonu olan muhasebeye yansıması bulut muhasebesi kavramını ortaya çıkarmıştır.

Bulut bilişim tabanlı yazılım uygulamaları, işletmelere maliyet ve zaman tasarrufu, esnek bir yapıda çalışma ve erişim kolaylığı gibi önemli ve rekabet üstünlüğü sağlayacak avantajlar kazandırmaktadır. Şirketler açısından bakacak olursak nelere dikkat etmeli sorusuna verebilecek cevaplar:

- Ufak ve orta şirketler Servis olarak sunulan bulut yazılım‟ı na –SaaS- ve halka açık ya da kamu bulutuna- public cloud- geçiş yapabilirler.
- Büyük şirketler kendi özel bulutlarını – private cloud- ya da karma bulutu – hybrid cloud- oluşturabilirler.
- Kamu kuruluşları ise herkese açık kamu bulutunu – public cloud- oluşturup kullanabilirler.

Sektörsel olarak baktığımda ise önce Telekom sektörünün ve hosting firmalarının Buluta geçiş yapıp, belki IT açısından kuvvetlerini böylece birleştirip topluluk bulutunu oluşturabileceklerini görüyorum. Daha sonra medya sektörünün sosyal ağları da arkasına alarak bulut servislerini kullanarak hayatımızı değiştireceklerine inanıyorum. Medyayı sağlık sektörünün ya da belediyelerin takip edeceğini sanıyorum. Özellikle sağlık kuruluşlarının bulut bilişimden faydalanarak sağlık verilerinin erişim hakları tanımlanmış yetkili kişi ve kuruluşlarca ulaşılabilir, her bireyin kendi kişisel sağlık verilerine erişebildiği, uluslararası standartlara uyumlu, karar destek sistemleri ile desteklenen, yüksek bant genişlikli ve tüm ülkeyi kapsayan bir iletişim omurgasında paylaşılmasını desteklenebilir.

Bulut bilişimde ilerleyen yıllarda dikkatle incelenmesi gereken konuları kendimce şöyle sıralayabilirim:

Yüksek erişimi sağlamak için mobil cihazlardan erişim, sensörler, akıllı ajanlar, dil çözümleme teknolojileri, semantik teknolojileri, RFID ve biyometrik teknolojileri, wifi, vimax ve geniş bant gibi altyapılar, sosyal yazılımlar için web 2.0 teknolojileri, güvenlik ve yasal gelişmeler yakından takip edilmelidir.

Bulut bilişim ile ilgili son trendlere baktığımızda güvenlik risklerini elimine etmek amacıyla New Servers gibi fiziksel olarak sunucuları da bulut ortamında sağlayan firmalara rastlamakta New Servers bulut ortamını fiziksel sunucularla kullanıcılarına özel sunmaktadır. Yüksek erişilebilirlik - High Availability (HA)- kavramından bahsediliyor. Bu kavram VMware Infrastructure 3 ile birlikte kritik uygulamalarda bozulan makinede çalışan sanal makinenin otomatik olarak sistem yöneticisinin müdahalesi olmadan diğer makineye geçirilmesidir.

Ayrıca servis kontratı içeriği de tartışılmaktadır. Özellikle hukuksal boyut gündemde, konuşuluyor. Servis kontratının hem veri şifrelemesini – encryption- hem de iletişim şifrelemesini – cryptography- içermesi gerektiği güvenlik düşünüldüğünde aşikardır. Bulut Bilişimde verinin bulunduğu yer dünyanın herhangi bir yeri olabileceğinden ve bazı ülkelerde şifre anahtarlarının devletle paylaşılmasının zorunlu olduğu düşünüldüğünde hukuksal boyutun mutlaka gözden geçirilmesi

gerekmektedir. Bu amaçla ISACA Cloud Security Alliance Controls Matrix oluşturulmuştur. Ekte bu matrisi bulabilirsiniz. Matriste bulut bilişim de dikkat edilmesi gereken güvenlik konuları güvenlikle ilgili çeşitli denetim kuruluşlarının da katkısıyla ele alınmış. Bulut Bilişim"de güvenliğin önemli olduğu düşünüldüğünde bu dokümanında mutlaka gözden geçirilmesi gerekir.

Sonuç olarak, Bulut Bilişim teknolojisi ile esnek alt yapıda sunulan her türlü bilgiye istek anında her yerden yetkisi olanların daha hızlı ve daha ucuz erişebilmesi sağlanarak her türlü hizmet çok daha başarılı verilecektir. Uygulamaya geçmek için tüm dönüşümler irdelenmeli ve eldekiler gözden geçirilmeli, gerekli hazırlıklar yapılmalı. Daha sonra hazırlanacak proje çerçevesinde ekonomisi de göz önüne alınarak Bulut Bilişime geçiş yapılırken pilot uygulamaya, dokümantasyona önem verilmelidir.

Kaynaklar

[1] Mell, P. and Grance, T., "The NIST Definition of Cloud Computing". National Institute of Standards and Technology, Information Technology Laboratory. NIST SP 800-145. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf (2009).

[2] Pearson, S., "Privacy, Security and Trust in Cloud Computing". HP Laboratories. HPL-2012-80R1 (2012).

[3] Google App Engine, https://developers.google.com/appengine/

[4] Engine Yard, http://www.engineyard.com/

[5] Force.com, http://www.force.com/

[6] Heroku, http://www.heroku.com/

[7] VMware, http://www.vmware.com/

[8] Amazon Web Services, http://aws.amazon.com/

[9] Windows Azure, http://www.windowsazure.com/

[10] GoogleDrive, https://drive.google.com/

[11] SkyDrive, https://skydrive.live.com/

[12] Dropbox, https://www.dropbox.com/

[13) box, https://www.box.com/

[14] White Paper, "Amazon Web Services: Overview of Security Processes", Amazon Web Services (AWS), May 2019.

[15] Amazon Elastic Compute Cloud (EC2), http://aws.amazon.com/ec2/

[16] IBM SmartCloud Resilience, http://www-935.ibm.com/services/us/en/it-services/smartcloud-resilience-services.html

[17] Cyber-Ark, http://www.cyber-ark.com/

[18] Microsoft SQL Azure Service Level Agreement, http://download.microsoft.com/download/B/0/9/B09851E2-6177-4A62-83AB-3B591659CE1E/SQL%20Azure/SQL%20Azure%20SLA-English.doc