BM 482 BİLGİSAYAR AĞLARI DERSİ

VİZE ARAŞTIRMA ÖDEVİ

Ayben GÜLNAR-191180041

NİSAN 2023

İçindekiler Tablosu

Şekiller Listesi

Tablolar Listesi

1.ÖZET

Günümüzde işletmelerin bulut bilişim hizmetlerinden yararlanma oranı hızla artmaktadır. Bu hizmetler sayesinde işletmeler, BT altyapılarını kurmak ve işletmek için gereken maliyetleri azaltabilirler. Bununla birlikte, işletmelerin büyümesi ve bulut bilişim teknolojilerinin gelişmesi, tek bir bulut sağlayıcısına bağımlılık riskini arttırmaktadır. İşletmeler, farklı bulut sağlayıcılarından hizmetleri alarak, kaynaklarını çeşitlendirebilir ve bulut hizmetlerindeki potansiyel riskleri azaltabilirler. Bu noktada, "multicloud" konusu önem kazanır. Multicloud, farklı bulut sağlayıcılarından hizmetleri kullanarak, işletmelerin bulut tabanlı uygulama ve hizmetlerinin performansını ve esnekliğini arttıran bir yaklaşımdır. Multicloud, birçok avantaj sunarken, işletmelerin bulut bilişim altyapılarının yönetimi ve güvenliği gibi zorluklarla da karşılaşabilecekleri anlamına gelir. Bu zorlukların üstesinden gelmek için, işletmeler bulut bilişim güvenliği için doğru stratejileri benimsemeli ve uygun araçları kullanmalıdırlar.

Tabii ki, buluttan bahsederken çoğumuz bugün sahip olduğumuz büyük halka açık bulut tekliflerini düşüneceğiz: AWS, Microsoft Azure ve GCP. Başka bir tanıma göre, çoklu bulut, bu farklı platformlardan en iyi çözümleri bir araya getirerek işletme için ek değer yaratan bir çözüm ve/veya hizmettir. Bu nedenle, bulut kullanmak, ya halka açık bulutta çözüm ve hizmetlerin bir kombinasyonunu ya da özel bulut çözümleriyle birleştirilerek olabilir [1].

Araştırmamda, Multi-Cloud Networking konusuna değinilmiş olup ve konu birçok farklı açıdan ele alınmıştır. İlk olarak Cloud Computing ve Multicloud kavramları tanımlanmış ve çeşitli Multicloud türleri incelenmiş. Daha sonra Multicloud'un fırsat ve zorluklarına değinilmiş ve kullanım case'leri ile örnekler verilmiş. Bu bölümlerden sonra, Multicloud hizmet sağlayıcıları için bulut bilişim güvenliği ele alınmış ve çeşitli faktörler incelenmiş. Ardından Multicloud Networking'de performans ve Multicloud Networking software'larının tanımı ve nasıl çalıştığı konuları ele alınmıştır. Daha sonra bu yazılımların faydaları ve zorlukları üzerinde durulmuş ve bu yazılımların çeşitli örnekleri incelenmiştir. Ayrıca bu yazılımların kullanım alanları da örneklerle ele alınmıştır. Ardından, Virtual Application Networks (VAN) for Multi-Cloud, Multi-Cluster and Cloud-Edge Interconnect konusuna değinilmiş ve bu konuda bilgi verilmiştir. Son olarak, Agile Risk Management for Multi-Cloud Software Development ve New Open-Source Multi-Cloud Asset to Build SaaS konularına da değinilmiştir. Bu içerikte, Multi-Cloud Networking konusu detaylı bir şekilde ele alınmış ve konuya dair birçok farklı açıdan bilgi verilmiştir.

2.MULTİCLOUD NETWORKİNG TANIM VE KAVRAMLARI

2.1 Cloud Computing ve Multicloud Kavramları

Bulut bilişim, internet üzerinden ihtiyaç duyulan anda IT kaynakları ve işlevlerinin sağlanması ve ölçeklendirilebilmesi anlamına gelir. Fiziksel olarak veri merkezleri ve sunucuların satın alınması, sahip olunması ve bakımının yapılması yerine, Amazon Web Services (AWS) gibi bir bulut sağlayıcısından hesapta ihtiyaç duyulan teknoloji hizmetlerine erişmek mümkündür[2].

Multicloud, birden fazla bulut sağlayıcısından bulut hizmetlerinin kullanımıdır ve işletmelerde giderek daha yaygın hale gelmektedir. Farklı sağlayıcılardan birden çok yazılım hizmeti kullanmak kadar basit olabileceği gibi, genellikle Amazon Web Services (AWS), Google Cloud Platform, IBM Cloud ve Microsoft Azure gibi birden çok bulut hizmeti sağlayıcısından platform hizmeti (PaaS) veya altyapı hizmeti (IaaS) üzerinde kurumsal uygulamalar çalıştırmayı ifade eder. Multicloud çözümlerinin farklı bulut sağlayıcılarının altyapılarına taşınabilir olmasını sağlamak için, genellikle tüm halka açık bulut sağlayıcıları tarafından desteklenen Kubernetes gibi açık kaynaklı, bulut doğal teknolojiler üzerine kurulmuştur. Ayrıca, birden çok bulutta iş yüklerinin merkezi bir konsolda yönetilmesi için genellikle "tek pencere" olarak adlandırılan yetenekleri içerirler. Önde gelen bulut sağlayıcıları ve VMware gibi bulut çözüm sağlayıcıları, hesaplama altyapısı, geliştirme, veri depolama, bulut depolama, yapay zeka (AI), makine öğrenimi (ML), felaket kurtarma ve iş sürekliliği gibi çeşitli kullanım durumları için çeşitli multicloud çözümleri sunarlar. Multicloud çözümlerinin sağladığı esneklik ve ölçeklenebilirlik ile, işletmeler bulut kaynaklarını daha etkili bir şekilde kullanabilir ve benzersiz ihtiyaçlarını karşılamak için bulut stratejilerini optimize edebilirler [3].

2.2 Multicloud'un Farklı Türleri

Mimari açısından, çoklu bulut modeli merkezi veya merkezi olmayan tipler olarak kategorize edilebilir. Bu bölümde, iş gereksinimleri açısından dört farklı türde çoklu bulut modeline daha ayrıntılı olarak değineceğiz. Amaç, bu modellerin kullanıcıların çeşitli ve gelişen iş taleplerine nasıl hizmet ettiği ve mevcut merkezi bulut bilişim modeline nasıl tamamlayıcı olduğunu açıklamaktır. Coğrafi olarak dağıtılmış bulut, hibrit bulut ve federatif bulut adı verilen ilk üç çoklu bulut modeli merkezi bir yapıya sahipken, dördüncüsü olan merkezi olmayan bulut, merkezi olmayan bir bulut mimarisi ile çalışır.

Coğrafi olarak dağıtılmış bulut, Amazon, Google ve Microsoft gibi büyük bulut sağlayıcıları dünya genelinde büyük veri merkezleri kurarak konum çeşitliliğinden yararlanabilirler. Dağıtılmış bulutlar, daha düşük hizmet gecikmesi, daha iyi yük dengeleme ve daha iyi

performans (örneğin, hizmet güvenilirliği ve kullanılabilirliği) için bulut hizmetleri sağlayabilirler. Örneğin, çevrimiçi içerik hizmeti sağlayıcılarından Netflix, kullanıcıların dünya genelinde Netflix videolarını hızlı bir şekilde izlemelerine olanak tanımak için Amazon dağıtılmış bulutlarında hizmetlerini dağıtır. Özünde, coğrafi olarak dağıtılmış bulut, geleneksel merkezi bulutun yatay bir genişlemesidir. Tüm kaynaklar hala aynı varlık tarafından sahip olunur. Bu nedenle, kullanıcıları hala veri güvenliği, gizlilik ve tedarikçi bağımlılığı sorunlarıyla karşı karşıya kalır.

Hybrid cloud, yani karma bulut, özellikle büyük şirketler olmak üzere birçok şirketin farklı sebeplerle hala kendi özel veri merkezlerine sahip olduğu bir modeldir. Bu sebepler arasında en önemlisi, veri güvenliği ve gizliliği konusudur. Ancak, devasa bulut veri merkezleriyle karşılaştırıldığında, kendi veri merkezleri nispeten küçük ve kaynak esnekliği açısından daha az etkilidir. Bu nedenle, önemli olan hizmetlerini ve verilerini kendi özel veri merkezlerinde, diğer daha az önemli iş yüklerini ise genel bulutta barındırarak karma bir hesaplama modeli kullanmayı tercih ederler. Birçok literatürde bu, patlayıcı iş yükünün buluta taşınması olarak adlandırılır. Dropbox gibi karma bulut modelinin iyi bir örneğinde, dosya sisteminin meta verileri kendi özel veri merkezlerinde saklanır ve kullanıcı verileri şifrelendikten sonra bulutta saklanır. Karma bulutun yardımıyla, işletmeler kritik hizmetlerini kendi özel veri merkezlerinde kullanabilir ve görev açısından önemsiz iş yüklerini genel buluta gönderebilirler.

Federated cloud. Küçük veri merkezlerinin kapasitesini genişletmenin başka bir yolu federasyondur ve bu, birden çok kaynak sağlayıcısından kaynakları tek bir kaynak havuzuna toplar. Dağıtılmış ve hibrit bulut modellerinden farklı olarak, federasyon bulutundaki her katılımcı kaynak sağlayıcıları ve tüketicileridir. Federasyon bulutundaki tüm katılımcılar birbirlerine güvenir. Federasyon bulutundaki kaynaklar, tüm katılımcılar tarafından tanınan merkezi bir kurum tarafından yönetilir. Merkezi kurum ayrıca, katılımcıların birbirinden kaynak talep etmelerine ve kaynak tahsis etmelerine izin veren bir bulut etkileşim katmanı da uygular. Bulut federasyonu sayesinde, her katılımcı daha fazla donanım yatırımı yapmadan daha fazla kapasite elde edebilir. Federasyonlu bir bulutu tanımlamak için kullanılan başka bir benzer terim de "bulutların bulutu"dur. Burada, kaynak sağlayıcıları halka açık ticari bulutların bir kombinasyonudur. Ancak, bulutların bulutunda, her bulut sadece kaynak sağlayıcısıdır ve diğerlerinden kaynak kullanmaz. Bulutların bulutunun ana amacı, tek bir bulut modelinin sınırlamalarını aşmak için kaynak sağlayıcılarına çeşitlilik eklemektir.

Decentralized cloud, yani merkezi olmayan bulut bilişim modelinde, kaynaklar bir grup birey veya küçük organizasyon tarafından eşler arası bir şekilde katkıda bulunulur ve paylaşılır.

Federated cloud ile benzer şekilde, merkezi olmayan bulutta her bir eş, kaynak sağlayıcısı ve tüketici olarak hareket eder. Ancak, merkezi olmayan bulutta bulunan eşler, kendi taleplerine göre buluta katılmak veya buluttan ayrılmak için daha demokratik haklara sahiptir. Ayrıca, tüm katılımcılar, farklı tercihlere dayalı olarak stratejilerin uygulandığı bir stratejik ortamda kaynak tahsisi konusunda kararlarını verebilirler (örneğin, konum yakınlığı, gizlilik endişeleri, yasal kısıtlamalar vb.). İyi bir örnek olarak SpotCloud (şimdi EMC tarafından satın alındı) verilebilir. Bu platform, bulut kaynaklarının alıcılarını ve satıcılarını bir araya getirerek çevrimiçi bir pazar sağlar. Kaynak sağlayıcıları, boşta kalan kaynaklarını para kazanmak için kullanabilirken, son kullanıcılar da performans, maliyet ve konum parametrelerine göre çeşitli kaynak sağlayıcıları arasından kaynak seçerek faydalanabilirler [4].

2.3 Multicloud, Hybrid Cloud And Hybrid Multicloud

Hybrid bulut hem kamusal hem de özel bulut ortamlarının kullanımını ifade eder ve bunların tek bir optimize edilmiş BT altyapısı olarak yönetilmesine, orkestrasyonuna ve kullanılmasına olanak tanır. Hybrid ve multicloud terimleri sık sık birbirinin yerine kullanılsa da, hybrid multicloud, iki veya daha fazla bulut sağlayıcısından kamusal veya özel bulut hizmetlerinin kullanımını ifade eder. Hybrid multicloud, geliştirici üretkenliğini artıran, geliştirme yöntemlerini ve bulut doğalı uygulama teknolojilerini, örneğin mikro hizmet mimarisi, konteynerlar ve sunucusuz bilgi işlemi mümkün kılan birçok fayda sağlar.

Hybrid multicloud'un önemli avantajlarından biri, geliştirici üretkenliğini önemli ölçüde artırabilen Agile ve DevOps geliştirme yöntemleri ve bulut doğalı uygulama teknolojilerine erişim sağlamasıdır. Ek olarak, multicloud ortamlarında mevcut olan en iyi güvenlik ve uyumluluk teknolojilerine erişim sağlayarak, organizasyonların hassas verileri veya yüksek düzenlemeli yükleri güvenli ve uyumlu bir şekilde dağıtmasına ve ölçeklendirmesine olanak tanır.

Hybrid multicloud ayrıca, iş yüklerinin nerede dağıtıldığı ve ölçeklendirildiği konusunda daha fazla esneklik ve kontrol sunarak, organizasyonların kullanıcılara daha yakın bir konuma dağıtarak performansı optimize etmelerine ve gecikmeleri azaltmalarına olanak tanır. Bu da, şirketlerin en maliyet-etkin bulut hizmetini seçmelerine ve mevcut uygulamaları daha hızlı modernize etmelerine yardımcı olarak verimliliği ve maliyet optimizasyonunu artırır. Dahası, hybrid bulut, bulut hizmetlerini bulut veya yerinde altyapıdaki verilerle bağlayarak, organizasyonlara yeni değerler sağlar [5].

2.3 Multicloud Fırsat ve Zorlukları

Multicloud hizmetlerinden yararlanmak, IT esnekliğini ve ölçeklenebilirliğini artırmak için birçok fırsat sunabilir. Multicloud'un en yaygın faydaları:

Multicloud, birçok bulut sağlayıcısından seçim yapmanıza ve belirli özellikleri ve yetenekleri eşleştirmenize olanak tanır, böylece bulutta iş yüklerinizi optimize etmek için hız, performans, güvenilirlik, coğrafi konum ve güvenlik ve uyumluluk gereksinimleri gibi faktörlere göre karar verebilirsiniz.

Multicloud ortamı, herhangi bir yerde hızlı bir şekilde oluşturmanıza olanak tanır. Multicloud yaklaşımıyla bir sağlayıcıya bağlı kalmazsınız. Tek bir buluta çok bağımlı olduğunuzda ortaya çıkan veri, uyumluluk ve maliyet sorunlarını azaltırken işletmenizin gereksinimlerine en uygun çözümü seçebilirsiniz

Multicloud ortamları, IT harcamalarınızı en aza indirmek için iyi bir seçenek olabilir. Halka açık bulut, ihtiyacınıza göre ölçeklendirmenize izin verirken daha az işletme gideri ile birlikte gelir. Farklı sağlayıcılar arasındaki en iyi fiyatlandırma ve performans kombinasyonundan yararlanarak TCO'yu düşürebilirsiniz.

Bulut sağlayıcıları sürekli olarak yeni ürünler ve hizmetler geliştiriyorlar. Multicloud, size, tek bir bulut sağlayıcısının sunduğu seçeneklerle sınırlı kalmadan yeni teknolojileri benimseyerek kendi sunumunuzu geliştirmenize olanak tanır.

Multicloud stratejisi, hizmet, sağlayıcı veya ortamdan bağımsız olarak tüm iş yüklerinizde güvenlik politikalarını ve uyumluluk teknolojilerini tutarlı bir şekilde uygulamanızı sağlar.

Multicloud, tek bir nokta arızası riskini azaltarak planlanmamış kesinti veya kesinti süresini azaltır. Bir bulutta bir kesinti olursa, diğer bulutlardaki hizmetleri etkilemeyecektir ve eğer bulutunuz düşerse, hesaplama ihtiyaçlarınız başka bir hazır buluta yönlendirilebilir [3].

Çoklu bulutun birçok avantajına rağmen, bazı organizasyonlar için zorlu bir yönü de vardır. En yaygın çoklu bulut zorlukları arasında artan yönetim karmaşıklığı, tutarlı güvenlik sağlama, yazılım ortamlarını entegre etme ve bulutlar arasında tutarlı performans ve güvenilirlik sağlama yer alır.

Çoklu bulut stratejisi, iş gereksinimlerini, tasarım ve geliştirme faktörlerini ve mevcut sistemlerden kaynaklanabilecek herhangi bir mimari kısıtlamayı dikkate almalıdır. Mevcut bilgi işlem ortamınızı neden taşımak istediğinizi, halka açık bulutta optimize etmek istediğiniz

anahtar ölçümleri ve organizasyonunuzda çoklu bulut kurulumunu kullanma uzun vadeli planınızı net bir vizyon belgesinde açıkça tanımlamak için zaman ayırmak önemlidir [5].

2.4 Multicloud Kullanım Case ve Örnekleri

Multicloud, organizasyonların müşterilerine daha iyi hizmet etmelerine yardımcı olacak bir dizi fırsat sunar. İşte bazı yaygın kullanım durumları:

Afet Kurtarma: Multicloud, kritik uygulamalarınızı yedeklemenize izin verir. Bir felaket veya tek bir tedarikçi kesintisi durumunda, diğer sağlayıcılara güvenebilirsiniz.

Dünya genelinde daha iyi gecikme süresi: Küresel bir organizasyon için, multicloud düşük gecikme süresi ile daha iyi bağlantılar sağlayarak farklı konumlardaki sunuculara erişmenize yardımcı olabilir ve müşterilere daha iyi hizmet sunabilirsiniz.

Bölgesel gereksinimler: Multicloud, farklı sağlayıcılardan on-premises, özel ve halka açık manzaralar arasında geçiş yapabilme imkanıyla bölgesel özel uyum kurallarına uymayı sağlar.

Multicloud stratejisi sunan birçok teknoloji şirketi vardır. Bu şirketler arasında AWS, Microsoft Azure, Google Cloud, IBM Cloud, Oracle Cloud, VMware Cloud, Red Hat OpenShift ve Dell Technologies gibi önde gelen isimler yer alır. Bunlar, müşterilerine birden fazla bulut sağlayıcısından hizmet seçenekleri sunarak, farklı ihtiyaçlara göre en uygun çözümleri sağlamaya yardımcı olurlar [5].

3.MULTICLOUD HİZMET SAĞLAYICILARI İÇİN BULUT BİLİŞİM GÜVENLİĞİ

3.1 Kimlik ve Erişim

Çoklu bulut hizmeti sağlayıcıları, sistemlerinin ve verilerinin yetkisiz erişime karşı güvenli olduğundan ve müşterilerinin verilerinin korunduğundan emin olmak zorundadır. Müşterilerine sunulan hizmetlerin kesintisiz bir şekilde çalıştığından ve müşteri verilerinin kaybolmadığından veya bozulmadığından emin olmak da gereklidir. Bu nedenle, çoklu bulut hizmeti sağlayıcıları, sistemlerini ve verilerini korumak için güçlü güvenlik politikaları ve prosedürleri uygulamalı ve sürdürmelidirler. Müşteri için yeni veya tanımlanamayan risklerin oluşmaması için risk değerlendirme planlarına sahip olmaları da gereklidir.

Bulut güvenliği, fiziksel altyapıdan başlayarak uygulama ve verilere kadar uzanan çok katmanlı bir yaklaşımdır. Çoklu bulut hizmeti sağlayıcıları için, bu tüm bulutun veri merkezinden uygulama katmanına kadar her yönünü kapsayan bir güvenlik planı oluşturmayı ve bu plana

sıkı sıkıya uymayı gerektirir. Fiziksel altyapı, veri merkezi, ağ altyapısı ve bulutu oluşturan bilgisayarlar ve depolama da dahil olmak üzere bulut güvenliğinin ilk katmanıdır. Uygulama katmanı, bulutta çalışan uygulamaları korur: web uygulamaları, mobil uygulamalar ve API güvenliği gibi. Veri katmanı, bulutta depolanan verileri korur. Bu katman, veri şifreleme, yedekleme ve kurtarma yöntemlerini içerir.

Çoklu bulut hizmeti sağlayıcıları, veri merkezinin, ağ altyapısının, sunucuların ve depolamanın, uygulama geliştirme sürecinin ve bulutta depolanan verilerin güvenliğini sağlayan kapsamlı bir güvenlik programı uygulamalıdır. Multi-cloud hizmet sağlayıcıları, bulut güvenliğini sağlamak için kapsamlı bir IAM (Kimlik ve Erişim Yönetimi) planı da uygulamalıdır. IAM, kullanıcı hesaplarının, kimlik doğrulamanın ve yetkilendirmenin yönetimini içerir. Çoklu bulut hizmet sağlayıcıları için IAM, ACL'ler için yönlendirme sağlayarak bulutta bulunan verilere ve kaynaklara erişimi kontrol etmeye yardımcı olur. Yetkili kullanıcılara erişimi sınırlandırarak IAM, yetkisiz erişimi önlemeye ve iş sürekliliğini sağlamaya yardımcı olur. Bulut verilerini güvende tutmak için çoklu bulut hizmet sağlayıcıları için güçlü bir IAM çözümü gereklidir. Bu çözüm, bulutta bulunan veri ve kaynaklar için kullanıcı hesaplarının, kimlik doğrulamanın, yetkilendirmenin ve ACL'lerin yönetimini içermelidir.

Çoklu bulut hizmeti sağlayıcıları, sistem ve verilerinin yetkisiz erişime karşı güvende olduğundan ve müşterilerinin verilerinin korunduğundan emin olmak zorundadır. Ayrıca, sistemlerinin sürekli olarak kullanılabilir olmasını ve müşteri verilerinin kaybedilmemesini veya bozulmamasını sağlamalıdırlar. Bu nedenle, çoklu bulut hizmet sağlayıcıları güçlü bir güvenlik politikası ve prosedürleri uygulamalı ve sürdürmelidir. Ayrıca, müşteri için bulut üzerindeki sistem ve verilerin yeni veya tanımlanamayan riskler oluşturmadığından emin olmak için bir risk değerlendirme planı olmalıdır.

Bulut güvenliği çok katmanlı bir yaklaşımdır ve fiziksel altyapıdan uygulamalara ve bulutta çalışan verilere kadar uzanır. Çoklu bulut hizmeti sağlayıcıları için, bu, veri merkezinden uygulama katmanına kadar bulutun tüm yönlerini kapsayan sıkı bir güvenlik planının oluşturulması ve bunun takip edilmesi anlamına gelir. Fiziksel altyapı, veri merkezini, ağ altyapısını ve bulutu oluşturan bilgisayarları ve depolamayı içeren bulut güvenliğinin ilk katmanıdır. Bu ayrıca çoklu bulut hizmeti sağlayıcıları için veri merkezi altyapısının güvenliğini de sağlar. Daha sonra, uygulama katmanı bulutta çalışan uygulamaları korur: web uygulamaları, mobil uygulamalar ve API güvenliği gibi. Çoklu bulut hizmeti sağlayıcıları için, bu aynı zamanda kalite güvencesi ve güvenlik uygunluğu dahil uygulama geliştirme sürecinin güvenliğini de sağlar. Bulut güvenliğinin son katmanı veri katmanıdır ve bulutta depolanan

verileri korur. Bu katmanda veri şifreleme, veri yedeklemeleri ve veri kurtarma yöntemleri bulunur.

Bunun yanı sıra, çoklu bulut hizmeti sağlayıcıları bulut güvenliğini sağlamak için kapsamlı bir IAM (Kimlik ve Erişim Yönetimi) planı uygulamalıdır. IAM, kullanıcı hesaplarını, kimlik doğrulamasını ve yetkilendirmeyi yönetmeyi içerir. Çoklu bulut hizmeti sağlayıcıları için IAM, ACL'lerin yönlendirilmesi yoluyla bulutta bulunan verilere ve kaynaklara erişimi kontrol eder. Verileri bulutta güvence altına alırken üç önemli hususu dikkate almak gerekir: istirahatteki veriler, aktif veriler ve veri şifrelemesi. Veriler istirahatteyken bir sunucuda veya sabit diskte saklanır. Bu verileri korumak için organizasyonlar BitLocker veya FileVault gibi araçlar kullanarak verilerini şifreleyebilirler. Veri şifrelemesi, izinsiz kullanıcıların verilere erişmelerini zorlaştırır. Veriler aktifken bir yerden başka bir yere gönderilirken VPN veya TLS/SSL gibi araçlar kullanılarak veriler şifrelenebilir. Veri şifrelemesi, izinsiz kullanıcıların verileri ele geçirmesini ve okumasını zorlaştırır. Veri şifrelemesi verileri kodlama işlemi ile korur ve bu güvenlik önlemi hem istirahatteki verileri hem de aktif verileri korur. Bulut hizmeti sağlayıcısı seçerken veri güvenliğinin üç yönünü de dikkate almak gerekir. Çoklu bulut hizmeti sağlayıcıları, veri şifrelemesi, VPN veya TLS/SSL gibi veri güvenliği özellikleri sunmalıdırlar.

Bilgisayarlar, dizüstü bilgisayarlar ve masaüstü bilgisayarlar, verilerin yetkisiz erişimden korunması için yerleşik güvenlik özellikleri içerirler. Bununla birlikte, dosyaları bulutta saklamadan önce bireyler ve organizasyonlar, dosyaları daha fazla güvence altına almak için ilave önlemler alabilirler. BitLocker ve FileVault, sabit diskleri şifreleyerek ve uygun kimlik bilgilerine sahip olmayan kimselere hassas verilere erişimi önleyerek güvenlik sağlayan iki popüler seçenektir. BitLocker, belirli Windows sürümlerine dahil edilmiş bir özelliktir ve diğer sürümlere ek olarak sunulur. Verileri doğru anahtar olmadan okunamaz hale getirmek için Advanced Encryption Standard (AES) yöntemini kullanır. BitLocker, bir sabit diski veya belirli bölümleri veya hacimleri şifrelemek için ayarlanabilir. FileVault da macOS ile birlikte gelen benzer bir araçtır. Verileri korumak için AES şifrelemesi kullanır ve tıpkı BitLocker gibi tüm sabit diski veya yalnızca belirli hacimleri şifrelemek için kullanılabilir. FileVault'un bir avantajı, makinenin başlangıç diskinin şifrelenmesidir, bu da birinin söz konusu bilgisayara fiziksel erişimi olsa bile izinsiz erişimi önlemeye yardımcı olur.

Offline veri yedeklemeleri, şirket verilerine veya sistemlere kötü amaçlı aktörlerin eriştiği ve şifrelediği zaman, verilerin kaybedilmemesini sağlayarak bu tür saldırılara karşı koruma sağlar.

Herhangi bir güvenlik politikası, aşağıdaki faktörleri hesaba katmalıdır:

1. Hangi veri güvenlik özellikleri mevcut?
2. Veri güvenliği ihlalleri nasıl ele alınıyor?
3. Çalışanlara hangi veri güvenliği eğitimleri veriliyor?
4. Hangi üçüncü taraf güvenlik denetimleri yapılmış?
5. Bir veri güvenliği ihlali durumunda olaya müdahale planı nedir?

Veri güvenliği konusunda her üç faktör de dikkate alınmalıdır: veri dinleniyor durumda iken, veri aktarılırken ve veri şifrelemesi. Veri dinleniyor durumdayken, veriler bir sunucuda veya sabit diskte depolanır. Kuruluşlar, verilerini BitLocker veya FileVault gibi araçlar kullanarak şifreleyebilirler.

Veri şifrelemesi, izinsiz kullanıcıların verilere erişmesini zorlaştırır, hatta sunucuya veya sabit diske fiziksel erişimi olsa bile. Veri aktarılırken, veriler bir yerden başka bir yere gönderilmektedir. Kuruluşlar, verilerini korumak için bir VPN veya TLS / SSL kullanarak şifreleyebilirler. Benzer şekilde, veri şifrelemesi, verilerin gönderilirken izinsiz kullanıcıların verileri ele geçirmesini ve okumasını zorlaştırır [4].

3.2 Çıkış/Giriş Trafik Kontrolü

Egress trafiği, bulut ortamından ayrılan verileri ifade ederken, ingress trafiği ise buluta giren verileri ifade eder. Egress trafiği ile ilgili en ciddi risklerden biri, verilerin uygun şekilde şifrelenmemesi veya güvenlik duvarındaki açıklar nedeniyle veri sızıntısının meydana gelmesidir. Veri sızıntısını önlemek için, çoklu bulut sağlayıcıları tüm bilgilerin transit ve dinlenme sırasında şifrelenmiş olduğundan emin olmalıdır. Ayrıca, çok katmanlı güvenlikli bir güvenlik çevresi kurmalıdırlar. Ingress trafiği de bir güvenlik endişesi olabilir ve kötü niyetli aktörlere bulut ortamına erişim izni verir. Bunun önlenmesi için, çoklu bulut sağlayıcıları sağlam bir güvenlik duvarı, intrusion detection ve prevention sistemleri ve tüm ortama giren verilerin kötü amaçlı yazılım ve virüsler için tarandığından emin olmalıdırlar. IP whitelist mekanizmaları, bulut ACL'leri ve güvenlik duvarı yapılandırmaları, sıfır günlük saldırılar gibi herhangi şüpheli aktivitenin proaktif olarak tespit edilmesini sağlamak için yüksek güvenlikli olmalıdır [4].

3.3 Bulut Güvenliğinde Dikkate Alınacak Faktörler

Bir bulut bilişim güvenliği stratejisi geliştirilirken dikkate alınması gereken birkaç temel faktör vardır. Bunlar, korunması gereken veri ve kaynaklar, gereken güvenlik seviyesi ve mevcut bütçe gibi unsurlardır. Kapsanması gereken veri ve kaynak türleri işletmeye ve sektöre göre değişebilir: örneğin, sağlık kuruluşları perakende kuruluşlarınınkinden farklı güvenlik

gereksinimlerine sahiptir. Benzer şekilde, gereken güvenlik seviyesi de işletmeye ve sektöre göre değişecektir. Bazı durumlarda, düzenlemelere uyum belirli bir güvenlik seviyesini gerektirebilir. Diğer durumlarda, işletme belirli bir koruma düzeyini tercih edebilir. Mevcut bütçe de bulut bilişim güvenliği stratejisi açısından önemlidir. Bazı durumlarda, güvenlik önlemlerinin maliyeti yüksek olabilir. Diğer durumlarda, verileri ve kaynakları korumak için yapılan yatırımın maliyeti değerli olabilir. Küçük ve orta ölçekli işletmeler, birçok durumda pahalı bulut hizmetleri yerine zaten geliştirilmiş dahili araçları benimseyebilirler. Açık kaynak çözümlerini benimsemek de mümkündür, örneğin detect-secret modülü kaynak kontrolünde herhangi bir gizli belirteç, şifre veya özel anahtarın yanlışlıkla taahhüt edilmesini önlemek için kullanılabilir. Prowler, çeşitli uyumluluk çerçevelerini kapsayan birçok güvenlik denetimini, olay yanıtını, sürekli izlemeyi, adli hazırlığı ve güvenlik değerlendirmelerini sağlayan başka bir açık kaynak güvenlik aracıdır. Bulut bilişim güvenliği stratejisi düzenli olarak gözden geçirilmeli ve güncellenmelidir. Bu düzenli kalite güvence incelemesi, planın yetkisiz erişim, açıklama veya yok edilme yoluyla verileri ve kaynakları korumada etkili kalmasını sağlar. Buna göre, en yaygın siber suçlu taktikleri, teknikleri ve prosedürleri göz önünde bulunduran kapsamlı bir bulut bilişim güvenliği stratejisine sahip olmak önemlidir [4].

4.MULTİ-CLOUD NETWORKİNG'DE PERFORMANS

Birçok organizasyon için bulut altyapı yeteneklerini ve harcamalarını optimize etmek için, çoklu bulut dağıtımı her şeyin en iyisi bir yaklaşım olabilir. Bu yapılandırma, organizasyonların iş yüklerini birden fazla bulut sağlayıcısına dağıtmalarına izin verir. İdeal olarak, bulutlar birbirleriyle etkileşimli ve bağlantılıdır, böylece kullanıcılar bunları kolayca birbirine bağlayabilirler. Ancak, bu yetenek, başarılı bir çoklu bulut dağıtımı kurulumunda en önemli zorluklardan birini sunar.

Bulut veri tabanı hizmetleri, şirketlere kendi veri merkezlerinde veri tabanı sistemlerini geliştirme ve işletme konusunda göreli avantajlar sunar. Ancak, organizasyonlar bulutun ölçeklenebilirliği ve çevikliğini benimserken, uzun vadede her ihtiyacı karşılayamayan bir sağlayıcıya bağlı kalma konusunda endişeli olabilirler.

Burada, çoklu bulutun avantajları vardır. Çoklu bulut yaklaşımı, organizasyonlara daha kolay bir göç, daha büyük ölçeklenebilirlik ve çeviklik, sağlam felaket kurtarma, farklı bulut sağlayıcıların sunduğu benzersiz yeteneklere erişme ve hizmetler için rekabetçi fiyat avantajı gibi faydalar sağlar. Organizasyonlar ayrıca tek bir bulut sağlayıcısına olan bağımlılıklarını

azaltarak, sağlayıcılar arasında taşınabilirliği artırarak iş sürekliliği ve felaket kurtarma gücünü artırabilirler [7].

5.MULTİ-CLOUD NETWORKİNG SOFTWARE NEDİR?

Bu konuda kaynakçam da belirttiğim üzere çok kaynak bulamadığım için bir araştırma için hazırlanan Gartner raporundan edindiğim bilgilere göre [8]:

Günümüzde birçok şirket, verileri ve uygulamaları depolamak, işlemek ve yönetmek için bulut teknolojisini kullanıyor. Genel bulut sağlayıcıları, bu işletmeler için kullanımı kolay ve uygun maliyetli bir seçenek olabilir. Ancak, özellikle büyük ve karmaşık olan bazı işletmelerin ihtiyaçları, genel bulut sağlayıcılarının yerleşik ağ oluşturma yetenekleri tarafından karşılanamayabilir. Kuruluşlar, birden çok bulut sağlayıcısından bulut kaynaklarını yönetmek ve bunlara erişmek için farklı çoklu bulut yazılımları seçer. Bu yazılımlar, bulut kaynakları arasında ağ bağlantıları oluşturarak veri aktarım işlemlerinin daha hızlı ve güvenli bir şekilde yapılmasını sağlar. Ayrıca şirketler, bulut kaynaklarını daha esnek bir şekilde yönetebilir ve iş ihtiyaçlarına göre değiştirebilir. Bu yazılımların yardımıyla şirketler, farklı bulut hizmetlerinden faydalanabilir ve iş ihtiyaçlarına uygun bir bulut çözümü oluşturabilir. Bulut bilgi işlem, işletmelerin kaynakları hızla ve esnek bir şekilde ölçeklendirmesini, yönetmesini ve maliyetleri düşürmesini sağlayan güçlü bir teknolojidir. Bununla birlikte, genel bulut hizmeti sağlayıcılarının yerleşik ağ oluşturma kapasitesi, bazı kullanım durumları için yeterli olabilir, ancak daha büyük ve daha karmaşık kuruluşların ihtiyaçları için yetersiz olabilir. Böylece çoklu bulut internet yazılımı doğdu. Çoklu bulut yazılımı, farklı bulut hizmeti sağlayıcıları arasında ağ bağlantıları oluşturarak kaynakların daha verimli yönetilmesini sağlar. Bu yazılım, özellikle programlanabilirlik, entegrasyon ve esnek lisanslama alanlarında geleneksel sanal yönlendiricilerden ve sanal cihazlardan daha güçlüdür. Bu, hem genel hem de özel bulut ortamlarında ağ yönetiminde daha fazla esneklik ve kontrol sağlar. Çoklu bulut internet yazılımı, tüm bulut kaynaklarına tek bir kullanıcı arayüzünden erişim sağlayarak daha iyi bir kullanıcı deneyimi sunar. Ayrıca bu yazılımlar bulut kaynaklarının yönetimini kolaylaştırmakta ve operasyonel verimliliği artırmaktadır. Özellikle çoklu bulut yazılımı, farklı bulut hizmeti sağlayıcılarının kaynaklarını birleştirerek şirketlerin kaynak kullanımını optimize etmesine olanak tanır. Bu, maliyetleri azaltır ve aynı zamanda performansı artırır. Ancak, Multicloud web yazılımını yüklemek ve yönetmek biraz daha karmaşık olabilir. Şirketlerin yazılım ihtiyaçlarını karşılayan altyapıyı ve çalışanların yazılımı etkin bir şekilde kullanma becerilerini sağlamaları önemlidir.

5.1 Öneriler

Bulut ve uç altyapısından sorumlu altyapı ve işletme yöneticileri şunları yapmalıdır: Genel bulut sağlayıcılarının yeteneklerinden yararlanarak başlasalar bile, geleneksel ağ stratejilerini genel buluta taşımamalılar. Birden çok genel bulut ortamı için gelişmiş ağ özellikleri veya birleşik bir ağ iş modeli gerektiğinde, MCNS ile genel bulutta dahili ağ performansını artırmalısınız. Sağlam, iyi belgelenmiş API'lerle gelen ve satın almadan önce test etmeyi sağlayan hafif, bulut tabanlı ürünleri seçerek MCNS yatırımınızı optimize edilmelidir [8].

5.2 Market Tanımı

MCNS, birden çok genel bulut ortamında ağ tasarımını, dağıtımını ve yönetimini kolaylaştıran bir yazılımdır. Kuruluşlar, MCNS'yi tek bir genel bulut ortamında veya birden çok genel bulut ortamında devreye alabilir ve yazılımı uç noktalar ve özel veri merkezleri gibi diğer ağ konumlarına genişletebilir. MCNS ürünleri, tek bir yönetim noktası aracılığıyla birden çok bulut ortamında birleşik ağ politikası, güvenlik, yönetim ve ağ görünürlüğü sağlayarak yönetimi basitleştirir. MCNS ürünleri, trafik yönlendirme, güvenli G/Ç ve genel bulut hizmetleriyle entegrasyon gibi çeşitli özellikler içerir. Yazılım olarak sağlanan MCNS ürünleri, API'ler ve kullanıcı arayüzleri aracılığıyla erişilen, kendi kendini yöneten bir hizmet olarak da kullanılabilir. Yer paylaşımları ve aracılar kullanılarak veya yerleşik bulut sağlayıcı işlevleri yönetilerek daha da özelleştirilebilirler. Bu, kurumların ağ yönetimi fonksiyonlarını daha etkin ve verimli bir şekilde gerçekleştirmelerini sağlar. [8].

5.3 Market Açıklaması

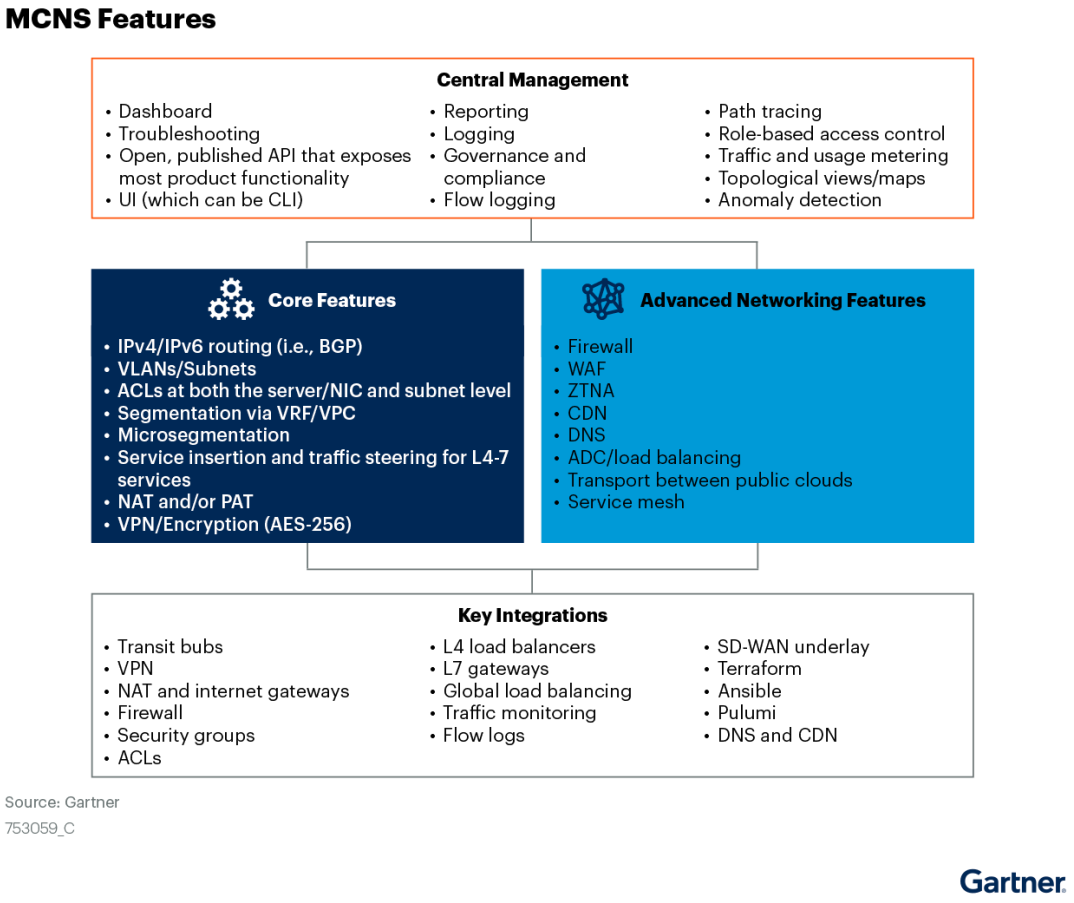
MCNS, genellikle genel bulut hizmeti sağlayıcılarının ağ işlevlerini genişleten veya değiştiren bir yazılımdır. MCNS, farklı bulut ortamlarında aynı ağ işlevlerini ve yönetimi sağlamak için tasarlanmıştır. Aksi takdirde bu bulut ortamları farklı özelliklere ve yönetim platformlarına sahip olabilir. MCNS, yönlendirme gibi temel ağ işlevlerinin yanı sıra CDN, ADC ve güvenlik duvarı gibi Katman 4-7 hizmetleri gibi gelişmiş işlevler sağlar. Ayrıca bulut ortamları ve otomasyon yazılımı gibi temel entegrasyonları da içerir. Bu nedenle, MCNS pazarı, esas olarak VPN bağlantıları için kullanılan "vRouters" içermeyen gelişmiş özelliklere ve entegrasyona sahiptir. MCNS, genel buluta doğrudan bağlantı veya İnternet üzerinden fiziksel trafiği içermez. Bu, bulut hizmeti sağlayıcısının sorumlu olduğu bir alandır. Birçok müstahkem ağa sahip olan 7. ve 4. seviye. 1. Kademe donanım satıcıları, ürünlerinin sanallaştırılmış sürümlerini sunarak, bunların şirket içi ve genel bulutlar dahil olmak üzere birden çok bulut ortamında devreye alınmasına olanak tanır. Dolayısıyla "Sadece vRouters veya vAppliances değil mi?" Soru, birkaç bulut ağ yazılımı hakkında sorulur. Cevap nüanslı. Müşteriler genellikle şirket

içinde bir genel bulut ortamına temel VPN bağlantıları kurmak için bu sanal yönlendiricileri kullanır. Ancak müşteriler bu vRouter'ları temel VPN kullanım durumlarının ötesine genişletmeye çalıştıklarında, nadiren ihtiyaçlarını karşıladıklarını söylüyorlar. Müşteriler, bu ürünlerin birkaç nedenden dolayı buğulanmadığını söylüyor:

Bulut farkındalığı/entegrasyon eksikliği – Ürünler, hizmetler, bölgeler veya kullanılabilirlik bölgeleri gibi bulut tabanlı özelliklerin farkında değilsiniz. Genel bir bulut ortamında bulunurlar, ancak çevredeki hizmetlerle dinamik olarak etkileşime girmezler. Sınırlı Programlanabilirlik – Bir API ile bile kullanılabilirlik, destek, dokümantasyon veya işlevsellik, otomasyon/düzenleme açısından bulut ekiplerinin ihtiyaç duyduğu şeylerin yakınından bile geçmez. Lisanslama - Ürün maliyetleri, lisanslama modelleri ve/veya iş koşulları, bulut ekiplerinin sorunsuz erişim, değişken ve öngörülemeyen tüketim veya self servis isteklerini tatmin etmez. Sınırlı Deneyim – Satış ekibi, kanallar, teknik destek ekipleri ve/veya teknik belgeler, gerçek bir bulut ortamında referans müşteri ve/veya kullanıcı deneyiminden yoksundur. Bant genişliği veya veri aktarım hızı gibi performans sınırları [8].

5.4 MCNS Elementleri

Şekil 5.4.1, MCNS ürünlerinde bulunabilecek çeşitli unsurları göstermektedir [8].



Şekil 5.4.1 MCNS Özellikleri

Tablo 1: MCNS Hizmet Sağlayıcıları

Şirket	Cloud Networking Ürünü
Alkira	Cloud Networking
Arrcus	Arrcus Multi-Cloud Networking (MCN)
Arista Networks	Any Cloud Platform
Aviatrix	Aviatrix Cloud Network Platform
Cohesive Networks	VNS3
Cisco	Cisco Cloud Services Router 1000V (CSR1kv), Cisco Catalyst 8000V Edge Software, Cisco Cloud APIC
F5	F5 Distributed Cloud Platform
Prosimo	AXI Platform
VMware	NSX Cloud

5.5 Market için Öneriler

Public cloud'da veri merkezi ağ tasarımlarını ve satıcılarını forklift etmek, bütünleşme ve maliyet verimsizliğine yol açabileceğinden, I&O liderleri başlangıçta cloud sağlayıcıların kendi özelliklerini tercih etmelidir. İşletme için ağ özellikleri derinliği veya operasyonel ağ tutarlılığı çeşitli cloud'lar arasında önemli olduğunda, MCNS'ye yatırım yapılmalıdır. Tek bir yönetim platformu aracılığıyla, birden fazla sağlayıcıda (örneğin, yönlendirme, DNS, CDN, WAF, güvenlik duvarı ve izlenebilirlik gibi) geniş, "tam yığın" seviye 3 ila seviye 7 ağ ve ağ güvenliği yeteneklerinin tutarlı bir seti gerektiğinde, MCNS'ye yatırım yapılmalıdır. bulut ve kenar altyapısıyla ilgili olan I&O liderlerinin, stratejik bulut sağlayıcılarının yeni ağ özelliklerini düzenli olarak incelemelerinin ve bu özelliklerin açıklarını nasıl kapattığını gözlemlemelerinin önemlidir. API-öncelikli yaklaşımlar sunan ve "cloud fluent" (yani, bulunduğu ortamla dinamik olarak etkileşime geçen, cloud platform API'lerini kullanan) MCNS tekliflerini tüketim lisanslama yoluyla sunan MCNS tekliflerini tercih etmek gerekmektedir. Gereksinimler öngörülemeyen veya son derece dinamik olduğunda, tüketim temelli fiyatlandırma sunan MCNS satıcılarını seçmek önerilir. Piyasanın yeni katılımcıları ve yüksek bir değişim seviyesi ile dinamik olmasını beklediğimiz için, kısa vadeli bir planlama süreci kullanarak, bir ila üç yıllık sözleşmeler imzalayarak veya tüketim temelli seçenekleri kullanarak yaklaşmak uygun olacaktır. %90'dan fazla işlevselliği ortaya koyan, tamamen belgelenmiş, açık API'ler sunan ve ters uyumluluk geçmişine sahip olan MCNS satıcılarını seçmek önemlidir [8].

6. MULTİ-CLOUD NETWORKİNG SOFTWARE ARTI VE EKSİLERİ

Çoklu-bulut ağ yazılımları (MCNS) nın birçok yararı vardır. Örneğin, farklı ağ araçları ve yetenekleriyle uğraşma ihtiyacını ortadan kaldırarak, bulut dağıtımlarını hızlandırabilir. Ayrıca, MCNS çözümleri, ayrı bulut ortamlarında ağ performansını optimize etmeye yardımcı olabilir ve ağlamayı basitleştiren soyutlamalar ve düşük kodlu iyileştirmeler sağlayarak, karmaşıklığı ve ilişkili maliyetleri azaltır. MCNS benimsemek, tüm çoklu-bulut ortamını kapsayan tutarlı bir ağ ve güvenlik altyapısına sahip olma imkanı sunarak insan kaynakları maliyetlerini azaltabilir. Ayrıca, NetOps, DevOps ve SecOps takımları arasındaki boşluğu kapatır ve daha hızlı uygulama dağıtımı sağlar. Ancak, MCNS benimsemenin bazı zorlukları da vardır. Örneğin, maliyetli olabilir ve kuruluşların değerlendirme sürecini tamamlamak için bir mühendis ekibine yatırım yapması gerekebilir. MCNS çözümlerinin karmaşıklığı, organizasyonların ekibini etkili bir şekilde desteklemek için yeniden eğitmesi gerektirir. Çoklu-bulut mimarileri, yeterli uçtan uca performans ve güvenlik sağlamak için ağ dahil tüm BT altyapısının geniş çaplı

modernizasyonunu gerektirir. Ayrıca, çoklu-bulut ağları, bulutlarda aralıklı veya kısmi görünürlük dahil olmak üzere görünürlük zorluklarına neden olabilir [9].

7. MULTİ-CLOUD NETWORKİNG SOFTWARE ÇÖZÜMLERİ

Bu platformlar, birden fazla bulut sağlayıcısına bağlanarak uygulama ve veri trafiğini yönetmek için kullanılan multicloud yazılım çözümleridir.

7.1 VMware Nsx

VMware NSX, veri merkezinde ve bulutta uygulama güvenliği sağlamak için kullanılır ve birden fazla bulut sağlayıcısı arasında geçiş yapabilen bir multicloud platformu sunar [10].

7.2 Cisco ACI

Cisco ACI, ağ ve uygulama alanlarını bir araya getirerek, bulut ve veri merkezi ortamlarında çalışan uygulamaları güvenli ve basit bir şekilde yönetmek için kullanılır [11].

7.3 Google Multicloud

Google Multicloud, birden fazla bulut sağlayıcısına bağlanarak kaynakları optimize etmek ve bulut maliyetlerini azaltmak için kullanılır [12].

7.4 Microsoft Azure Virtual WAN

Microsoft Azure Virtual WAN, bulut altyapılarını bağlayarak, veri merkezlerini ve şube ofislerini bağlayarak uygulama performansını artırır [13].

7.5 F5 Cloud Services Platform

F5 Cloud Services Platform, birden fazla bulut ortamında uygulama yönetimini ve güvenliğini sağlar [14].

7.6 Aviatrix

Aviatrix, birden fazla bulut ortamında ağ yönetimini ve güvenliğini sağlayarak, multicloud ortamlarındaki uygulamaların hızlı bir şekilde yönetilmesine olanak tanır [15].

7.7 Citrix SD-WAN

Citrix SD-WAN, birden fazla bulut sağlayıcısı arasında veri trafiğini yönetmek için kullanılır ve uygulamaların bulutta hızlı ve güvenli bir şekilde dağıtılmasını sağlar [16].

8. MULTİ-CLOUD NETWORKİNG SOFTWARE İÇİN USE CASES

Tablo 2: MCNS için En Önemli Kullanım Senaryoları

Kullanım Senaryosu	Açıklama	Büyüme Oranı
Tekil Halka Açık Bulut	Tek bir halka açık bulut sağlayıcısı içinde ağ özelliklerini geliştirmek veya işlemleri iyileştirmek.	Artıyor
Uygulama Odaklı	Belirli bir uygulama veya uygulama kümesi için geniş bir ağ ve güvenlik özellikleri seti sağlamak (dahilînde seviye 3'ten seviye 7'ye kadar).	Artıyor
Çoklu Bulut	Birden fazla halka açık bulut sağlayıcısı arasında tutarlı yönetim ve işlemler.	Hızla artıyor
Genişletilmiş Halka Açık Bulut	Halka açık bulut ortamlarında kullanılan MCNS ağ özelliklerinin ve işletimsel yönetim modelinin bulut dışı yerlere genişletilmesi. Bu yerler, kenar ağları (kenar hesaplama ve ağ geçidi yerleri desteği), veri merkezi ağları ve kiralık tesislerdir.	Hızla artıyor

Table 10. *Overview of research trends identified.*

Research topic	Research trends and opportunities
Multi-cloud concept	• Cloud continuum characterization and understanding • Incorporation of new paradigms to the multi-cloud concept: Fog Computing, Osmotic Computing
Multi-cloud by design [RQ3]	• Architectural patterns for multi-cloud native applications • Means and methods to model at high level of abstractions (platform/technology independent) heterogeneous infrastructural elements and application components. • Linking the applications models to the infrastructural models through NFRs characterization especially network, communications, security (i.e., especially data sharing) or even legal
DevOps for multi-cloud	• Lightweight benchmarking and multi-objective optimization for the selection of the best combination of infrastructural elements. • Federation models for the Cloud Continuum, including IoT and networks elements to the traditional Cloud Services. • Application self-healing and migration at runtime, with special focus on data portability and stateful components
Multi-cloud security	• Standard security models or SLA to evaluate security • Conflicting security policies • Frameworks to provide, assess and monitor security with a quantitative approach • Trustable Cloud Services
Multi-cloud certification	• Compositional cloud certification and combination with IoT and 5G certification

Şekil 8.1 Trend Araştırmaları

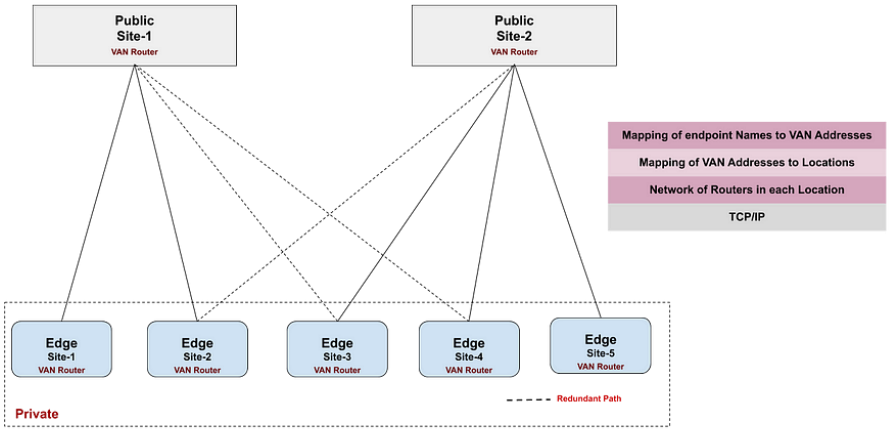
Çok sayıda bulut hizmetinin heterojenliğinden kaynaklanan birçok yön, özellikle Cloud Standartlarının uygulanmasıyla geliştirilebilir veya hatta çözülebilir. Ancak, bulut

standartlaştırma çabaları henüz ilk aşamalarındadır ve yakın zamanda olgun bir çözüm beklenmiyor. Mevcut uygunluk şemaları alanında büyük bir parçalanma var, sadece kontrollerin kapsadığı alanlarda değil, aynı zamanda uygunluk değerlendirme yöntemlerinde de. Dahası, bulut sağlayıcıları kendilerini rekabet avantajlarını ve çeşitliliği korumaya yönelik birleşik yaklaşımlara karşı çıkıyorlar ve müşteri çekmek için farklılaşmayı tercih ediyorlar. Bu sorunu ele almak için, Avrupa Komisyonu, Avrupa Birliği Siber Güvenlik Ajansı ENISA aracılığıyla Avrupa Bulut Hizmetleri Şeması (EUCS) adlı Avrupa bulut sertifikasyon çerçevesini oluşturmuştur. Bu çerçeveden kaynaklanan önlemlerin ve gereksinimlerin uygulanması, özellikle aşağıdaki konular açısından araştırma zorlukları yaratacaktır: Bileşimsel bulut sertifikasyonu ve IoT ve 5G sertifikasyonu ile birleştirme [17].

9.VİRTUAL APPLİCATİON NETWORKS (VAN) FOR MULTİ-CLOUD, MULTİ-CLUSTER AND CLOUD-EDGE INTERCONNECT

Virtual Application Network (VAN), bulut tabanlı uygulama ortamlarında dağıtılmış yazılım bileşenleri arasında gelişmiş iletişim sağlayarak VPN'ler, güvenlik duvarları ve erişim politikaları gibi karmaşık layer 3 ağ kontrolleriyle uğraşmayı gerektirmez. TCP/IP tabanlı internet üzerinde bindirilmiş bir uygulama katmanı ağı olan VAN, tek bir dizüstü bilgisayar kadar küçük veya kıtaları kapsayan küresel bir ağ kadar büyük olabilir. VAN'ın kurulumu, yetkisiz bir geliştirici tarafından hızlı bir şekilde yapılabildiği gibi topolojisi de kolayca değiştirilebilir. Mevcut protokoller arasında HTTP, gRPC, AMQP, TCP veya UDP gibi herhangi bir şeyi kullanabilen uygulamalar, değişiklik yapmadan bir VAN üzerinde çalıştırılabilir. VAN adreslemesi, altta yatan ana bilgisayar ve bağlantı noktası bilgilerine bağlı kalmadan uç noktalara doğrudan atıfta bulunmak için belirli dizeler kullanır. IP adresleme genellikle tek noktaya yayın (unicast) kullanır ve her adres bir ana bilgisayarı temsil eder. IPV4 ve IPV6, çok noktaya yayın (multicast) desteği sağlar, ancak IPV6 ayrıca herhangi bir noktaya yayın (anycast) desteği sağlar. Bununla birlikte, yerel ağ kapsamını aşan uygulamalar için kullanılmaz. VAN adreslemesi, çok noktaya yayın veya herhangi bir noktaya yayın olarak kullanılabilir. Aynı adresle ağa birden çok yazılım bileşeni eklemeyi mümkün kılarak çok noktaya yayın teslimatı veya yük dengelemesi yapılabilir. VAN çok noktaya yayın ve herhangi bir noktaya yayın, bileşen konumundan bağımsızdır ve bu nedenle ağ genelinde çok noktaya yayın teslimatı ve herhangi bir noktaya yayın yük dengelemesi sağlar.

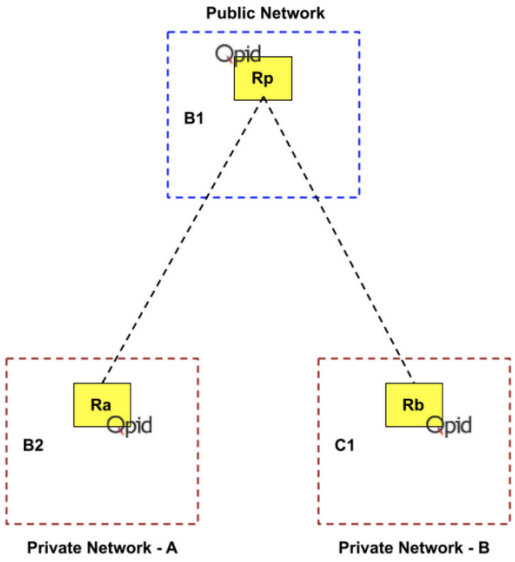
Her bir konumda bir VAN yönlendiricisi (dağıtım yönlendiricisi) kurularak ve güvenli bağlantılar kurularak dağıtılmış bir uygulama alan adına ait bir VAN oluşturulur. Bir konum, bir LAN'daki bir veri merkezi, tek bir ana bilgisayar veya bir ad alanındaki bir Kubernetes kümesi olabilir. Skupper, VAN yönlendiricisi olarak hafif ve durumsuz olan Apache Qpid Dispatch Router'ı kullanır ve AMQP protokolüne dayanır. Skupper ayrıca, ağ kurulumunu kolaylaştırmak ve HTTP, gRPC ve TCP gibi yaygın olarak kullanılan protokollerden VAN ağına eşlemeler sağlamak için araçlar sunar. Dispatch Router, hafif bir AMQP mesaj yönlendiricisi olarak ölçeklenebilir, kullanılabilir ve performanslı mesajlaşma ağları oluşturmak için kullanılır. Dispatch Router, müşteriler, sunucular ve mesaj aracıları dahil olmak üzere herhangi bir AMQP etkin uç nokta arasında mesajları esnek bir şekilde yönlendirir. AMQP, açık bir standart protokol olup, sistemler arasında mesajlaşma uyumluluğuna izin verir ve HTTP'ye göre hizmet ve API teslimi için gerçek avantajlar sağlar. Yönlendiricilerin ağı, topolojiyi algılamak ve her çift konum arasındaki en az maliyetli yolun hesaplanmasını sağlamak için OSPF veya IS-IS gibi Link-State yönlendirme protokolünü kullanır. Yönlendirme protokolü, topolojideki değişikliklere hızlı ve otomatik olarak yanıt vererek başarısızlığa karşı dayanıklılık sağlar ve ayrıca ağa konum ekleme veya çıkarma işlemlerini genişleme veya değişiklikler gerektiğinde kolaylaştırır.



Şekil 9.1 VAN Router

Aşağıdaki örnek yapıda, Private Network-A ve Private Network-B iki farklı özel ağdır. Müşteri C1, Private Network-B'de bulunurken arka uç B2, Private Network-A'dadır. Dispatch yönlendirme kullanarak müşteri C1, Private Network-A'da bulunan kuyruk, konu ve diğer AMQP hizmetlerine yönlendiriciler arasındaki bağlantılar kullanılarak Public Network üzerinden erişebilir. Örneğin, Ra ve Rp yönlendiricileri B2 brokerında ve B1 brokerında bulunan kuyrukları ağda görünür hale getirmek için yapılandırılabilir. Müşteri C1 daha sonra

yerel yönlendirici Rb'ye bağlanabilir, "b1.event-queue" ve "b2.event-queue" abonelik bağlantılarını açabilir ve B1 ve B2 brokerlarında depolanan kuyruklarda bulunan mesajları alabilir. Bu senaryoda, B1, B2 veya C1 hiçbir şekilde değiştirilmemiş ve birbirlerinin arasında bir mesaj yönlendirici ağı olduğu gerçeğinden haberdar olmalarına gerek yoktur [18].



Şekil 9.2 Public- Private Network Şeması

10. AGİLE RİSK YÖNETİMİ FOR MULTİ-CLOUD SOFTWARE DEVELOPMENT

Tüm sektörlerdeki endüstriler, işletmelerinin merkezine yazılımı yerleştiren köklü bir dijital dönüşüm yaşamaktadır. Sürekli değişen kullanıcı gereksinimlerine ve dinamik piyasalara yanıt vermek için şirketler, rekabetçi olabilmek için esnekliklerini artıracak sağlam iş akışları oluşturmak zorundadır. Bu hızlı dönüşüm, özellikle Nesnelerin İnterneti veya bulut bilişim gibi alanlarda, dinamizm ve çevik kısa vadeli planlama, riskleri tespit etme ve yönetme yeteneğini azalttığı için yüksek kaliteli yazılım garantilemek için önemli zorluklar ortaya çıkarmaktadır. Bu çalışmada, yazarlar, tüm sektörlerde faaliyet gösteren 20'den fazla çevik koçun 15 yıldır sürekli çalıştığı yüzlerce takım deneyimine dayanarak, çevik yazılım geliştirmede risk yönetimi ile ilgili ana zorlukları tanımlamaktadır. Ayrıca, bu zorlukları dikkate alan ve işbirliği, çeviklik ve sürekli gelişimi destekleyen bir risk yönetimi çerçevesi önermektedirler. Bu çerçevenin bir uygulaması, çoklu bulut uygulamalarının geliştirilmesiyle ilgili riskleri ve önleme eylemlerini ele alan bir araçta açıklanmaktadır. Yöntem ve araç, bir ekip tarafından değerlendirilmiş ve kentsel akıllı mobilite hizmeti ve havayolu uçuş planlama sistemi geliştirmede kullanımını değerlendirmeleri istenmiştir.

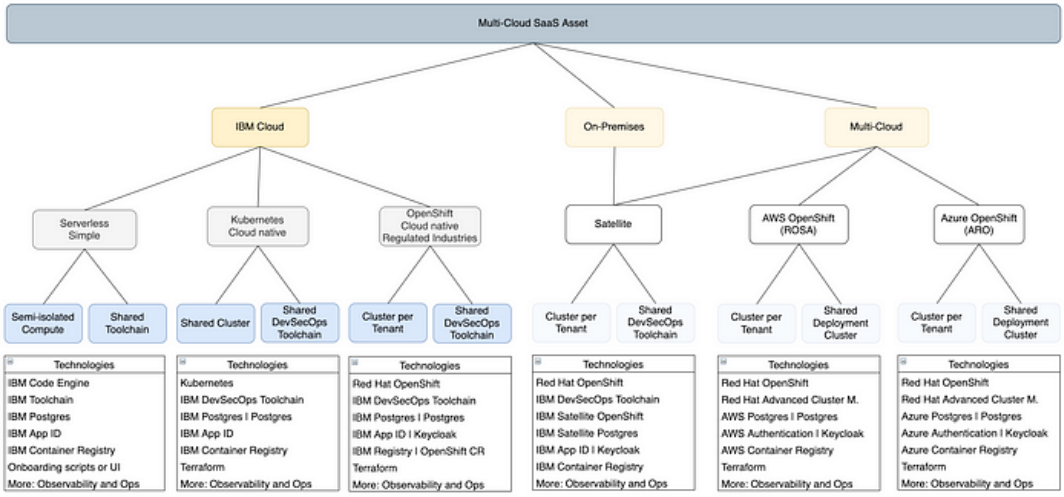
Bu makale, bir bulut bilgi işlem ortamında yazılım geliştirme için önerilen bir yaklaşımı özetlemektedir. Bu yaklaşım, yazılımın yaşam döngüsü boyunca bulut bilişim kaynaklarının kullanımını optimize etmeyi amaçlar. Yaklaşım beş ana bölümden oluşmaktadır:

" Elastic Requirements": Esnek Talepler, bulut bilgi işlem kaynaklarının dinamik kullanımına olanak sağlayan ve talep üzerine ölçeklenebilir olan talepler anlamına gelir. " Cloud-based Development Environment": Bulut tabanlı bir geliştirme ortamı, yazılım geliştirmenin bir bulut bilgi işlem ortamında yürütülmesini sağlar. "Cloud Runtime Environment": Cloud Runtime, Yazılımın çalıştırıldığı ortamı ifade eder. Bu ortam, mümkün olduğu kadar çok bulut bilgi işlem kaynağı kullanarak yüksek performans ve ölçeklenebilirlik sağlar. " Cloud-aware Software Architecture": Bulut bilgi işlem ortamıyla uyumlu yazılım mimarisi, yazılımın bulut bilgi işlem kaynaklarını verimli bir şekilde kullanmasını sağlar. " Cloud Deployment and Management": Bulut dağıtımı ve yönetimi, yazılımın bir bulut bilgi işlem ortamında başarılı bir şekilde dağıtılmasını ve yönetilmesini sağlar. Bu beş bileşen, yazılım geliştirme sürecinin farklı aşamalarını kapsar ve bulut bilişim ortamının sunduğu avantajlardan yararlanmak için tasarlanmıştır. Bu yaklaşım, geliştiricilere daha hızlı, daha esnek ve daha ölçeklenebilir yazılım geliştirme için bir çerçeve sağlar [19].

11. SAAS YAPISI KURMAK İÇİN YENİ OPEN-SOURCE MULTİ-CLOUD ASSET

Hizmet olarak yazılım (SaaS), çok kiracılı bir yaklaşımla sunulduğunda, her bir kiracının dağıtım ve bakım maliyetlerini en aza indirmeye yardımcı olur. Bu avantajlardan yararlanmak için uygulamaların güvenlik yalıtımını korurken birden çok kiracıyı destekleyecek şekilde tasarlanması gerekir. Aynı zamanda, yeni SaaS sürümlerinin mevcut kiracılara dağıtılabileceği veya bu modele güvenilir ve verimli bir şekilde entegre edilebileceği tek tip dağıtım ve işletim modellerine ihtiyaç vardır. Aşağıdaki diyagram, gri ve mavi kutularda gösterilen bazı seçenekler dahil olmak üzere çeşitli IBM Cloud devreye alma platformlarına yönelik seçenekleri göstermektedir. Beyaz ve açık gri kutular, IBM Cloud tarafından yönetilen bir OpenShift kümesinden yararlanan müşteri veri merkezlerinde şirket içi devreye alma için IBM Cloud Satellite'ın eklenmesi de dahil olmak üzere planlanan gelecekteki gelişmeleri temsil eder. Ayrıca, aynı SaaS uygulaması, AWS ROSA ve Azure ARO gibi diğer yönetilen OpenShift hizmetlerine dağıtılabilir. Başlamanın en kolay yolu, uygulamanızı çalıştırmak için tam olarak yönetilen IBM Code Engine platformunu kullanarak sunucusuz kullanmaktır. Gelişmiş bulut tabanlı uygulamalar için özel bir Kubernetes veya OpenShift kümesi kullanılabilir. Bilgi işlem

yalıtımı, Kubernetes ad alanları / OpenShift projeleri kullanılarak paylaşılan bir kümeyle sağlanabilir veya her SaaS kiracısı için ayrı kümeler oluşturulabilir.



Şekil 11.1 Saas Assets

Kullanılan temel teknolojiler:

- Kubernetes using either IBM Kubernetes Service or OpenShift on IBM Cloud
- IBM Code Engine (serverless)
- IBM Continuous Delivery CI/CD
- IBM Cloud Databases
- IBM App ID
- IBM Container Registry
- Terraform [20]

12. SONUÇ

Çoklu bulut, günümüzde birçok şirket için popüler bir tercih haline geldi. Farklı bulut hizmeti sağlayıcılarının hizmetlerini birleştirmek, şirketlerin iş ihtiyaçları için en uygun ve uygun maliyetli çözümleri oluşturmasına yardımcı olabilir. Çoklu bulutun en büyük avantajlarından biri, tek bir hizmet sağlayıcıya bağımlı olmaktan kaçınmaktır. Farklı bulut sağlayıcılarının hizmetlerini kullanmak, işletmelerin hizmet kesintisi riskini veya tek bir sağlayıcının güvenlik açığına maruz kalma riskini en aza indirmesine yardımcı olur. Ancak, çoklu bulut kullanmanın da zorlukları vardır. Farklı bulut sağlayıcıları arasında uyum sağlama, veri yönetimini ve veri güvenliğini sürdürme ve ağ performansını optimize etme gibi zorluklar, çoklu bulut stratejisi uygulayan şirketler için yaygın zorluklardır. Çoklu bulut ağları, birden çok bulut sağlayıcısı arasında esnek veri ve uygulama hareketliliği sağlayabilir. Ancak bu, veri hareketliliğinin ve

farklı sağlayıcılar arasındaki uyumluluğun yönetilmesini de gerektirebilir. Çoklu bulut yazılımı ve MCNS (Çoklu Bulut Ağ Yazılımı) çözümleri, verilerin ve uygulamaların farklı bulut hizmeti sağlayıcıları arasındaki hareketini optimize etmek, ağ yönetimini basitleştirmek ve ağ performansını iyileştirmek için tasarlanmıştır. Ancak bu programların seçimi, uygulanması ve yönetimi de zorluklara ve maliyetlere neden olabilmektedir. Çoklu bulut, işletmeler için önemli bir trend olmaya devam ediyor. Şirketler, farklı bulut hizmeti sağlayıcıları arasında bulut hizmetlerini kullanırken uygun bir çoklu bulut stratejisi ve uygun çoklu bulut yazılımı seçerek esnekliği ve verimliliği artırabilir. Çoklu bulut yazılım çözümlerinde birçok büyük şirket var. Örnekler arasında VMware NSX, Cisco ACI, OpenStack Neutron, Microsoft Azure Virtual WAN, F5 Bulut Hizmetleri Platformu, Aviatrix ve Citrix SD-WAN yer alır. VMware NSX, hem bulut ortamlarında hem de geleneksel veri merkezlerinde çalışan bir çoklu bulut ağ sanallaştırma platformudur. Cisco ACI, bulut ve veri merkezi altyapılarını birbirine bağlarken OpenStack Neutron, bulut ortamlarında ağ operasyonlarını yönetmek için bir platform sağlar. Microsoft Azure Virtual WAN, şirketlerin farklı bulut hizmetleri arasında güvenli ve optimize edilmiş bir ağ oluşturmasını sağlayan bulut tabanlı WAN (Geniş Alan Ağı) hizmetleri sağlar. F5 Bulut Hizmetleri Platformu, bulut tabanlı uygulama hizmetlerinin performansını, güvenliğini ve yönetimini optimize etmek için tasarlanmıştır. Aviatrix, bulut ortamlarında ağ operasyonlarını yönetmek için gelişmiş bir pano sağlar. Citrix SD-WAN, bulut tabanlı uygulamaların performansını iyileştirmek için tasarlanmış bir platformdur. Bu tür büyük işletmeler için çoklu bulut yazılım çözümleri, hem tek bulut sağlayıcıları hem de birden çok bulut sağlayıcısı kullanarak bulut tabanlı iş yüklerini yöneten işletmelerin ihtiyaçlarını karşılamak üzere tasarlanmıştır. Bu çözümler, bulut ağlarını yönetmek için gereken güvenlik, performans, esneklik ve ölçeklenebilirliği sağlayarak bulut tabanlı iş yüklerinin başarıyla yönetilmesine yardımcı olur. Gelecekte çoklu bulut yazılım çözümlerinin daha da geliştirilmesi ve genişletilmesi bekleniyor. Bu çözümler, bulut kaynaklarının yönetimini ve kullanımını kolaylaştırmak ve otomatikleştirmek için daha da geliştirilmiştir. Bu, şirketlerin bulut kaynaklarını daha verimli kullanmalarına ve maliyetleri düşürmelerine yardımcı olur. Ayrıca, gelecekteki çoklu bulut yazılım çözümleri, farklı bulut hizmeti sağlayıcıları arasındaki veri aktarımını ve yönetimini daha da optimize ederek şirketlerin daha hızlı ve daha güvenli çalışmasına olanak tanıyacak. Bu çözümler aynı zamanda işletmelerin bulut kaynaklarına daha iyi erişime ve daha esnek operasyonlara sahip olmalarını sağlar. Ancak çoklu bulut yazılım çözümleri geliştikçe bu alanda güvenlik sorunları artabilir. Bu nedenle, geleceğin çoklu bulut yazılım çözümleri daha da güçlü ve kapsamlı güvenlik önlemleriyle donatılacaktır. Farklı bulut

çözümlerinin sorunsuz bir şekilde bağlanabilmesi için bulut hizmeti sağlayıcıları arasındaki entegrasyonların daha da geliştirilmesi ve standartlaştırılması da bekleniyor.

13.KAZANIMLAR

Bu araştırmamda multi-cloud networking ve multicloud networking software kavramlarını detaylıca ele aldık. İki kavramın tanım, performans, güvenlik, use caseleri gibi birçok anlamda araştırdık. Gelecek vaad eden bir teknoloji olduğu konusunda hemfikir olduk. Multicloud network faydalarını da detaylıca öğrendik. Tekrar kısaca anlattıklarımızı özetlemek gerekirse; Multi-cloud networking, bir organizasyonun birden fazla bulut platformunu kullanarak uygulamalarını barındırmasına olanak tanır. Bu, her bulut platformunda ayrı ağ yapılandırmaları ve güvenlik politikaları gerektirir. Multi-cloud networking, ağ yapılandırmasının merkezi bir yönetimini sağlayarak, birden fazla bulut platformunda uygulamaların etkili bir şekilde çalışmasına olanak tanır. Multi-cloud networking software'leri, multi-cloud networking için kullanılan yazılım araçlarıdır. Bu yazılımlar, birden fazla bulut platformunda uygulamaların ağ yapılandırmasının merkezi bir yerden yönetilmesine olanak tanır. Bu yazılımlar, aynı zamanda birden fazla bulut platformunda ağ güvenliği politikalarının tutarlı bir şekilde uygulanmasını sağlar. Multi-cloud networking software'leri, ağ yönetimini otomatikleştirir, operasyonel verimliliği arttırır ve ağ performansını optimize eder. İşletmeler, birden fazla hizmet sağlayıcıya veya cloud platformuna bağımlılıktan kurtulur ve daha fazla esneklik elde ederler. Bu sayede, işletmeler ölçeklenebilirliği daha iyi yönetebilir ve farklı iş gereksinimlerine uygun çözümler sağlayabilirler. Multicloud software'leri, farklı hizmet sağlayıcılardan veri depolama, yedekleme ve güvenlik gibi hizmetlerin kullanılmasını sağlayarak, işletmelerin maliyetlerini azaltmalarına yardımcı olur.

Ayrıca, multicloud software'leri, birden fazla cloud platformu arasında kaynakları yönetmek için tek bir arabirim sağlar. Bu, kaynakların kolayca yönetilmesini ve kullanılmasını sağlar. Multicloud software'leri, işletmelerin hizmetlerinin performansını artırmalarına yardımcı olur. İşletmeler, birden fazla cloud platformu arasında uygulamalarını dengeleyebilir, böylece performans ve kullanılabilirli sorunları en aza indirilir. Son olarak, multicloud software'leri, işletmelerin verilerinin güvenliğini artırır. Birden fazla cloud platformunda verilerin depolanması, yedeklenmesi ve korunması, işletmelere daha iyi bir güvenlik stratejisi sağlar.

14.KAYNAKÇA

1. "Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions" by Jeroen Mulder (ISBN: 978-1800569354)
2. M. Özkan, "Why and what is cloud computing?," Analytics Vidhya, 2021. [Çevrimiçi]. Available: https://medium.com/analytics-vidhya/why-and-what-is-cloud-computing-474e917ac040.
3. IBM. (n.d.). Multicloud. Retrieved April 19, 2023, from https://www.ibm.com/topics/multicloud
4. Arefin, A. S. M., Niamul Bari, M., & Granville, L. Z. (2017). Multicloud Resource Allocation: Cooperation, Optimization and Sharing. EPFL Technical Report No. 7483. Retrieved from https://infoscience.epfl.ch/record/229524.
5. "What is multicloud? | Google Cloud". [Online]. Available: https://cloud.google.com/learn/what-is-multicloud.
6. S. Achar and S. Balakrishna, "Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in Our Modern Threat Landscape," 2021 IEEE 11th International Conference on Cloud Computing, New York, NY, USA, 2021, pp. 169-176, doi: 10.1109/CLOUD52353.2021.00031.
7. Oracle. (2021, June 30). Top Reasons Why Multicloud Improves Performance. Oracle Cloud Infrastructure Blog. [Online]. Available: https://blogs.oracle.com/cloud-infrastructure/post/top-reasons-why-multicloud-improves-performance.
8. Gartner. (2021). [Title of reprint]. Reprint. [Online]. Available: [URL of reprint].
9. Mearian, L. (2021, November 17). Cisco embraces multi-cloud networking software. Network World. [Online]. Available: https://www.networkworld.com/article/3670109/cisco-embraces-multi-cloud-networking-software.html.
10. VMware NSX. [Online]. Available: https://www.vmware.com/products/nsx.html.
11. Cisco ACI. [Online]. Available: https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html.
12. Google Multicloud. [Online]. Available: https://cloud.google.com/multicloud.
13. Microsoft Azure Virtual WAN. [Online]. Available: https://azure.microsoft.com/en-us/services/virtual-wan/.
14. F5 Cloud Services Platform. [Online]. Available: https://www.f5.com/products/cloud-services-platform.
15. Aviatrix. [Online]. Available: https://aviatrix.com/.

16. Citrix SD-WAN. [Online]. Available: https://www.citrix.com/en-in/products/citrix-sd-wan/.

17. Alonso-Ibarra, J. (2020). Analysis of Cloud Computing Architecture for Big Data Processing. Doctoral dissertation, University of the Basque Country. https://addi.ehu.es/bitstream/handle/10810/58456/TESIS_ALONSO_IBARRA_JUNCAL.pdf?sequence=1&isAllowed=y

18. Jain, V. (2020). Virtual Application Networks (VAN) for Multi-Cloud, Multi-Cluster, and Cloud Edge Interconnect. ITNEXT. Retrieved from https://itnext.io/virtual-application-networks-van-for-multi-cloud-multi-cluster-and-cloud-edge-interconnect-1f63a8081f41

19. J. Yang, X. Liu, Y. Zhang, Y. Sun, "A Model-Driven Virtual Network Function Deployment Framework for Multi-Cloud Applications", IET Software, vol. 13, no. 3, pp. 172-181, 2019. [Online]. Available: https://doi.org/10.1049/iet-sen.2018.5295(or arXiv:2001.03356v1 [cs.SE] for this version)

20. N. Heidloff, "New Open Source Multi-Cloud Asset to Build SaaS," Medium, 26-Sep-2018. [Online]. Available: https://medium.com/@nheidloff/new-open-source-multi-cloud-asset-to-build-saas-dd8502788dc7.