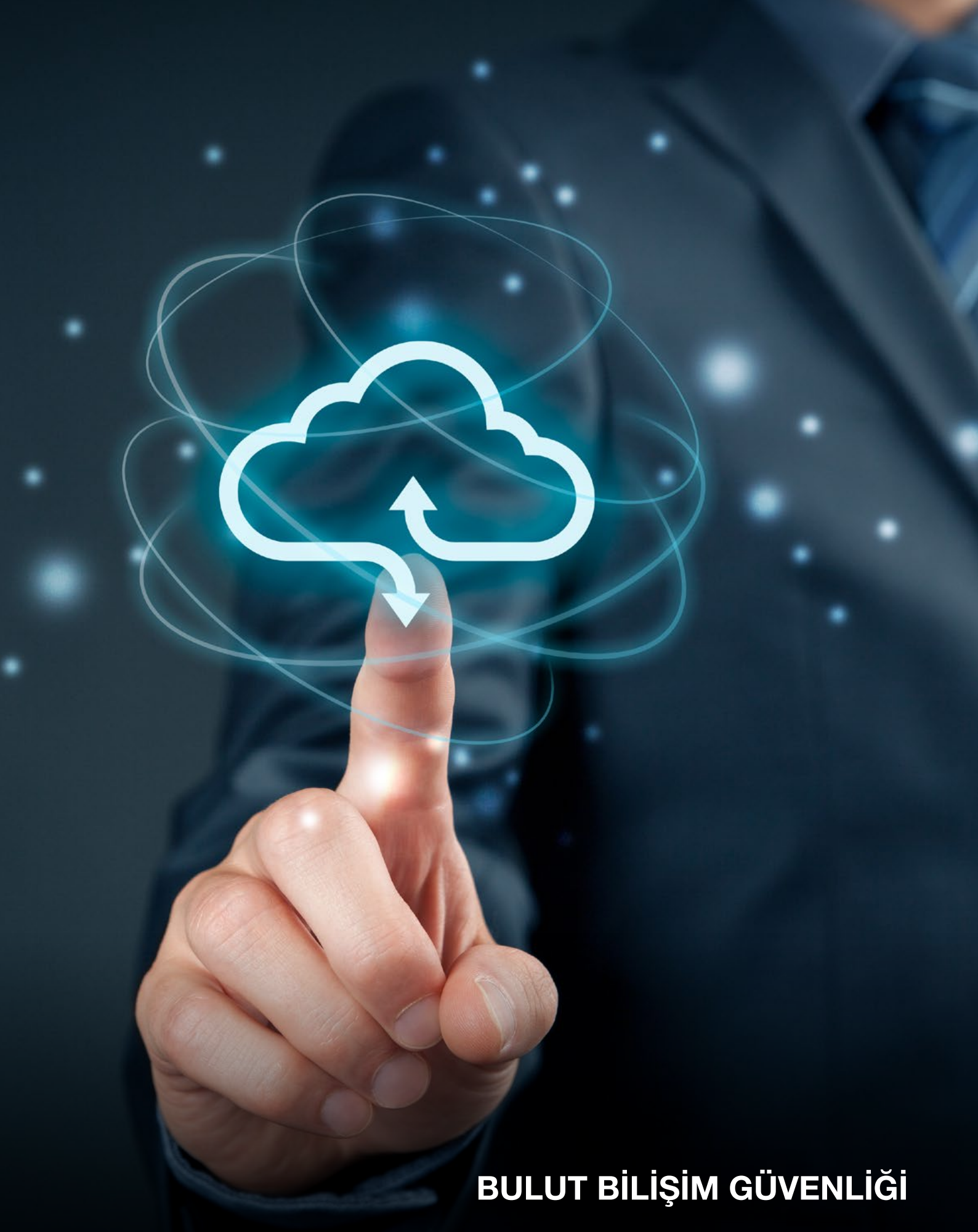
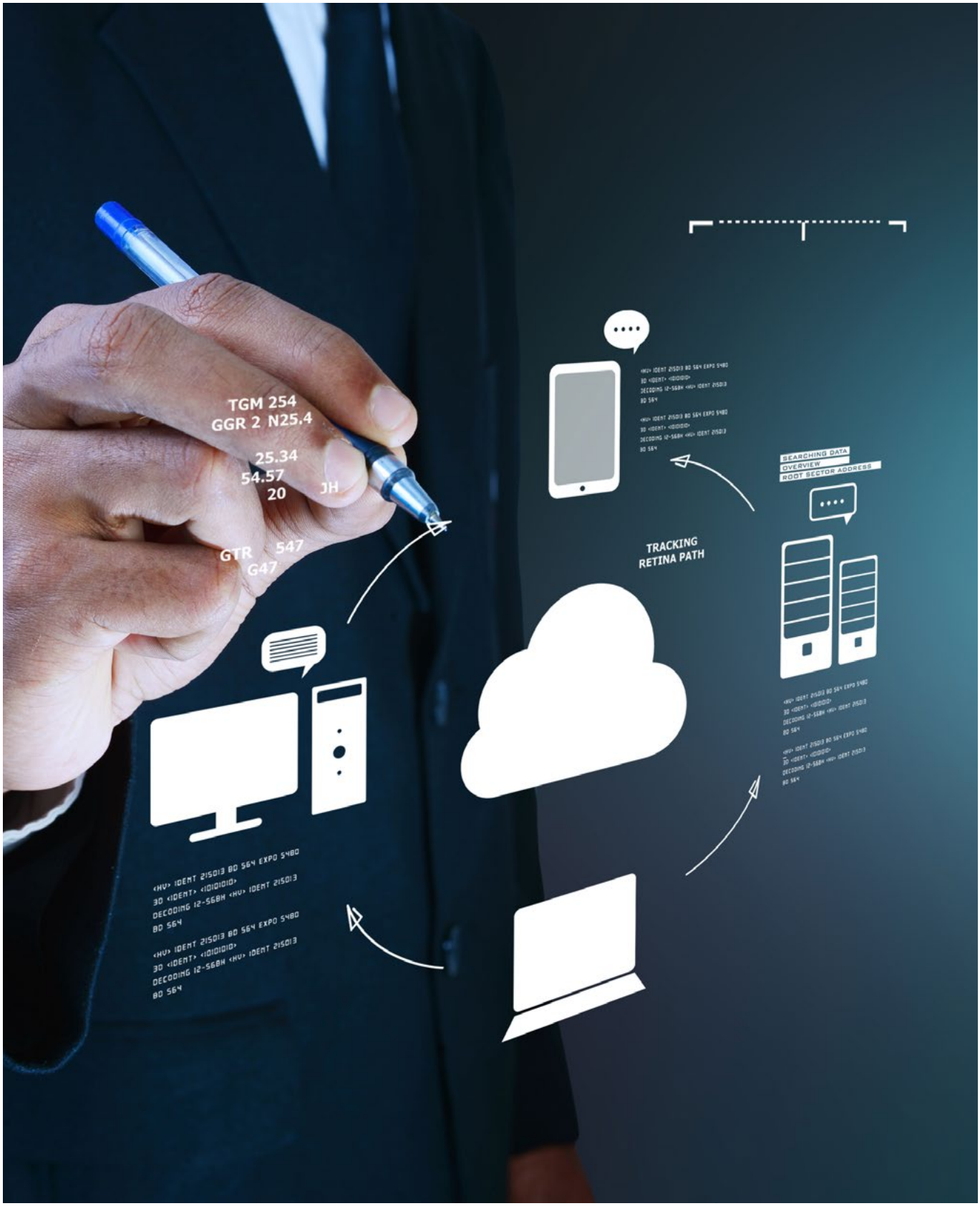


BULUT BİLİŞİM GÜVENLİĞİ

TREND ANALİZİ MART 2022

thinktech
STM Teknolojik Düşünce Merkezi



STM ThinkTech

1. GİRİŞ

Günümüz dünyasında teknolojinin dokunmadığı bir alan neredeyse bulunmamaktadır. Dijitalleşen dünyada şirketler hizmetlerini sanal ortamlara taşırken uzaktan yürütülebilen operasyonlar, ticari işlemler ve güvenlik operasyonları hızlı ve her yerden erişilebilen yeni hizmetlere ihtiyaç duymaktadır.

Kablosuz teknolojiler arttıkça gelişen sistemler daha hızlı iletişim teknolojilerinin ortaya çıkmasına olanak vermiştir. İletişim teknolojileri geliştikçe daha fazla alan yönetimi ve daha güçlü bilişim sistemlerini beraberinde getirmiştir. Günümüzde bilgisayar oyunlarında bile elinizdeki sistemin imkânı yetersiz olsa da hızlı bir internet bağlantısıyla bulut üzerinden en yüksek kapasitedeki oyunların oynanması mümkündür. Fotoğraflarınızı saklayabildiğiniz, ortak çalışmalar yapabildiğiniz ve işlerin uzaktan yönetilmesine imkân veren bulut sistemleri geleceğin teknolojilerinin önemli bir parçasıdır. Bulut bilişim, dijitalleşen dünyada kamudan özel sektöre her alanda dijital teknolojiler için yepyeni bir ufuk vadetmektedir.

Analizimizde; bulut bilişimin temel özellikleri kapsamında hem avantaj hem de dezavantaj olarak değerlendirilebilecek güvenlik özellikleri detaylıca incelenecektir. Bulut bilişim güvenliğinde son yıllarda ortaya çıkan dönüşüm dikkat çekmektedir. Güvenlik özelinde ortaya çıkan zorluk ve tehditlerin ortadan kaldırılması sayesinde, bu alanda yaşanan son gelişmeler bulut bilişimi farklı bir noktaya taşırken, analizimizde bulut bilişim güvenliğinin geleceğine yönelik geniş bir bakış açısı sunulması hedeflenmektedir.

2. BULUT BİLİŞİM NEDİR?

Bulut bilişim, farklı hizmetlerin internet üzerinden sunulmasına verilen isimdir. Bulut bilişim genel olarak kaynaklar, veri depolama, sunucular, veritabanları, ağ iletişimi ve yazılım gibi araçlar ile uygulamaları içermektedir.

Bulut bilişimde dosyalar özel bir sabit sürücüde veya yerel depolama aygıtında tutulmaktansa bulut tabanlı depolama ile uzak bir veritabanına kaydedilebilmektedir. Bu sayede herhangi bir elektronik cihazın internete erişimi olduğu sürece, verilere ve onu çalıştıracak yazılım programlarına erişimine imkân verilmektedir.

Bulut bilişim, ekonomik olması, üretkenliği artırması, hız ve verimlilik sağlaması, performans ve güvenlik katkıları gibi çeşitli nedenlerle bireysel kullanıcılar ve işletmeler için günümüzde popüler bir seçenek hâline gelmiştir[1].

Bulut bilişim, Bilgi Teknolojileri (BT) altyapısını bir yardımcı programa dönüştürmektedir. İnternet aracılığıyla altyapıya bağlanmanıza, ayrıca bilgi işlem kaynaklarını tesis içinde kurmadan ve bakımını yapmadan kullanmanıza olanak tanımaktadır.

Bulut bilişim terimi aslında bulutun çalışmasını sağlayan teknolojiyi ifade etmektedir. Bu durum bir tür sanallaştırılmış BT altyapısını içermektedir. Böylece veriler ve işlemler fiziksel donanım sınırlarına bakılmaksızın bir havuzda toplanabilmekte ve bölünebilmektedir[2].

Bulut bilişim, istemci cihazların uzak sunuculardan, veritabanlarından ve bilgisayarlardan internet üzerindeki verilere erişmesine izin vererek çalışmaktadır.

Bir internet ağ bağlantısı, ön ucu (bağlantı kuran kullanıcı, sunucu veya web hizmeti), veritabanları, sunucular ve bilgisayarlardan oluşan arka uç (veritabanları, sunucular ve bilgisayarlar) ile bağlar. Arka uç, ön uç tarafından erişilen verileri depolayan bir havuz işlevi görür.

Ön ve arka uçlar arasındaki iletişim, merkezi bir sunucu tarafından yönetilir. Merkezi sunucu, veri alışverişini kolaylaştırmak için protokollere güvenmektedir. Merkezi sunucu, farklı istemci cihazları ve bulut sunucuları arasındaki bağlantıyı yönetmek için hem yazılımı hem de ara yazılımı kullanır. Tipik olarak, her bir bireysel uygulama için özel bir sunucu olmalıdır[3].

Bulut bilişimin temel özellikleri verilen hizmetin yapısını belirlemede kullanılabilmektedir.

3. BULUT BİLİŞİMİN TEMEL ÖZELLİKLERİ

Bulut bilişim, tek yöneticili, çok kullanıcılı uygulama bulutundan (Software as a Service -SaaS) çok yöneticili, genel amaçlı, isteğe bağlı bulutlara (Platform as a Service - PaaS) hatta kullanıcılara güvenli bir veri merkezi işlem gücü, veri depolama kapasitesi ve ağ oluşturmak için bilgi işlem kaynaklarına erişim sağlayan altyapı servisi (Infrastructure as a Service - IaaS) gibi çeşitli hizmetlere imkân vermektedir[4].

Son 15 yılda gelişen bulut bilişim teknolojisinin önemi, COVID-19 salgınıyla beraber daha fazla artmıştır. Salgın, milyonlarca ofis çalışanını bir gecede evden veya uzaktan çalışanlara dönüştürmekle kalmamış, aynı zamanda bilgi teknolojileri bölümlerinin çalışma şeklini de değiştirmiştir.

ABD Ticaret Bakanlığının bir kurumu olan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standarts and Technology -NIST) bulut bilişimi tanımlarken, “minimum yönetim çabası ve hizmet sağlayıcısı desteği ile yayınlanabilecek ortak havuzlara ve ayarlanabilir kaynaklara anında erişim sağlayan bir model” açıklamasını kullanmıştır. NIST tanımlamasına göre bulut bilişim; isteğe bağlı self-servis, geniş ağ erişimi, kaynak havuzu, hızlı esneklik ve ölçülen hizmet olmak üzere en az beş temel özelliği içermelidir[5].

3.1 İsteğe Bağlı Self Servis (On Demand Self Service)

İsteğe bağlı self servis, müşteriler, tüketiciler ve hizmet sağlayıcılar arasında insan teması olmadan, bulut bilişimi istedikleri gibi kullanmasına olanak tanımaktadır. Tüketiciler, isteğe bağlı self servis özelliklerini kullanarak, gerektiğinde çeşitli bulut kaynaklarını düzenleyerek çalıştıkları bu sistemde özgür bir şekilde hareket imkânı bulmaktadır. Self servis sistemi müşteriye karşı güvenli ve özenli olmanın yanı sıra, çeşitli bulut kaynaklarına erişmek ve hizmet tekliflerini etkin bir şekilde takip etmek için kullanıcı dostu olacak şekilde tasarlanmalıdır. İsteğe bağlı self servis bulut bilişimin en önemli faydası, hem tüketiciler hem de bulut hizmetleri sağlayıcıları için verimli bir çözüm sunmasıdır[6].

3.2 Genel Ağ Erişimi (Broad Network Access)

Genel ağ erişimi, tabletler, bilgisayarlar ve akıllı telefonlar gibi çok çeşitli cihazlardan erişilebilen özel bir bulut ağında kullanılan kaynakları ifade etmektedir. Bu kaynaklara ayrıca çevrimiçi erişim sunan çok çeşitli konumlardan erişilebilir bir sistem olan genel ağ erişimi, dünyanın neresinde olunursa olsun sistemin kullanımına izin vermektedir[7].

Bulut sağlayıcıları, müşterilerin bulut kaynaklarına ve verilere nasıl eriştiğini yansıtan gecikme, erişim süresi, veri işleme hızı gibi farklı ölçümleri izleyip genel ağ erişimini kaydeder. Kayıtlar ağdaki hizmet kalitesinin artırılmasıyla ilgilidir ve daha iyi hizmet vermek için özellikle önemlidir[5].

3.3 Çok Kiracılı Mimari ve Kaynak Havuzu (Multitenancy and Resource Pooling)

Bulut bilişimin farklı kiracılara hizmet vermesini sağlayan ve her birinin diğerinden izole edildiği bir yazılım programı özelliği taşıyan yapı, çok kiracılı bulut bilişim olarak adlandırılmaktadır. Bir bulut sağlayıcısı, sıklıkla sanallaştırma teknolojilerinin kullanımına dayanan çoklu kiralama modellerini kullanarak birden çok bulut hizmeti tüketicisine hizmet vermek için BT kaynaklarını bir havuzda toplayabilir. Çoklu kiralama teknolojisinin kullanılmasıyla BT kaynakları, bulut hizmeti tüketici taleplerine göre dinamik olarak atanabilir ve yeniden programlanabilir.

Kaynak havuzu oluşturma, bulut sağlayıcılarının birden çok bulut tüketicisine hizmet vermek için büyük ölçekli BT kaynaklarını bir araya getirmesine olanak tanımaktadır. Farklı fiziksel ve sanal BT kaynakları, bulut tüketici talebine göre dinamik olarak atanır ve yeniden programlanır. Bu sistem genellikle istatistiksel çoğullama yoluyla çalışmaktadır. Kaynak havuzu, yaygın olarak çok kiracılı teknolojilere destek amacıyla kullanılır ve çok kiracılı sistemin karakteristik özelliklerini taşır[8].

İyi bir bulut hizmeti için sağlayıcıların kaynak havuzu çok büyük olmalı ve birden çok müşteri gereksinimine hizmet edecek ve ölçek ekonomisi sağlayacak kadar esnek olmalıdır. Kaynak tahsisi kritik üretim uygulamalarının performanslarını etkilememelidir[5].

3.4 Hızlı Esneklik ve Ölçeklenebilirlik (Fast Flexibility And Scalability)

Bulut bilişimin ölçeklenebilirliği, müşteri taleplerindeki değişiklikleri karşılamak için BT kaynaklarını eklemek veya azaltmakla ilgilidir. Bir sistemin daha büyük veya daha küçük yükleri barındırma yeteneği olmalıdır. İşletmeler yukarı veya aşağı ölçeklenebilir özelliktedir. Dolayısıyla ölçek büyütme, donanımı daha güçlü hâle getirir.

Hızlı esneklik, bulut bilişim kaynaklarının fiili olarak artması veya azalması ile ilgilidir. Bu, kaynakları dinamik olarak yüklerle başa çıkmak için esnetebilme yeteneği olan bu özellik genellikle ölçülebilirlik ile bağlantılıdır. Bulut bilişimin yükü arttığında, sistem daha fazla kaynak ekleyerek ölçeklenir. Talep düştüğünde ise kaynaklar azaltılır veya kaldırılır.

Esneklik, ihtiyaç duyulmayan kaynaklar için ödeme yapmak istenmediğinde ve sadece gerektiğinde artan talebin karşılanması istendiğinde çok önemlidir[9].

Bulut esnekliğinin en yaygın kullanım örnekleri arasında e-ticaret ve perakende, SaaS, mobil, Dev Ops ve altyapı hizmetlerinde sürekli değişen taleplere sahip diğer ortamlar bulunur. Ölçeklendirme özelliği ise performansın istikrarlı olduğu, tahmin edilebilir bir iş yüküne sahip işletmeler için maliyet tasarrufu seçeneği sunabilir[5].

3.5 Ölçülen Hizmet (Measured Service)

Ölçülen hizmet, BT uzmanlarının bulut bilişim için kullandığı bir terimdir. Bu terim, bulut sağlayıcısının faturalandırma, kaynakların etkin kullanımı veya genel tahmine dayalı planlama dahil olmak üzere çeşitli nedenlerle hizmetlerin sağlanmasını ölçtüğü veya izlediği sistemin bir referansıdır[10].

Ölçme ve raporlama hizmetleri, bulutu kuruluşlar için en iyi seçenek yapan özelliklerden biridir. Hizmetlerin ölçülebilmesi hem sağlayıcının hem de müşterinin hangi hizmetlerin ne amaçla kullanıldığını izlemesini ve raporlamasını sağlar[5].

4. BULUT SİSTEMİ ÇEŞİTLERİ

Tüm bulut sistemleri aynı değildir. Tek bir bulut bilişim türü herkese uygun olmayabilir. İhtiyaçlarınız için doğru çözümü sunmaya yardımcı olmak için farklı model, tür ve hizmetlerde bulut bilişim sistemleri geliştirilmiştir. Bu sistemler genel bulut, özel bulut, hibrid bulut ve çoklu bulut olarak sınıflanmaktadır[11].

4.1 Genel Bulut

Genel bulut, isteğe bağlı oluşturulan bilgi işlem hizmetlerinin ve altyapısının üçüncü taraf bir servis sağlayıcı tarafından yönetildiği ve genel internet kullanan birden fazla kuruluşla paylaştığı bir BT modelidir. Genel bulut hizmeti sağlayıcıları, kullanıcılara IaaS, PaaS veya SaaS gibi bulut tabanlı hizmetleri aylık veya kullanım başına ücretlendirme karşılığında sunabilir. Genel bulut sistemi kullanıcıların bu hizmetleri kendi veri merkezlerine kurma ihtiyacını ortadan kaldırmaktadır. Ekonomik BT altyapısı tercih eden kurumsal işletmeler, fiziksel BT altyapılarını genişletmeden mevcut BT kaynaklarını isteğe bağlı olarak ölçeklendirmenin bir yolu olarak genel bulut sistemini tercih edebilmektedir[12].

4.2 Özel Bulut

Özel bulut, tek bir müşteriye ayrılmış bir bulut bilişim sistemidir. Bu sistem bulut bilişimin birçok avantajını şirket içi BT altyapısının güvenliği ve denetimiyle birleştirerek faaliyet gösterir. Birçok şirket, yasal uyumluluk gereksinimlerinin karşılanması için daha kolay bir yol olduğundan özel bulut sistemine yönelmektedir. Özel bulutu tercih eden bazı şirketler ise özellikle gizli belgeler, fikri mülkiyet, kişisel bilgiler (Personally Identifiable Information -PII), tıbbi kayıtlar, finansal veriler veya diğer hassas verilerle ilgili güvenlik uygulamaları daha sıkı olduğundan bu sistemi uygulamaktadır[13].

Özel bulut hizmetleri için iki farklı sistem uygulanabilmektedir. Bunlardan birincisi, bir şirketin bilgi işlem, ağ ve depolama gibi altyapı kaynaklarını hizmet olarak kullanmasına izin veren IaaS'dir. İkincisi ise bir şirketin basit bulut tabanlı uygulamalarından gelişmiş etkin kurumsal uygulamalarına kadar her şeyi sunmasını sağlayan PaaS'dır. Özel bulutlar, genel bulutla birleştirilerek hibrid buluta da dönüşebilmektedir[14].

4.3 Hibrid Bulut

Hibrid bulut, şirket içi altyapı, özel bulut hizmetleri ve genel buluttan oluşan karma bir bilgi işlem, depolama ve hizmetler ortamını tanımlamaktadır. Hibrid bulutun en önemli avatajı çevikliktir. Hızla uyum sağlama ve yön değiştirme ihtiyacı, dijital bir işletmenin temel ilkesidir. İşletmelerin rekabet avantajı için ihtiyaç duyduğu çevikliği elde etmesi için genel bulutları, özel bulutları ve şirket içi kaynakları birleştirmek bir avantaj yaratabilmektedir[15].

4.4 Çoklu Bulut

Çoklu bulut sistemi birden fazla bulut servis sağlayıcısından hizmet alınarak oluşturulan yapılanmaları temsil etmektedir. Bu sistemde kullanıcı aynı anda farklı sistemlerin birbiriyle iletişim hâlinde olduğu ortak bir sistem üzerinden erişimle işlemleri gerçekleştirebilir[9].

Kuruluşlar, bulut hizmeti sağlayıcılara bağlı kalmaktan kaçınmak, seçim yapılabilecek daha fazla hizmete sahip olmak ve daha fazla yeniliğe erişmek için çoklu bulutu tercih etmektedir. Ancak ne kadar çok farklı bulut hizmeti kullanılırsa bu ortamı yönetmek o kadar zor olabilir[16].

5. BULUT HİZMETLERİ NELERDİR?

Bulut bilişimin üç ana hizmet modeli bulunmaktadır. Bunlar, Hizmet Olarak Altyapı (IaaS), Hizmet Olarak Platform (PaaS) ve Hizmet Olarak Yazılım'dır (SaaS). Bu üç sistem ile depolama ve kaynak havuzu açısından bir işletmeye sunulabilecekler arasında açık farklar bulunmaktadır. Ancak bu sistemler aynı zamanda kapsamlı bir bulut bilişim modeli oluşturmak için birbirleriyle etkileşime girebilmektedir[17].

5.1 IaaS

Bu sistem, sanal sunucular, ağ, işletim sistemleri ve veri depolama sürücülerinin temel altyapısını sunduğu için bulut bilişimin en yaygın hizmet modelidir. IaaS, tamamen öde ve kullan modeli bir hizmettir. Genel, özel veya hibrid bulut için bir altyapı olarak tercih edilebilmektedir[18].

5.2 PaaS

Bulut bilişim sağlayıcılarının altyapı ve yazılım çerçevesini oluşturduğu yer PaaS'dır. Ancak bu sistemde işletmeler ayrıca kendi uygulamalarını geliştirebilir ve çalıştırabilirler. Web uygulamaları, PaaS aracılığıyla hızlı ve kolay bir şekilde oluşturulabilir ve hizmet, bunları destekleyecek

kadar esnek ve sağlam oluşturulabilir. PaaS çözümleri ölçeklenebilir ve birden fazla geliştiricinin tek bir proje üzerinde çalıştığı iş ortamları için idealdir.

5.3 SaaS

Bu bulut bilişim çözümü, abonelik veya kullanım başına ödeme modeli aracılığıyla ödeme yapan çeşitli işletmelere internet üzerinden yazılımın dağıtımını içermektedir. SaaS, merkezi bir konumdan yönetilir, böylece işletmelerin kendilerinin bakım konusunda endişelenmelerine gerek kalmaz ve kısa vadeli projeler için ideal bir platform oluşturulur[17].

Bulut hizmetleri, BT teknolojilerinde yarattıkları devrimle işletmelerin sanallaştırılmış BT altyapısı geliştirmesine ve bir kullanıcının işletim sisteminden bağımsız olarak bulut üzerinden yazılım kullanmasına olanak tanıyan IaaS, PaaS ve özellikle SaaS gibi hizmetleri ortaya çıkarmıştır. Microsoft Azure, Amazon Web Servisleri, Google Cloud, IBM Cloud, Oracle Cloud Altyapısı ve CloudLinux bilinen en yaygın bulut hizmet sağlayıcılardır[19].

6. BULUT BİLİŞİMİN AVANTAJLARI

Bulut bilişim, işletmeler ve son kullanıcılar için birçok avantaja sahiptir. Bulut bilişimin başlıca avantajları aşağıda belirtilmiştir.

6.1 Maliyet Tasarrufu

Kuruluşların ekipman satın almak ve bakımını yapmak için büyük miktarda para harcaması gerekmediğinden, bulut altyapısını kullanmak maliyetleri azaltabilmektedir. Ek olarak, şirketler, bulut sağlayıcılarının ekiplerinin uzmanlığına güvenebildikleri için bulut veri merkezi operasyonlarını yürütürken büyük BT ekiplerine ihtiyaç duymaz. Bulut bilişim, kesinti süresiyle ilgili maliyetleri de azaltmaktadır. Bulut bilişimde aksama süresi nadiren gerçekleştiğinden, şirketlerin arıza süresiyle ilgili olabilecek sorunları çözmek için zaman ve para harcaması gerekmemektedir.

6.2 Mobilite

Bilgileri bulutta depolamak, kullanıcıların herhangi bir cihazla herhangi bir yerden, yalnızca bir internet bağlantısıyla bu bilgilere erişebileceği anlamına gelmektedir. Bu durum, kullanıcıların, verilerine erişmek için USB sürücüleri, harici bir sabit sürücü veya birden fazla CD taşıması gerekmediği anlamına gelmektedir. Kullanıcılar, akıllı telefonlar ve diğer mobil cihazlar aracılığıyla kurumsal verilere erişebilir, bu da uzaktaki çalışanların iş arkadaşları ve müşterilerle güncel kalmasını sağlamaktadır.

6.3 Olağanüstü Durum Kurtarma

Tüm kuruluşlar veri kaybı konusunda endişelenir. Verileri bulutta depolamak, kullanıcıların verilerine her zaman erişebilmelerini garanti etmektedir. Bulut tabanlı hizmetlerle kuruluşlar, doğal afetler veya elektrik kesintileri gibi acil durumlarda bile verilerini hızla kurtarma kapasitesindedir[3].

6.4 Güvenilirlik

Bulut bilişim sistemlerinde veriler, bulut sağlayıcının ağındaki birden fazla yedek siteden kullanılabildiğinden veri yedekleme ve iş sürekliliği çok daha kolaylaşmaktadır.

6.5 Güvenlik

Pek çok bulut sağlayıcısı, genel olarak güvenlik durumunu güçlendiren, verileri, uygulamaları ve altyapıları olası tehditlerden korumaya yardımcı olan geniş bir politika, teknoloji ve kontrol seti sunmaktadır.

6.6 Performans

En büyük bulut bilişim sistemleri, düzenli olarak yeni nesil hızlı ve verimli bilgi işlem donanımı ile güncellenen dünya çapındaki güvenli veri merkezleri ağları ile faaliyet göstermektedir. Bu durum, uygulamalar için daha az ağ gecikmesi ve daha büyük ölçekli ekonomik çözümler de dahil olmak üzere tek bir kurumsal veri merkezi üzerinde çeşitli avantajlar sunmaktadır.

6.7 Hız

Bulut bilişim hizmetlerinin çoğu, self servis ve isteğe bağlı olarak sağlanmaktadır. Bu nedenle, çok büyük bilgi işlem kaynaklarına erişim yalnızca birkaç tıklamayla dakikalar içinde sağlanabilmektedir. Bu durum işletmelere oldukça fazla esneklik sağlar ve kapasite planlaması üzerindeki baskıyı azaltır[20].

7. BULUT BİLİŞİMİN DEZAVANTAJLARI

Bulut bilişim sistemlerinin avantajları olduğu kadar dezavantajları da olabilmektedir. Bu sistemlerin en büyük dezavantajı güvenlik açıklarından ortaya çıkmaktadır.

7.1 Güvenlik

Güvenlik konusu bulut bilişim için avantaj oluşturduğu kadar ortaya çıkardığı dezavantajlarla da ele alınması gereken bir alandır. Kuruluşlar bulut sistemine güvenirken veri ihlalleri, uygulama programlama arayüzlerinin (Application Programming Interface -API) hack'lenmesi, güvenliği ihlal edilmiş kimlik bilgileri ve kimlik doğrulama sorunları gibi risklerle karşı karşıya kalmaktadır. Ayrıca, bulut sağlayıcısıyla paylaşılan hassas bilgilerin nasıl ve nerede işlendiğine ilişkin şeffaflık eksikliği de önemli bir tartışma konusudur.

7.2 Hizmet Sağlayıcı Değişimi

Bulut hizmetinin sağlandığı kuruluşun değiştirilmesi gibi durumlarda geçiş süreçleri sıkıntılı olabilmektedir. Özellikle özel bulut uygulamalarında sistemin sıfırdan kurulmasına kadar giden sorunlar ortaya çıkmaktadır. Veritabanı uyuşmazlıkları, çalışanların yeniden eğitimi gibi konuların da eklenmesiyle bulut sisteminin değiştirilmesi oldukça zorlaşmaktadır[3].

8. BULUT BİLİŞİMDE GÜVENLİK

Bulut bilişim güvenliği bulut tabanlı sistem, veri ve altyapıları korumak için bir arada çalışan bir dizi politika, kontrol, prosedür ve teknolojiden oluşmaktadır. Bulut güvenlik önlemleri, verileri korumak, yasalara uyumu desteklemek ve müşterilerin gizliliğini korumanın yanı sıra, bireysel kullanıcı ve cihazlar için kimlik doğrulama kurallarını belirlemek için yapılandırılmıştır. Bulut güvenliği, erişim için kimlik doğrulamaktan veri trafiğini filtrelemeye kadar işletmelerin birçok özel ihtiyacını karşılayacak biçimde şekillendirilebilir. Bulut güvenlik kuralları tek bir yerden yapılandırılıp yönetilebildiğinden genel masraflarda tasarrufun yanında BT ekiplerinin işletmenin diğer alanlarına odaklanmasına da destek olmaktadır[21].

Geleneksel olarak ortaya çıkan güvenlik endişeleri, bulut hizmetlerini, özellikle de genel bulut hizmetlerini düşünen kuruluşlar için birincil sorun olmaktadır. Ancak bu durum için ortaya çıkan talebin karşılanması amacıyla bulut hizmeti sağlayıcıları tarafından son yıllarda sunulan güvenlik uygulamaları, şirket içi güvenlik çözümlerini istikrarlı bir şekilde geride bırakmaktadır.

Güvenlik yazılımı sağlayıcısı McAfee'nin istatistikleri, şirketlerin yüzde 52'sinin, şirket içinde olduğundan daha iyi bir güvenlik deneyimi yaşadığını ortaya koymaktadır.

Bulut bilişim güvenliğini sürdürmek, eski BT ortamlarından farklı prosedürler ve çalışan becerileri gerektirir[16].

Bulut bilişim güvenliğinin kullanıcılar ve işletmeler açısından birçok avantajı bulunmaktadır. Bu avantajların bazıları aşağıda detaylandırılmıştır:

- **Merkezi Güvenlik:** Bulut bilişimde güvenlik merkezileştirilerek yönetmesi kolay hâle gelebilmektedir. Bulut sistemlerinde birden fazla cihazın ve kullanıcının kontrolü tek bir sistem ile izlenebilir veya kontrol edilebilir. Bulut sistemlerde olası saldırı veya acil durumlarda kullanılacak acil kurtarma prosedürleri de tek bir sistem ile kolaylıkla kontrol edilebilmektedir.
- **Düşük Maliyetli Güvenlik Çözümleri:** Bulut sistemlerinde güvenliğin sağlanması için özel donanımlara yatırım yapılmasına gerek yoktur. Bu sayede yazılımsal çözümler ve çalışanların uzmanlaşması ile daha ekonomik güvenlik çözümleri sağlanabilmektedir.
- **Yönetim İhtiyacının Azalması:** Bulut bilişim güvenliği referansları güvenilir bir hizmet sağlayıcıdan alındığında sistemin bu alandaki yönetimi profesyonellerce yapılacağından işletme veya kişilerin ayrıca güvenlik konularına zaman ayırmasına gerek kalmayacaktır. Bu sayede azalan yönetim sorumlulukları farklı alanlara aktarılarak iş gelişimi desteklenebilmektedir.
- **Güvenilirlik:** Bulut bilişim hizmetleri, en üst düzeyde güvenilirlik sağlayabilmektedir. Bulut bilişim güvenliği önlemleri iyi bir şekilde planlandığında kullanıcıların nerede olduğu ve hangi cihazı kullandığına bakılmaksızın buluttaki verilere ve uygulamalara güvenle erişim sağlanabilmektedir[21].

9. BULUT BİLİŞİM GÜVENLİK UYGULAMALARI

Bulut bilişim güvenliği için çok çeşitli uygulamalar bulunmaktadır. Güvenlik uygulamaları sistemin ve kuruluşun ihtiyaçlarını karşılayacak şekilde planlandığında bulut bilişim sistemleri oldukça verimli hizmet sunabilmektedir. Güvenlik önlemleri son kullanıcı kontrollerinden çeşitli şifreleme tekniklerine kadar geniş bir yelpazede değerlendirilebilmektedir.

Bulut bilişim güvenliği için aşağıda belirtilen başlıklar uygulanabilmektedir:

9.1 Strateji ve Politika

Bütünsel bir bulut güvenlik programı, bulut güvenlik risklerinin sahipliğini ve sorumluluğunu, koruma kapsamındaki boşlukları hesaba katmalıdır. Program, bulut bilişim güvenliği sisteminin güvenilirliğini olgunlaştırmak ve istenen son duruma ulaşmak için gereken kontrolleri tanımlamalıdır[22].

9.2 Ağ Segmentasyonu

Ağ segmentasyonu, bulut bilişim sisteminin erişilebilir bölgeleri arasında hangi hizmetlere izin verildiğine ilişkin katı kurallar belirlemenize olanak tanıyan kanıtlanmış bir güvenlik stratejisidir. Bu sistem bölgeler içinde hassas verilerin ve kaynakların belirlenmesi, yalnızca belirlenmiş ana bilgisayarların ve diğer onaylanmış bölgelere ait kullanıcıların bunlara ulaşmasını sağlar. Bu sayede ağ boyunca hareketler zorlaştırılarak saldırılar kısıtlanabilmektedir. Bilgisayar korsanları ve kötü amaçlı yazılımlar, veri sızdırmak için sisteme erişemez, ayrıca engellenen kötü amaçlı bağlantılar kritik varlıkları tespit etmek için bağlantı noktası taraması da yapamaz[23].

Çok kiracılı ortamlarda, kaynaklar ile diğer müşterilerin kaynakları arasında hangi ağ segmentasyonun mevcut olduğunun değerlendirilmesi gerekmektedir.

9.3 Kimlik ve Erişim Yönetimi ile Ayrıcalıklı Erişim Yönetimi

Kimlik ve erişim yönetimi (Identity and Access Management -IAM), elektronik veya dijital kimliklerin yönetimini kolaylaştıran iş süreçleri, politikalar ve bunları destekleyen teknolojilerden oluşan bir yapıdır. BT yöneticileri IAM çerçevesi ile kuruluşlarındaki kritik bilgilere kullanıcı erişimini kontrol edebilmektedir[24].

Yalnızca yetkili kullanıcıların bulut ortamına, uygulamalara ve verilere erişmesini sağlamak için güçlü kimlik yönetimi ve kimlik doğrulama süreçlerinden yararlanılması büyük fayda sağlayacaktır. Bulut bilişimin güvenliğinin sağlanabilmesi için ayrıcalıkların rol tabanlı olduğundan ve ayrıcalıklı erişimin oturum izleme yoluyla denetlenip kaydedildiğinden emin olunması gereklidir[22].

9.4 Bulut Örnekleri ve Varlıkları

Bulut örnekleri, hizmetler ve varlıklar keşfedilip gruplandırıldıktan sonra, bunların yönetilmesi için aksiyon alınması gereklidir.

Bulut bilişim yönetim sistemlerinin en önemli bileşenlerinden biri olan bulut varlıkları Bulut Varlık Yönetimi (Cloud Asset Management -CAM) adı verilen bir bileşenle kontrol edilmektedir. Bulut varlık yönetimi, bulut ortamını oluşturan tüm varlıkların ve altyapının görünürlüğünü ve kontrolünü sağlamaktadır. Daha iyi optimize edilmiş, daha güvenli bir bulut için bu bileşen çok önemli bir ilk adımdır[25].

9.5 Şifre Kontrolü (Ayrıcalıklı ve Ayrıcalıksız Şifreler)

Paylaşılan parolaların kullanımına asla izin verilmemelidir. Hassas alanlar için parolalar, diğer kimlik doğrulama sistemleriyle birleştirilerek daha güçlü bir savunma sağlanabilir. Parola yönetimi için gerekli şartlar onaylandıktan sonra uygulamaların kullanılması önerilmektedir. Bu şartlar aşağıdaki şekilde belirlenebilir:

- **Sözlük kuralı:** Hem dil sözlüklerinden hem de korsan sözlüklerinden girişler içeren parolalar engellenmelidir.
- **Klavye kalıpları:** QWERTY, 12345, ASDFGH gibi yaygın klavye kalıpları reddedilmelidir.
- **Yinelenen kalıplar:** Ardışık olarak yinelenen karakterler, kullanıcı adlarından ardışık karakterler ve palindromlar içeren parolalar yasaklanmalıdır.
- **Çoklu karmaşıklık geliştirmeleri:** Parolalarda hem küçük hem de büyük harfler zorunlu kılınmalıdır. Gereken özel karakter ve rakamların tam sayısı belirtilmelidir. Unicode karakterleri zorunlu hâle getirilerek kompleks parolaların oluşturulması desteklenmelidir.
- **Parola sıfırlamaları için parola geçmişi kontrolü:** Kullanıcıların parola sıfırlamaları sırasında belirli aralıklarla parola değiştirilmesinin hatırlatılması ve eski parolalarının kullanımı önlenmelidir[26].

9.6 Güvenlik Açığı Yönetimi

Güvenlik açığı yönetimi, bulut bilişim güvenliğinde önemli bir rol oynamaktadır. Şirket içi ana bilgisayarların güvenlik açığı yönetimi, bulut ortamlarına uygulanamaz. Bu sebeple hızla değişen bulut ortamlarının güvenliği için, güvenlik açığı yönetiminin yeni bir yaklaşıma ihtiyacı vardır.

Normalde bulut bilişim sistemleri standart şirket içi ortamlardan daha güvenli olabilmektedir. Varsayılan ağ topolojileri ve yapılandırmaları saldırganların buluttaki ana bilgisayarlardan yararlanmalarını zorlaştırmaktadır. Ancak, güvenlik açıklarını iyi bilen ve yöneten bulut hizmet sağlayıcıları tercih edilmediğinde ciddi risklerle karşı karşıya kalınabilmektedir. Güvenlik açıklarının tespit edildiği bulut hizmetleri daha güvenli bir sistemin kurgulanmasında önemlidir[27].

Düzenli olarak güvenlik açıkları taranmalıdır. Sık sık güvenlik denetimleri gerçekleştirilmeli ve bilinen güvenlik açıkları düzeltilmelidir.

9.7 Şifreleme (Encryption)

Bulut şifreleme, verilerin buluta aktarılmadan ve bulutta depolanmadan önce orijinal düz metin biçiminden şifreli metin biçimine dönüştürülme işlemidir.

Bulut şifreleme, her veri şifreleme biçiminde olduğu gibi bilgileri şifreleme anahtarları olmadan kullanılamaz hâle getirmektedir. Bu sistem ile veriler kaybolsa, çalınsa veya yetkisiz bir kullanıcıyla paylaşılsa bile şifreleme aktif şekilde verileri koruyacaktır[28].

9.8 Olağanüstü Durum Kurtarma

Bulut hizmeti sağlayıcıları için veri yedekleme, saklama ve kurtarma ilkeleri ile süreçlerinden haberdar olunmalıdır. Yedekleme sistemlerinin şirket içi standartları karşılaması gerekir. Bu sayede herhangi bir durumda yaşanan veri kaybı sonrası işletmenin tekrar faaliyete geçmesi kolaylaşmaktadır. Yedeklemenin periyodik olarak tekrarlanması ve iş modeline göre bu periyotların belirlenmesi de bir diğer önemli konudur.

9.9 İzleme, Uyarı ve Raporlama

Tüm ortamlarda ve sistemlerde sürekli güvenlik ve kullanıcı etkinliği izlenmelidir. Bulut sağlayıcıları gelen verileri kurum içi ve dışından gelen verilerle entegre etmeye ve merkezileştirmeye çalışmalıdır. Bu şekilde bulut bilişim ortamında neler olup bittiğine dair bütünsel bir resme sahip olunabilir[22].

10. BULUT BİLİŞİM GÜVENLİK ZORLUKLARI VE TEHDİTLERİ

Bulut bilişim sistemlerinin güvenliğinde yaşanan en büyük zorluk yapılandırma ve konfigürasyon eksikliklerinden kaynaklı hataların doğurduğu açıklardır. Bulut bilişim sisteminin dışarıda kullanımına izin verdiği yazılımla, servis ve uygulamalar güvenlik açıklarının temelini oluşturmaktadır[29].

Genel olarak bulut sistemleri, net sınırları olmadığından fiziksel sistemlere göre farklı bir güvenlik gerçekliği sunmaktadır. Bulut bilişim güvenliği için belirlenmiş birçok zorluk ve tehdit bulunmaktadır.

10.1 Artan Saldırı Yüzeyi

Genel olarak bulut ortamı, buluttaki iş yükleriyle verilere erişmek ve bunları bozmak için güvensiz bulut giriş bağlantı noktalarından yararlanan bilgisayar korsanları için büyük bir saldırı alanı hâline gelmiştir. Kötü Amaçlı Yazılım, Sıfır Gün, Hesap Devralma ve diğer birçok kötü amaçlı tehdit, günden güne bulut sistemler için daha fazla tehdit oluşturmaktadır[30].

10.2 Görünürlük ve Takip Eksikliği

IaaS modelinde, bulut sağlayıcılar altyapı katmanı üzerinde tam kontrole sahiptir. Ancak görünürlük ve kontrol eksikliği, PaaS ve SaaS bulut modellerinde daha da geniş bir alana hitap etmektedir. Bulut müşterileri genellikle bulut varlıklarını etkili bir şekilde tanımlayamaz ve ölçemez veya bulut ortamlarını görselleştiremez.

Özellikle çoklu bulut ortamlarında görünürlüğü artırmak için çözümler bulunsa da bunlar her çeşit bulut güvenliği görünürlüğü sorununun üstesinden gelmek için yeterli olmayabilir. Ayrıca, bir işletme uygun olmayan bir

çözümü uyguladığında yanlış bir güvenlik algısı geliştirebilir ve diğer bulut tehditlerini gözden kaçırabilir[31].

10.3 Sürekli Değişen İş Yükleri

Bulut varlıkları, dinamik olarak çeşitli ölçekte ve hızda sağlanabilmektedir. Geleneksel güvenlik araçları, sürekli değişen ve kısa ömürlü iş yükleriyle esnek ve dinamik bir ortamda koruma ilkelerini uygulamak için yetersiz kalabilir[30].

10.4 DevOps, DevSecOps ve Otomasyon

Yüksek düzeyde otomatikleştirilmiş DevOps kültürünü benimseyen kuruluşlar, sistemin geliştirme döngüsünün başlarında uygun güvenlik kontrollerinin tanımlandığından ayrıca kod ve şablonlara yerleştirildiğinden emin olmalıdır. Üretimde bir iş yükü dağıtıldıktan sonra uygulanan güvenlikle ilgili değişiklikler, kuruluşun güvenlik duruşunu zayıflatabilir ve pazara sunma süresini uzatabilir.

Geliştirme, güvenlik ve operasyonların kısaltması olan DevSecOps (Development, Security, Operations) ilk tasarımdan itibaren entegrasyon, test, dağıtım ve yazılım teslimine kadar olan bütün süreçlerde yazılım geliştirme güvenliğinin entegrasyonunu otomatikleştirir[32].

10.5 Granüler Ayrıcalık ve Anahtar Yönetimi

Bulut kullanıcı rolleri genellikle çok gevşek bir şekilde yapılandırılmaktadır. Bu roller ile kullanıcılara amaçlanan veya gerekenin ötesinde kapsamlı ayrıcalıklar sağlanabilmektedir. Bulut sistemi ile ilgili yeterli eğitimi olmayan kullanıcılara veritabanı silme veya yazma izinleri verilmesi bu durumun en büyük örneklerinden biridir. Bu ve benzeri uygulama düzeyinde yanlış yapılandırılmış anahtarlar ve ayrıcalıklar, genel anlamda oturumları güvenlik risklerine maruz bırakır[30].

Çoklu bulut bilişim ortamlarının yaygınlaşmasıyla, ayrıcalıklı erişim yönetiminin (Privileged Access Management -PAM) hem bulut hem de şirket içi sistemlerini kapsaması kritik önem taşımaya başlamıştır. Bulut sektörü tehdit raporları, ihlallerin bir numaralı nedeninin kimlik bilgilerinin ve ayrıcalıkların yanlış veya kötüye kullanılması olduğunu tespit etmiştir[33].

10.6 Karmaşık Ortamlar

Küresel ölçekte işletmeler geliştikçe bulut ortamları daha karmaşık hâle gelmeye devam etmektedir. Çoğu işletme günümüzde en az bir genel bulut ve bir özel bulut hizmeti kullanmaktadır. Yapılan araştırmalar çoğu işletmenin üç ila dört bulut sistemini bir arada kullanmaya başladığını göstermektedir. Bu karmaşık bulut ortamının yönetiminin zor olduğu kanıtlanmıştır. Karmaşıklık arttıkça bu durum daha da zorlaşacaktır[34].

Günümüzde kuruluşlar tarafından tercih edilen hibrid ve çoklu bulut ortamlarında güvenliği tutarlı bir şekilde yönetmek oldukça zordur. Sistemin güvenliğini üst düzeyde tutmak için genel bulut sağlayıcıları, özel bulut sağlayıcıları ve şirket içi bağlantılar arasında sorunsuz bir şekilde çalışan yöntemler ve araçlar gerekmektedir[33].

10.7 Bulut Uyumluluğu ve Yönetim

Bulut bilişim yönetişimi ve uyumluluğu, önemli bir nedenden dolayı kritik öneme sahiptir. Bulut bilişim, iş ve kişisel yaşamın pek çok yönünü etkilemektedir. Bulut bilişim, müşteriler için büyük verimlilik kazanımları ve maliyet avantajları sunmaktadır. Ancak bir bulut bilişim stratejisini tanıtmak basit bir işlem değildir. Bulut yönetiminin devreye girdiği yer burasıdır. Basitlik, entegrasyon ve maliyet kontrolü için birden çok bulut bilişim hizmetini yönetme süreci bulut yönetimini oluşturan en önemli alanlardır. Bulut yönetiminin mevcutta kullanılan bütün sistemler ve yazılımlarla uyumlu olması ve güvenliği aksatmadan bağlantı kurması gereklidir[35].

Önde gelen tüm bulut sağlayıcıları, PCI 3.2, NIST 800-53, HIPAA ve GDPR gibi iyi bilinen akreditasyon programlarının çoğuna uyum sağlamıştır. Ancak yönetimin doğru yapılabilmesi için müşterilerin, iş yüklerinin ve veri süreçlerinin uyumlu olmasını sağlaması gerekmektedir. Bulut ortamının dinamiklerinin yanı sıra zayıf görünürlük göz önüne alındığında, sürekli uyumluluk kontrolleri gerçekleştirmek ve yanlış yapılandırmalar hakkında gerçek zamanlı uyarılar vermek için araçlar kullanılmadıkça, uyumluluk denetimi süreci neredeyse imkânsız hâle gelmektedir[33].

Bir bulut platformu, kendi hizmet teslim modelini kullanarak birçok hizmet sunmaktadır. Fakat bulut platform üzerindeki saldırılar, hizmet kalitesine zarar vermek ve veri korumasını ihlal etmek için bulut hizmet modelinin her katmanında çeşitli bileşenleri istismar etmektedir. Bulut bilişim sistemlerine çok çeşitli saldırılar yapılabilmektedir[36].

10.8 Hizmet Hırsızlığı

Bu saldırıda, bir sistem değişkeni sıfırlanarak daha az ödeme ile sanal makinenin daha uzun süre kullanılmasına izin verilir[37].

10.9 Hizmet Aksatma

Bu saldırı türünde saldırgan bulut platformunu hedef alarak bulut müşterilerine sağlanan hizmetlerin kullanımını engellemektedir[38].

10.10 Veri Temizleme

Veri temizleme saldırısında kullanıcı, kendisine ait veriyi bulut deposundan silerken dosya sistemleri veriyi tamamen yok etmemektedir. Böylece silinen veri, saldırganlar tarafından ele geçirilerek kullanılabilmektedir[36].

10.11 Müşteri Veri Manipülasyonu

Bulut platformuna dışardan erişim sağlayan herhangi bir kullanıcı, uygulama bileşeninden sunucu uygulamasına gönderilen verileri değiştirerek web uygulamalarına saldırabilmektedir. Bulut bilişim sistemlerine SQL enjeksiyonu, komut enjeksiyonu ve siteler arası her türlü yazılı (betik) çalıştırma saldırılarıyla veri manipülasyonu kolaylıkla gerçekleştirilebilmektedir[39].

10.12 Veri Sızıntısı

Verinin transferi, depolanması, denetimi ve işlenmesi sırasında veri sahibinin yetki verdiği kullanıcılar dışında

farklı kişiler tarafından verilerin ele geçirilmesi işlemine veri sızıntısı denilmektedir[40].

10.13 Buluta Kötücül Yazılım Enjekte Etme

Buluta enjekte edilen kötücül yazılım aracılığı ile bulut verileri ele geçirilip değiştirilebilir ve verilere erişim engellenebilir hatta veri üzerinde istenilen tüm haklara sahip olunabilir. Bu saldırıda düşman kendi kötücül hizmet uygulama modelini (SaaS ya da PaaS) ya da sanal makine örneğini (IaaS) oluşturur ve buluta ekler. Daha sonra bu sistemlerin düşman tarafından saldırıya uğramış bazı özel hizmetler için geçerli örnekler arasında olduğunu ve bazı yeni hizmet uygulama örnekleri olduğunu bulut sistemine inandırır. Eğer bu davranış başarılı olursa bulut otomatik olarak geçerli kullanıcının isteklerini kötücül hizmet uygulamasına yönlendirir ve kötücül kod çalıştırılır[41].

10.14 Hedeflenmiş Paylaşılan Hafıza

Bu saldırı türünde saldırganlar hem fiziksel hem de sanal makinelerin paylaşılmış hafızalarından yararlanarak, çalışan işlem sayısı, belirli bir süre içerisinde oturum açan kullanıcı sayısı ve hafızada bulunan geçici çerezler gibi bulutun iç yapısını ortaya çıkaran bilgilere yetkisiz erişim sağlayabilmektedir[42].

10.15 Kimlik Avı

Kimlik avı saldırısı, kişisel bilgilere yetkisiz olarak erişilmesine, kullanıcı bilgisayarına kötücül bir kod indirilmesine, bulut bilişim yapısının normalden farklı bir şekilde davranmaya zorlanmasına ve son kullanıcı için sunucunun erişilemez olmasına yol açmaktadır. Ayrıca bu saldırı sadece kullanıcıları değil aynı zamanda elektronik bankalar ve elektronik ödeme sistemleri gibi destekleyici finansal kurumları da savunmasız hâle getirebilmektedir[43].

10.16 Botnet'ler

Açık bir bulut ortamı göz önüne alındığında, yönlendirme ve şaşırtma açısından uzaktan yönetilen zombi bilgisayarların en tehlikeli gruplarından biri olan botnet'ler aracılığıyla bulut kaynaklarına yetkisiz erişim yapılabilmektedir. Ayrıca bulut sisteminin anormal bir şekilde çalışması sağlanabilmekte, hassas bilgiler ve kullanıcı verileri çalınmaktadır. Teknoloji geliştikçe botnet'lerin ağlardaki kamuflajını anlamak zorlaşmaktadır. Ayrıca yeni nesillerin de algılanması için kendilerini ağ içerisinde nasıl gizlediğini öğrenmek gerekmektedir[44].

10.17 Sesli Steganografi

Bulut depolama sistemlerinin en tehlikeli saldırılarından biri olan bu saldırı ile kullanıcıların düzenli olarak ses dosyalarında sakladıkları gizli veriler istismar edilebilmektedir. Bir kullanıcı, gizli verisini normal bir ses dosyası gibi bir medya dosyası içerisine saklayarak gönderebilmekte, bu durumdan yararlanan saldırganlar, kendi kötü amaçlı kodlarını ses dosyalarında saklayıp kurban sunuculara göndererek bulut sistemlerini korumak için alınan geleneksel önlemleri ve mevcut güvenlik mekanizmalarını aldatmaktadırlar[45].

11. BULUT BİLİŞİM GÜVENLİĞİ KONUSUNDAKİ SON GELİŞMELER

Bulut bilişim, internet üzerinden dağıtılmış bilgi işlem platformu aracılığıyla isteğe bağlı kaynaklara ve hizmetlere erişim sağlayan yeni ve faydalı bir teknolojidir. Günümüzde artan sayıda kuruluş, daha iyi hizmet kalitesi, verimlilik, maliyet tasarrufu, erişilebilirlik, dağıtılmış depolama, kaynak sağlama esnekliği ve ölçeklenebilirlik gibi birçok nedenden dolayı bulut bilişime geçiş yapmaktadır. Bulut bilişim platformu, dağıtılmış bilişim ve depolamayı güçlendirmek için birbirine bağlı sistemlerle yeni teknikler kullanır[46].

Son yapılan araştırmalar küresel ölçekte kuruluşların yüzde 92'sinin BT işlemlerini bulut bilişime taşıdığını göstermiştir. COVID-19 pandemisinden sonra, uzaktan çalışmada yaşanan artış bulut bilişimin benimsenmesini hızlandırmıştır. Artan esneklik, üretkenlik ve düşük maliyetler, bu teknolojiyi dünya çapındaki işletmeler için uygun bir seçenek hâline getirmiştir. Ancak büyük faydalarının yanında getirdiği riskler bulut bilişim güvenliğinin iyi anlaşılması ve tasarlanmasını şart koşmaktadır. Günümüzde ve gelecekte bulut bilişim güvenliğinde öne çıkan teknoloji trendlerine göz atılması kuruluşlar için önem taşımaktadır[47].

11.1 Bulut Güvenliği Duruş Yönetimi (Cloud Security Posture Management -CSPM)

Yönetim veya CSPM, bulut platformu hesaplarının yapılandırmasına bakarak veri ihlallerine ve sızıntılara yol açan olası yanlış yapılandırmaları belirler. CSPM, işletmelerin emniyet ve güvenlik açısından kullanıcılarıyla güven geliştirmesine yardımcı olur. Güvenliği otomatikleştirir ve bulutta uyumluluk güvencesi sağlar[48].

11.2 Buluta Ulaşmadan Önce Müşteri Verilerinin Korunmasını Sağlama

Bulut bilişimin sayısız faydası vardır ancak güvenlik her zaman risk altındadır. Bulut veriler, sahibinin doğrudan kontrolü dışındadır ve bu nedenle veri güvenliği en önemli konu hâline gelmektedir. Artan veri ihlalleri, işletmeleri önceki veri koruma formatlarını iyileştirmeye yöneltmektedir. Bu amaçla geliştirilen şifreleme teknikleri verilerin bulut ile kullanıcı arasındaki hareketlerinde koruma altına alınmaktadır[47].

11.3 Sıfır Güven Modeli (Zero Trust Model)

Sıfır güven; ağları, uygulamaları ve verileri korumak için güven kavramını ortadan kaldıran bir BT güvenlik modelidir. Bu model, kötü aktörlerin her zaman ağın güvenilmeyen tarafında olduğunu ve güvenilir kullanıcıların her zaman güvenilen tarafta olduğunu varsayan geleneksel çevre güvenlik modelinin tam tersidir. Sıfır güven ile bu varsayımlar geçersiz kılınır ve tüm kullanıcıların güvenilmez olduğu varsayılır[49].

11.4 Bulut İçinde Yazılım Yaşam Döngüsü (SDLC) ve DevSecOps

DevOps ve bulut güvenliği, modern uygulama geliştirmenin en önemli alanlarından ikisidir. Farklı

sistemler olsalar da bunlar birbirlerini tamamlamaktadır. Bu nedenle, DevSecOps'tan en iyi şekilde yararlanmak ve DevSecOps'un bulut güvenliğinin anlamını ve önemini gerçekten anlamak için güvenli bir yazılım geliştirme yaşam döngüsünün kavranması çok önemlidir.

DevOps, yazılım geliştirme yaşam döngüsünü optimize etmeye yönelik en iyi uygulamaları içermektedir. Bu sistem, geliştirme, operasyonlar ve güvenlik ekipleri arasındaki iletişim ve işbirliğinin önemini vurgular. Ekipler, birlikte çalışarak potansiyel güvenlik sorunlarını SDLC'-de erkenden tespit edebilir ve çözebilir. Sonuç olarak iyileştirilmiş bulut güvenliği ve daha verimli bir uygulama geliştirme süreci ortaya çıkar[50].

11.5 Akıllı Bulut Bilişim Güvenliği

Yapay zekâ ve makine öğrenmesinde yaşanan gelişmeler işletmelerin güvenlik tekniklerini yeniden değerlendirmelerini gerektirmektedir. Yeni teknoloji teknik gelişmeler, verilerin tam olarak korunmasını sağlayarak işletmeleri ciddi siber hırsızlıklardan kurtarabilir. Tespit edilmeyen hırsızlıklar, iyileşmesi zaman alan ciddi hasarlara neden olabileceğinden çok önemlidir. Yapay zekâ gibi akıllı teknolojiler siber tehditlere karşı çok daha verimli ve hızlı bir savunma çözümü yaratmaktadır[47].

12. BULUT BİLİŞİM GÜVENLİĞİNİN GELECEĞİ

Bulut bilişim gelecekte bilgisayar kullanan herkesin kullanacağı bir teknoloji olarak gelişmektedir.

Küresel bulut bilişim pazarının 2021 yılında 120 milyar dolara ulaşması, özellikle pandemi sonrasında ne kadar önemli bir teknoloji hâline geldiğinin en büyük kanıtıdır[51].

BT güvenliği ve veri uyumluluğu hem işletmeler hem de müşteriler için önemli bir endişe kaynağıdır. Günümüzün hizmet veren bulut sistemleri bu endişeleri gidermek için sürekli gelişmektedir. Hizmet sağlayıcılar tekliflerini hassas verileri yönetirken insan hatası riskini azaltan önde gelen veri kontrolleri ve savunmalarla donatmaktadır.

Giderek artan veri kaynaklarından daha fazla veri toplayan şirketler veri koruma düzenlemelerini yürürlüğe koyan hükümetlerle uyumlu olacak şekilde iş modelleri planlamalıdır. Bulut sistemleri iş verilerine erişimi iyileştirirken, şirketlerin bilgileri nasıl yöneteceği hakkında ek kontrol imkânı sağlar. Veri yönetimi, özellikle hassas finansal verileri veya müşterilerle ilgili diğer kişisel bilgileri işleyen tüm BT yatırımları için temel bir konudur. Bu konu gelecekte daha da önem kazanarak siber saldırılara karşı alınması gereken önlemlerde kritik bir rol oynayacaktır[52].

Bulut bilişim güvenliği söz konusu olduğunda iki tür güvenlik teknolojisi dikkat çekmektedir. Bunlardan ilki, bir saldırıyı tespit edip yanıt veren reaktif güvenlik sistemidir. İkinci güvenlik teknolojisi ise tehlikeli bir olayı meydana gelmeden önce tahmin edebilen ve olmasını önlemek için hazırlık yapabilen tahmine dayalı güvenlik teknolojisidir. Tahmine dayalı (öngörülü) güvenlik, bulut bilişim sistemlerinin geleceğini oluşturmaktadır.

Yapay zekâ ve makine öğrenmesi de bulut bilişim güvenliğinin geleceğinde kilit rollere sahiptir. Özellikle tahmine dayalı güvenlik teknolojilerinde verilerin olağanüstü bir hızla analiz edilerek tehditlerin ortaya çıkarılması ve olası önlemlerin sunulması yapay zekâ ile mümkündür[53].

2021 yılında 34,8 milyar dolara ulaşan küresel bulut bilişim güvenliği pazarının, 2026 yılına kadar yıllık yüzde 14,2'lik bir artışla 67,6 milyar dolara ulaşması beklenmektedir. Pazarın hızlı büyümesinde daha fazla sayıda bulut tabanlı veri dağıtımı modeli ile bulut tabanlı hizmetlere olan talebin artması gibi kilit faktörler bulunmaktadır. Ayrıca, dijital dönüşüm nedeniyle artan siber saldırılar gelecekteki veri ihlallerini ve veri hırsızlıklarını önlemek için bulut güvenliği pazarının büyümesine yardımcı olmaktadır[54].

Sosyal medya, ticari kuruluşlar, devlet kuruluşları ve bireysel kullanıcılar, kullandıkları son teknolojilerin çoğunda bulut bilişimden faydalanmaktadır. Faydalanılan küçük ölçekli servislerin gelecek yıllarda artan bir hızla sömürülmesi beklendiğinden, bu alanda yenilikçi gelişmeler ve yazılımlara ihtiyaç duyulacaktır. Bulut bilişim; genişleyen pazarı, araştırma alanları ve güvenlik ihtiyaçlarıyla yükselen bir teknoloji trendi olarak öne çıkmaktadır[29].

13. SONUÇ

Bulut bilişim sistemleri teknolojinin hızla güncellendiği ve dijital dönüşümün benimsendiği günümüzde bireylerin ve işletmelerin en büyük yardımcılarından biri olarak öne çıkmaktadır. Verilerin depolandığı işlerin pandemi şartları sebebiyle uzaktan yönetildiği ve çokuluslu firmaların dünyanın her yerinden çalışanlarını tek bir platformda toplayabildiği bulut bilişim, kattığı değerlerin yanında güvenlik riskleri de barındırmaktadır.

Bulut hizmetini sunan servis sağlayıcıların veya bulut hizmetini kendi sistemine entegre eden kuruluşların gerekli bütün güvenlik açıklarını titizlikle incelemesi, müşteri ve çalışan girişlerini sıkı bir şekilde denetlemesi ve düzenli kontroller sağlaması her kullanıcı için faydalı olacaktır. Güçlü bilişim şirketlerinden danışmanlık alınması ve kullanılacak bulut bilişim sistemlerinin gelecek gelişmeler de öngörülerek güncellenebilir şekilde planlanması, büyüyen dünya ekonomisinde hayatta kalmak için kritik bir rol oynayabilir.

Bulut bilişim sistemlerinde uzmanlaşan şirketler, güvenlik uygulamalarını benzeri görülmemiş bir şekilde güçlendirmelidir. Buna ek olarak, bulut bilişim güvenliğinde tecrübe sahibi olan kuruluşlardan da dönemsel veya sürekli danışmanlık ve destek alınması, kablosuz teknolojilerin geleceğe hâkim olduğu dünyada vazgeçilmez bir teknoloji hâline gelen bulut bilişimin güvenilir, hızlı ve faydalı bir donanıma dönüşmesini sağlayacaktır.

KAYNAKÇA

[1] Frankenfield, Jake; (2020), "Cloud Computing", *Investopedia*, (28 Temmuz 2020), https://www.investopedia.com/terms/c/cloud-computing.asp. (Erişim Tarihi: 11 Ocak 2022)

[2] *IBM*, (2020), "Cloud Computing", (18 Ağustos 2020), https://www.ibm.com/cloud/learn/cloud-computing. (Erişim Tarihi: 11 Ocak 2022)

[3] Chai, Wesley; "cloud computing", *TechTarget*, https://searchcloudcomputing.techtarget.com/definition/cloud-computing. (Erişim Tarihi: 11 Ocak 2022)

[4] Bourne, James; (2012), "Nine specifications for a Cloud Computer: A call to action", *CloudTech*, (22 Haziran 2012), https://cloudcomputing-news.net/news/2012/jun/22/nine-specifications-cloud-computer-call-action/. (Erişim Tarihi: 11 Ocak 2022)

[5] *GlassHouse*, "Bulut Bilişimin Beş Temel Özelliği ve Türkiye'nin İhtiyacı Olan Altıncı Özellik", https://www.glasshouse.com.tr/list/bulut-bilisimin-bes-temel-ozelligi-ve-turkiyenin-ihtiyaci-olan-altinci-ozellik. (Erişim Tarihi: 11 Ocak 2022)

[6] Biswas, Himadri, (2021), "Recent Trends in Computational Intelligence Enabled Research", *ScienceDirect*, https://www.sciencedirect.com/topics/computer-science/on-demand-self-service. (Erişim Tarihi: 11 Ocak 2022)

[7] *techopedia*, "What Does Broad Network Access Mean?", https://www.techopedia.com/definition/28785/broad-network-access. (Erişim Tarihi: 11 Ocak 2022)

[8] *Arcitura*, "Multitenancy (and Resource Pooling)", https://patterns.arcitura.com/cloud-computing-patterns/basics/cloud-characteristics/multi_tenancy. (Erişim Tarihi: 11 Ocak 2022)

[9] Cichy, Wojciech; (2021), "Cloud Computing Scalability: What Is It and Why It's Important?" *netguru*, https://www.netguru.com/blog/cloud-computing-scalability. (Erişim Tarihi: 11 Ocak 2022)

[10] *techopedia*, "What Does Measured Service Mean?", https://www.techopedia.com/definition/14469/measured-service-cloud-computing. (Erişim Tarihi: 11 Ocak 2022)

[11] *Microsoft*, "What is cloud computing?",
https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#cloud-deployment-types. (Erişim Tarihi: 11 Ocak 2022)

[12] *wmware*, "What is Public Cloud?", https://www.vmware.com/topics/glossary/content/public-cloud. (Erişim Tarihi: 11 Ocak 2022)

[13] *IBM*, "What is supply chain management?", https://www.ibm.com/topics/private-cloud. (Erişim Tarihi: 11 Ocak 2022)

[14] *Microsoft*, "What is a private cloud?", https://azure.microsoft.com/en-us/overview/what-is-a-private-cloud/. (Erişim Tarihi: 11 Ocak 2022)

[15] NetApp, "What is hybrid cloud?", https://www.netapp.com/hybrid-cloud/what-is-hybrid-cloud/. (Erişim Tarihi: 11 Ocak 2022)

[16] *IBM*, "What is hybrid cloud?", https://www.ibm.com/topics/cloud-computing. (Erişim Tarihi: 11 Ocak 2022)

[17] *LeadingEdge*, "What are the Types of Cloud Computing?", https://www.leadingedgetech.co.uk/it-services/it-consultancy-services/cloud-computing/what-are-the-types-of-cloud-computing/. (Erişim Tarihi: 11 Ocak 2022)

[18] *Akamai*, "Cloud Computing Services", https://www.akamai.com/our-thinking/cloud/cloud-computing. (Erişim Tarihi: 11 Ocak 2022)

[19] Drake, Nate; Turner, Brian; (2022), *ITProPortal*, (4 Ocak 2022), https://www.itproportal.com/guides/best-cloud-computing-services/. (Erişim Tarihi: 11 Ocak 2022)

[20] *Microsoft*, "Top benefits of cloud computing", https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#cloud-deployment-types. (Erişim Tarihi: 11 Ocak 2022)

[21] *Forcepoint*, "Bulut Güvenliği nedir?", https://www.forcepoint.com/tr/cyber-edu/cloud-security. (Erişim Tarihi: 11 Ocak 2022)

[22] *BeyondTrust*, "Cloud Security/Cloud Computing Security", https://www.beyondtrust.com/resources/glossary/cloud-security-cloud-computing-security. (Erişim Tarihi: 11 Ocak 2022)

[23] Rheault, Dan; (2019), "Cloud Network Segmentation: Mission Impossible?", *The Security Policy Company*, (21 Mayıs 2019), https://www.tufin.com/blog/cloud-network-segmentation. (Erişim Tarihi: 11 Ocak 2022)

[24] Gittlen, Sandra; "What is identity and access management? Guide to IAM", *TechTarget*, https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system. (Erişim Tarihi: 11 Ocak 2022)

[25] *Cass Information Systems*, (2019), "What is identity and access management? Guide to IAM", (28 Şubat 2019), https://www.cassinfo.com/cloud-management-blog/what-is-cloud-asset-management. (Erişim Tarihi: 11 Ocak 2022)

[26] *ManageEngine*, "Enforce better cloud security with granular password policies", https://www.manageengine.com/products/self-serice-password/multi-platform-granular-password-policy.html. (Erişim Tarihi: 11 Ocak 2022)

[27] Srinivasan, Hari; Ward, Ashley; (2021), "Cloud Vulnerability Management for Hosts" *paloalto*, (9 Temmuz 2021), https://www.paloalto networks.com/blog/prisma-cloud/cloud-vulnerability-management/. (Erişim Tarihi: 11 Ocak 2022)

[28] *Crowdstrike*, "What is Cloud Encryption?", https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-encryption/. (Erişim Tarihi: 11 Ocak 2022)

[29] *STM ThinkTech*, (2022), "Bütünleşik Güvenlik Bağlamında Siber", (18 Şubat 2022), https://thinktech.stm.com.tr/tr/butunlesik-guvenlik-baglaminda-siber. (Erişim Tarihi: 18 Şubat 2022)

[30] *Checpoint*, "What is Cloud Security?", https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/. (Erişim Tarihi: 11 Ocak 2022)

[31] *CloudHealth*, "How You Can Overcome Cloud Security Visibility Issues In Multicloud Environments", https://www.cloudhealthtech.com/blog/how-you-can-overcome-cloud-security-visibility-issues-multicloud-environments. (Erişim Tarihi: 11 Ocak 2022)

[32] *IBM*, "What is supply chain management?", https://www.ibm.com/topics/devsecops. (Erişim Tarihi: 11 Ocak 2022)

[33] *BeyondTrust*, (2019), "Effective Privilege Management for the Cloud: The 3 Keys", (27 Kasım 2019), https://www.beyondtrust.com/blog/entry/effective-privilege-management-for-the-cloud-the-3-keys. (Erişim Tarihi: 11 Ocak 2022)

[34] Newman, Daniel; (2017), "Mastering the Management of Complex Cloud Environments", Converge, (18 Nisan 2017), https://convergetechmedia.com/mastering-management-complex-cloud-environments/. (Erişim Tarihi: 11 Ocak 2022)

[35] Taylor, Christine; (2017), "Cloud Computing Governance and Compliance", *Datamation*, (13 Nisan 2017), https://www.datamation.com/cloud/cloud-computing-governance-and-compliance/. (Erişim Tarihi: 11 Ocak 2022)

[36] KARABEY AKSAKALLI, Işıl; "BULUT BİLİŞİMDE GÜVENLİK ZAFİYETLERİ, TEHDİTLER VE BU TEHDİTLERE YÖNELİK GÜVENLİK ÖNERİLERİNİN İNCELENMESİ", *Dergipark*, https://dergipark.org.tr/tr/download/article-file/751027

[37] Ahmad, Azeem; (2016), "An identification and prevention of theft-of-service attack on cloud computing", *Research Gate*, (Nisan 2016), https://www.researchgate.net/publication/304457193_An_identification_and_prevention_of_theft-of-service_attack_on_cloud_computing. (Erişim Tarihi: 11 Ocak 2022)

[38] R, Deshmukh; K, Devadkar; (2015), "Understanding DDoS attack & its effect in cloud environment", https://www.mendeley.com/catalogue/81e325e6-d60a-312c-a0d7-bcc45aa5331f/. (Erişim Tarihi: 11 Ocak 2022)

[39] Hashizume, Keiko; (2013), "An analysis of security issues for cloud computing", *Springer Open*, (27 Şubat 2013), https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5. (Erişim Tarihi: 11 Ocak 2022)

[40] *Ioactive*, (2010), "Top Threats to Cloud Computing V1.0", (Mart 2010), https://ioactive.com/wp-content/uploads/2018/05/csathreats.v1.0-1.pdf. (Erişim Tarihi: 11 Ocak 2022)

[41] Mašetić, Zerina; (2017), "Cloud computing threats classification model based on the detection feasibility of machine learning algorithms", Research Gate, (Temmuz 2017), https://www.researchgate.net/publication/318493757_Cloud_computing_threats_classification_model_based_on_the_detection_feasibility_of_machine_learning_algorithms. (Erişim Tarihi: 11 Ocak 2022)

[42] M. Khalil, Issa; (2014), "Cloud computing security: A survey", *New Jersey Institute of Technology*, (Mart 2014), https://researchwith.njit.edu/en/publications/cloud-computing-security-a-survey. (Erişim Tarihi: 11 Ocak 2022)

[43] Mahalingam M, Sankara; (2016), "Cloud Based Security Center: To Protect Networking Attack by Forensic Scrutiny", *International Journal of Computer Science and Network Security*, (Şubat 2016), http://paper.ijcsns.org/07_book/201602/20160214.pdf. (Erişim Tarihi: 11 Ocak 2022)

[44] R Kebande, Victor; (2014), "A Cognitive Approach for Botnet Detection Using Artificial Immune System in the Cloud", *Research Gate*, (Nisan 2014), https://www.researchgate.net/publication/265778893_A_Cognitive_Approach_for_Botnet_Detection_Using_Artificial_Immune_System_in_the_Cloud. (Erişim Tarihi: 11 Ocak 2022)

[45] Tupakula, Udaya; (2011), "Intrusion Detection Techniques for Infrastructure as a Service Cloud", *Research Gate*, (Aralık 2011), https://www.researchgate.net/publication/220716332_Intrusion_Detection_Techniques_for_Infrastructure_as_a_Service_Cloud. (Erişim Tarihi: 11 Ocak 2022)

[46] Malomo, Olumide; (2018), "A Survey on Recent Advances in Cloud Computing Security", *Research Gate*, (Mart 2018), https://www.researchgate.net/publication/324277661_A_Survey_on_Recent_Advances_in_Cloud_Computing_Security. (Erişim Tarihi: 11 Ocak 2022)

[47] Belani, Gaurav; (2021), "8 Cloud Security Trends to Watch Out For in 2022", IEEE, (10 Eylül 2021), https://www.computer.org/publications/tech-news/trends/8-cloud-security-trends-2022. (Erişim Tarihi: 11 Ocak 2022)

[48] S. Gillis, Alexander; "Cloud Security Posture Management (CSPM)", https://searchcloudsecurity.techtarget.com/definition/Cloud-Security-Posture-Management-CSPM. (Erişim Tarihi: 11 Ocak 2022)

[49] Paloalto, "What Is Zero Trust for the Cloud?", https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-for-the-cloud. (Erişim Tarihi: 11 Ocak 2022)

[50] *ProjectCubicle*, "Basic SDLC Process for DevSecOps to Improve Cloud Security", https://www.projectcubicle.com/basic-sdlc-practices-for-devsecops-to-improve-cloud-security/. (Erişim Tarihi: 11 Ocak 2022)

[51] Goodison, Donna; (2020), "10 Future Cloud Computing Trends To Watch In 2021", *CRN*, (20 Kasım 2020), https://www.crn.com/news/cloud/10-future-cloud-computing-trends-to-watch-in-2021. (Erişim Tarihi: 11 Ocak 2022)

[52] Beaver, Scott; (2021), "19 Key Cloud Computing Trends to Watch in 2022", Oracle Netsuite, (13 Ekim 2021), https://www.netsuite.com/portal/resource/articles/erp/cloud-computing-trends.shtml. (Erişim Tarihi: 11 Ocak 2022)

[53] Almeda, Jesse; (2021), "What Does the Future Hold for Cloud Security?", (2 Mayıs 2021), https://hackernoon.com/what-does-the-future-hold-for-cloud-security-i82e35md. (Erişim Tarihi: 11 Ocak 2022)

[54] *Businesswire*, (2021), "Global Cloud Security Market (2021 to 2026) - by Application, Security Type, Service Model, Deployment, Organization Size, Industry Vertical and Geography - ResearchAndMarkets.com", (5 Ağustos 2021), https://www.businesswire.com/news/home/20210805005670/en/Global-Cloud-Security-Market-2021-to-2026---by-Application-Security-Type-Service-Model-Deployment-Organization-Size-Industry-Vertical-and-Geography---ResearchAndMarkets.com. (Erişim Tarihi: 11 Ocak 2022)

thinktech
STM Teknolojik Düşünce Merkezi
http://thinktech.stm.com.tr