

Gizli bilgi işleme çevrimiçi etkileşimlerin güvenliğini dönüştürüyor

Bulut tabanlı verilerin güvenli bir biçimde işlenebilmesi, sağlık hizmetlerinden kişisel finansa kadar geniş bir alanda dijital ilişkileri kökünden değiştiriyor



Gizli bilgi işleme, çevrimiçi etkileşimlerin güvenliğini dönüştürüyor

Bulut tabanlı verilerin güvenli bir biçimde işlenebilmesi, sağlık hizmetlerinden kişisel finansa kadar geniş bir alanda dijital ilişkileri kökünden değiştiriyor

Volkan Sözmen, IBM Türkiye Genel Müdürü

Sosyal mesafe ve uzaktan çalışma, pek çok iş yapış şeklini ve alışkanlığı yeniden tanımlıyor. Bununla birlikte çevrimiçi işlemlerin ve etkileşimlerin önemi, karmaşıklığı ve sıklığı da artıyor. Ancak dijital etkileşimlerin güvenliğini sağlamaya yönelik önlemlerin çoğu, birbiriyle sınırlı sayıda bağlantılara sahip bir dünya için geliştirilmişti. Öte yandan günümüzde birçok çevrimiçi işlem sadece kişisel verilerimiz aracılığıyla sağlanıyor, bu verilerin kötüye kullanılmayacağına inanırken yaşanan ihlaller duyduğumuz bu güveni zedeliyor.

Dijital işlemlerin kullanımı arttıkça ve bulut üzerinden daha fazla bilgi paylaşıldıkça; veri hırsızlığı ve sahtekârlık riskleri de artıyor. Dijital güvenin kötüye kullanılmasına dair haberlerdeki artış günümüzde kullanılmaya devam eden dijital şifrelemeye

duyulan güvensizliğin de katlanarak artmasına neden oluyor.

Kompleks bulut teknolojileri etrafında inşa edilmiş bir dünyada dünün şifreleme ve güvenlik akışları, operasyonların güvenliğini tam anlamıyla sağlayamaz.

IBM Security'nin Temmuz ayında yayınlandığı araştırma sonuçlarına göre ise veri ihlalleri, araştırmaya katılan şirketlere ortalama 4,24 milyon dolara mal oldu. Bu sonuç, raporun yayınlandığı 17 yıl boyunca görülen en yüksek maliyet olarak göze çarptı. 500'den fazla kuruluşta meydana gelen veri ihlallerine ilişkin kapsamlı analizlere dayanan araştırma, pandemi sırasında gerçekleşen büyük değişimler sebebiyle güvenlik açıklarının çok daha maliyetli ve kontrol altına alınması zor hale geldiğini ve maliyetlerin önceki yıla kıyasla yüzde 10 oranında arttığını gösteriyor.

Türkiye'den de 21 kuruluşun katıldığı araştırmada, çalınan kimlik bilgileri, yüzde 22 oranla veri ihlalinin en yaygın olduğu alan olurken, bunu yüzde 16 ile e-dolandırıcılık ve yüzde 15 ile yanlış bulut yapılandırması izliyor. Bu faktörler Türkiye'deki bir şirketin sırasıyla ortalama 1,29 milyon dolar, 2,19 milyon dolar ve 1,68 milyon dolar zarara uğradığını da ortaya koyuyor. Araştırmaya zarara sebep olan en pahalı neden ise ortalama 2,25 milyon dolarla üçüncü taraf yazılımlardaki güvenlik açıkları olarak belirlendi.

Basitçe ifade etmek gerekirse kişisel verilerle sağlanan güvenlik kompleks şifreleme ortamları için uygun değildir. Neyse ki, gizli bilgi işleme adı verilen yeni bir güvenlik inovasyonu bu sorunu çözme ve çok daha fazlasını sağlama potansiyeline sahip.

Gizli bilgi işleme nedir?

Şu ana kadar şifreleme yalnızca veriler herhangi bir donanım üzerinde tutulurken ya da bir ağ bağlantısı üzerinde hareket halinde olduğu durumlarda mümkündü. Gizli bilgi işleme, şifrelemeyi donanım tabanlı güvenilir bir yürütme ortamında işleterek verileri kullanım sırasında da koruyor ve bu süreçte yaşanabilecek olası güvenlik açıklarını da ortadan kaldırıyor. Bu yeni teknoloji, iki karşılıklı tarafın birbirlerinin bilgilerine erişmeksizin verileriyle etkileşim kurmasına olanak sağlama yeteneğine de sahip. Yerleşik şifreleme anahtarlarının kullanılması sayesinde de dış dünyadan erişilmesi kesinlikle mümkün değil.

Bir siber saldırganın sisteme yetkisiz erişmesi ve depolanan verileri alması durumunda, şifreleme anahtarı gibi bir araçla şifre çözülemedikçe, bulut sağlayıcısı dahil olmak üzere üçüncü partilerin şifreleme anahtarlara erişimi olmadığı için bu veriler kullanılamıyor. Dolayısıyla bu anahtar güvende tutulduğu ve dışarıdan gözlemlenemediği sürece veriler güvende kalıyor. İşte bu nedenle IBM Cloud Hyper Protect Services, Kendi Anahtarını Sakla (KYOK-Keep Your Own Key) özelliğini destekleyerek;

anahtarların yalnızca veri sahibinin kontrolünde olmasını ve bulut üzerinde verilerine erişimi kendisinin kontrol etmesini sağlıyor.

Gizli bilgi işleme nasıl uygulanabilir?

Gizli bilgi işleme yöntemleri kötü amaçlı kodun operasyon verilerine erişmesini engelleyebiliyor. Bu sayede Suudi Arabistan'daki Petro Rabigh petrokimya tesisini çevrimdışı bırakan saldırıya benzer siber saldırıların azaltılması veya önlenmesi için kullanılması mümkün. Ancak teknoloji, basit korumanın ötesine geçen çeşitli ek avantajlar da sunuyor; ticari ilişkilerin yönetilmesinde önemli bir rol üstleniyor.

Gizli bilgi işleme sayesinde, verilerin korunan bir bilgi işlem ortamında işlenmesini sağlayarak; fikri mülkiyeti savunmasız hale getirmeden veya mülkiyet haklarına tabi bilgileri açıklamadan, güvenli bir biçimde iş birliği yapmak mümkün. Gizli bilgi işleme, veri kümelerini birleştirmesine imkân tanıyarak farklı kuruluşların birbirlerinin bilgilerini görmeksizin analiz edilmesini sağlıyor. Örneğin, bir şirket, ticari açıdan hassas fikri mülkiyet gibi gizli tutmak istediği bilgilerin tümünü paylaşmadan verilerini başka bir şirketin tescilli araçlarının kullanımına açabilir.

Gizli bilgi işleme neden önemli?

Dijital alanda güvenlik gündeme yeni gelen bir konu değil. Örneğin, internet iletişiminin HTTPS ile korunması ve kredi kartı işlemlerine uygulanan ama sonrasında her yerde kullanılmaya başlanan SSL ve TLS gibi köklü bir uygulama. Gizli bilgi işleme de bulut teknolojisinin yaygın bir biçimde benimsenmesi ve inovasyonların hızından dolayı aynı ölçüde yaygınlaşma potansiyeline sahip.

Verilerin bulut çapında paylaşılması saldırılara açık bir kapı bırakırken, bulut ortamında işlenen veriler de yeni bir risk alanı yaratıyor. Gizli bilgi işleme, kullanıcılara çevrimiçi etkileşimler ve işlemler gerçekleştirirken ihtiyaç duydukları güvenliği sunarak, bu endişeleri doğrudan ortadan kaldırıyor. Bu nedenle, özellikle iş dünyasında gizli bilgi işlemeye yönelik ilginin artması şaşırtıcı değil.

Gizli bilgi işlemenin geleceğinde ne var?

Gizli bilgi işlemenin belirgin kullanım alanlarından biri; çoğu verinin hassas nitelikte olduğu ve hastalar, sağlık hizmetleri sağlayıcıları ve yöneticileri arasında karmaşık bir ağın olduğu sağlık hizmetleri sektörü. Uygulanması kişisel tıbbi verilerin ve bireysel tedavilerin yönetilmesinin ötesine uzanıyor. Aynı zamanda ilaç geliştirme alanında da kullanılması ve çok sayıda ilaç şirketi arasında her katılımcının fikri mülkiyetini savunmasız hale getirmeksizin, güvenli iş birliğine olanak sağlaması mümkün.

Benzeri yöntemler, anlaşmalara dair gizli ayrıntıların hukuk firmaları tarafından işlenmesini ve aracılık sağlanmasını gerektiren birleşme ve satın alma gibi uygulamalar için de kullanılmasına imkan veriyor. Bankalar ve perakende sektöründe ise, tarafların ticari bakımdan hassas verilere erişim sağlamaksızın; olası sahtekârlığı belirlemek üzere işlem kayıtlarını karşılıklı olarak kontrol etme olanağını elde ediyor.

Gizli bilgi işleme aynı zamanda yeni hizmet türleri sunma potansiyeline de sahip. Örneğin; Fransa merkezli Irene Energy, Sahra Altı Afrika'da insanların tek bir elektrik kaynağını paylaşmalarına ve yalnızca kullandıkları enerjinin ücretlendirilmesine olanak sağlayan bir enerji paketi işletiyor. Bu “enerji dolaşımı”, gizli bilgi işleme aracılığıyla doğrulanan dijital cüzdanların kullanımını esas alıyor.

Bankalar için gizli bilgi işlemenin, güvenlik kontrollerinde iki yönlü bir süreç haline de gelme olasılığı var. Müşteriler kendilerini arayan kişilerin güvenilir bir yetkili olup olmadığını ve banka da müşterinin söylediği kişi olup olmadığını, Privakey gibi şirketlerin sunduğu güvenlik işlemleri aracılığıyla; gizli bilgi işleme tabanlı güvenilir, otomatikleştirilmiş, aracılı süreçler kullanarak doğrulayabiliyorlar.

Taviz vermeksizin veri paylaşımı

Giderek artan dijital platformlar üzerinden işleyen bir dünyada, gizli bilgi işleme tarafından sağlanan veri güvenliği düzeyine duyulan ihtiyaç hiç bu kadar gerekli olmamıştı. Gizli bilgi işlemenin temel işlevleri sağlık hizmetleri, finansal hizmetler, kamu ve suçla mücadele dahil olmak üzere bir dizi sektörü dönüştürme potansiyeline sahip. Bu avantajların optimize edilmesi için; eksiksiz bir gizli bilgi işleme araçları yelpazesine, bunları verimli ve etkili bir biçimde devreye alma konusunda kanıtlanmış başarılı bir geçmişe sahip olmak son derece önemli. Son olarak, bu sistemi BT altyapısına entegre etme yeteneğine sahip bir teknoloji ortağıyla iş birliği yapmak büyük önem taşıyor.

<https://mea.newsroom.ibm.com/Gizli-bilgi-isleme>