Confidential Computing

Çağrı Günaydın

Eylül 2023

Doğuş Teknoloji

İçindekiler

Giriş

Cloud Computing, farklı sistemlere ihtiyaç duymadan, kullanıcıların internet üzerinden yazılım ve donanım hizmetlerini internet üzerinden almalarını ifade eder. Bu sayede, kullanıcıların Cloud üzerinden faydalandıkları yazılım ve donanımlarının bakımlarını ve geliştirmelerini Cloud merkezlerine bırakmalarını, ihtiyaçları dahilinde kolayca ölçeklendirebilecekleri bir hizmet almalarını sağlar. Düşük maliyetler, yüksek erişim yetenekleri, esnek yapıları gibi sebeplerle, Cloud kullanımı yazılım dünyasında hızla yükselmeye devam etmektedir. Bununla beraber yazılım sistemlerinin ve verilerin internet ortamında tutulması bir takım siber güvenlik sorunlarını da beraberinde getirmektedir. Cloud ortamlarının bu yüksek kullanım oranları, siber suçluların iştahını kabartmaktadır. Cloud ortamlarının ve internetin açıklarını yakalamak ve bu sistemlere sızmak isteyen kötü niyetli kişilerce sürekli saldırılar düzenlenmekte, Cloud yöneticileri ise sürekli iyileştirme modeli ile kendi sistemlerini güvenli tutmaya çalışmaktadır. Bu noktada riskin çift taraflı yani, hem kullanıcı, hem Cloud servis sağlayıcı tarafından ortaklaşa alındığını ifade etmek gereklidir. Servis sağlayıcıları, sistemlerini güvenlik açıklarına karşı sürekli yenilemek durumundayken, kullanıcı tarafı da bunlara uygun olarak sistemlerinin ve verilerinin güvenliğini sağlamak durumundadır. Bu risklerden bazıları ve çözümü için kullanılan yöntemler aşağıda listelenmiştir.

Kaynakların Yönetimi, Kontrolü ve İzlenmesi

Bir Cloud kullanıcısı tarafından kurulan bir sistemde kullanıcı, sistemin yazılımsal ve donanımsal kaynaklarını servis sağlayıcısına bırakmış demektir. Bu durum, eğer kullanıcı tarafında bu kaynakların managing/ monitoring gibi, sistemin sürekli takip edilmesi gereken çıktılarını görmezden gelmesine sebep olabilir. Cloud bir sistem kurulurken ilk olarak bunların da, hem bir maliyet kalemi olarak, hem de sistemin mimari tasarımında belirleyici bir nitelikte değerlendirilmesi ve uygun şekilde kurgulanması gerekmektedir. Bu şekilde sistemin, konfigürasyon ve network bazlı izlenmeleri takip edilmeli ve sistemin loglamaları yapılmalı ve daha şeffaf şekilde maliyet ve sistem yönetimi yapılmalıdır. Cloud servis sağlayıcıları bu gibi monitoring ve logging ihtiyaçları için pek çok tool sağlamaktadır.

Yanlış Konfigürasyonlar

Cloud sistemleri için konfigürasyonların doğru yapılandırılması hayati öneme sahiptir. Sistemin ve verilerin korunması için konfigürasyonların takibi yapılmalı ve kullanıcı tarafından kontrol edilmelidir. Bu şekilde konfigürasyon hatalarının önüne geçilmelidir.

Veri Kayıpları

Servis sağlayıcılarında yaşanan bir kesinti ya da hatadan veya kullanıcı kaynaklı öngörülemez bir durumdan kaynaklanan veri kayıplarının önüne geçilmesi için kullanıcı tarafında bir takım yedekleme mekanizmaları kurulmalıdır. Cloud servis sağlayıcıları, coğrafi olarak dağıtık data centerları yüksek iletişim ağlarıyla etkin bir şekilde yönettikleri için data kayıpları konusunda oldukça dayanıklıdır. Fakat kullanıcıların bunu kendi ihtiyaçlarına göre aktif bir şekilde kullanmaları beklenmektedir. Uygulamaların ve verilerin yedeklenmiş olarak tutulduğundan emin olunmalıdır.

Veri Sızıntıları

Cloud sistemler kullanan firmaların sistem kaynaklı oluşabilecek sızıntılara karşı özellikle dikkat etmesi gerekmektedir. Bu sızıntıların önüne geçmek için kullanılan sistem bazında regülasyonlar geliştirilmelidir. Cloud ortamları kullanmanın avantajları firmalar için çok fazla olmasına rağmen, önemli dataları sızıntıya karşı açık hale getirdiklerinin farkında olarak çalışmaları gerekmektedir.

Güvensiz Dış Bağlantılar

Cloud üzerinde servis edilen uygulamalar içerisinde kullanılan, sistemin dış bağlantılarını sağlayan sistemler üzerindeki güvenlik zaafiyetleri olmamasına özellikle dikkat edilmelidir. API'lar, veri senkronizasyonu için yazılan yan sistemler veya üçüncü parti entegrasyonları gibi, sistemlerin cloud dışına erişim bacaklarında ekstra güvenlik yöntemleri kullanmak gerekmektedir. Bu, verilerin encrypt edilmesinden, IP white list yöntemlerine kadar geniş güvenlik önlemlerini kapsayabilir.

Confidential Computing

Bir veri, donanımsal perspektiften incelendiğinde üç ana state'te bulunabilir. Bunlar; saklama (data in rest), transfer (data in transit) ve işlem(data in use) durumlarıdır. Geleneksel veri güvenlik modelleri data in rest ve data in transit statelerinde kriptografi kullanırken data in use state'inde kriptorafi kullanılmaz.

Confidential Computing, data in use state'indeki hassas verilerin Trusted Execution Environment (TEE) ortamından, korumalı bir işlemci tarafından izole edilerek, donanımsal seviyede korunmasıdır. Verilerin işlenirken bile korunması olarak tanımlanabilir.

Bu yaklaşımda veriler, donanımsal seviyede kapsüllenir ve sadece yetkilendirilmiş program kodu tarafından erişilebilir hale getirilir. bu seviyede, Cloud servis sağlayıcısı dahil, herhangi bir üçüncü parti tarafından görülemez.

Confidential Computing sayesinde, Cloud kullanıcıları, hassas verileri Cloud ortamlarında işlem anında bile koruyabilir. Confidential Computing, Cloud sistemlerinde veri gizliliği ve güvenliği için ekstra bir koruma seviyesi sağlar.

Geleneksel Veri Kontrolleri vs Confidential Computing

Geleneksel güvenlik modelleri, verilerin saklanması ve aktarılması sırasında koruma sağlar, ancak veri işlendiği sırada decrypt edilir. Confidential Computing ise veriyi işlerken de şifreli bir şekilde işlem yaparak bu boşluğu kapatmayı amaçlar.

Veri Koruma Alanı

Geleneksel güvenlik modellerinde veriler, genellikle aktarım (data in use) (örneğin, internet üzerinden gönderilirken) ve rest(data in rest) (örneğin, bir sabit sürücüde saklanırken) esnasında korunur. Confidential Computing'te ise işlenirken (yani çalışma zamanında) bile korunur.

Donanım Kullanımı

Geleneksel modellerde yazılım tabanlı güvenlik protokolleri kullanılır. Confidential Computing'te ise özel donanımlar veya modülleri (örneğin, özelleştirilmiş CPU'lar, donanım tabanlı enclave) kullanarak veri işleme sırasında veri güvenliğini sağlar.

Amaç ve Odak

Geleneksel modeller, yetkisiz erişimi engellemek ve veri sızıntılarını önlemek odaklıdır. Confidential Computing, ayrıca, yetkili kullanıcıların ve sistemlerin bile işlenen veriyi görmemesini sağlamak odaklıdır.

Bulut Hizmetleri ile Etkileşim

Geleneksel modeller, Cloud sağlayıcısının altyapısına güven duyar. Confidential Computing ise Cloud sağlayıcısına dahi veriye erişim yetkisi vermez, bu sayede veri işlendiğinde bile sağlayıcının veriyi görmesini engeller.

Geleneksel güvenlik modelleri ve confidential computing, tamamlayıcı yaklaşımlardır ve birçok durumda birlikte kullanılmaları, kapsamlı bir güvenlik stratejisi oluşturmak için en iyisidir.

Confidential Computing Consortium

Confidential Computing Consortium, Linux Foundition çatısı altında kurulmuş bir yazılım endüstrisi topluluğudur. Bu konsorsiyum, veri işleme anında (data in use) verilerin korunmasının (Trusted Execution Environment, kısaca TEE'nin) bir endüstri standardı haline gelmesini, donanım üreticilerini, Cloud servis sağlayıcıları ve yazılımcıları bir araya getirerek, açık kaynak projeleri destekleyerek ve tanıtarak destekler.

Birçok büyük teknoloji şirketinin bir araya gelmesiyle oluşturulmuştur. Bu şirketler Confidential Computing teknolojisinin endüstride benimsenmesi ve geliştirilmesi için ortak çalışma grupları oluşturarak, endüstri standartlarını belirleme ve uygulamaya koyma konusunda katkıda bulunmuştur.

Cloud Sağlayıcılarının Maliyetlendirme Yaklaşımları

Cloud servis sağlayıcıları farklı pek çok çözümü kullanıcının seçimine bırakmışlardır. Confidential computing, yapısı gereği bir donanımsal farklılığa gereksinim duyduğu için kullanılan server bilgisayarlar ve servis sağlayıcılar bazında farklılıklar oluşmaktadır. Bu sebeple ilgili çözümün maliyetleri kullanılan server'a ve sağlayıcıya göre değişiklik göstermektedir.

Örneğin Azure üzerinde pek çok farklı üründe confidential computing çözümleri sunulmaktadır. Azure, bu çözümler üzerinde farklı fiyatlandırma politikaları belirlemiştir. Örneğin, Confidential VM çözümünde ekstra bir ücret alınmaz, sadece server maliyeti değişiklik gösterir.

Related products

Confidential VMs with Application Enclaves

Create enclaves that protect data while processing in the CPU by keeping it encrypted and isolated in memory, thus protecting data from the operating system, hypervisors with escalated privileges, and Azure operators.

Confidential VMs

Easy way to deploy confidential workloads without requiring changes to existing applications or code

Confidential containers

Deploy and manage containerized applications more easily with a fully managed Kubernetes service

SQL Azure Always Encrypted

Expand confidential computing capabilities of Always Encrypted by enabling in-place encryption and richer confidential queries

Trusted launch

Improve the security of generation 2 VMs with trusted launch, protecting against advanced and persistent attack techniques

Azure confidential ledger

Tamperproof, unstructured data store hosted in trusted execution environments (TEEs) and backed by cryptographically verifiable evidence

Microsoft Azure Attestation

Remotely verify the trustworthiness of a platform and the integrity of the binaries running inside it

Azure Key Vault M-HSM

Safeguard cryptographic keys and other secrets used by cloud apps and services

Google Cloud tarafında ise, ücretlendirme fiyat üzerinden değil, cpu ve memory bazında belirlenmektedir. Eylül 2023 ayına ait fiyatlandırma bilgisi aşağıda yer almaktadır.

Pricing overview

Confidential VM incurs additional flat per-vCPU and per-GB costs,which vary depending on whether a Confidential VM instance is on demand or preemptible, as summarized in the following table:

Item	On-demand price	Spot price*
vCPUs	$4.000 / vCPU month	$0.936 / vCPU month
Memory	$0.536 / GB month	$0.125 / GB month

*Spot prices are dynamic and can change up to once every 30 days, but always provide discounts of 60-91% off of the corresponding on-demand price for machine types and GPUs. Spot prices also provide smaller discounts for local SSDs. For more information, see the Spot VMs documentation.

Doğuş Teknoloji'de Confidential Computing

Doğuş Teknoloji bünyesinde, hassas veriler barındıran tüm sistemler için Confidential Computing çözümü ekstra bir güvenlik katmanı olarak kurgulanabilir.

Doğuş İnşaat bünyesinde sözleşmeler ve maliyetler hassas veriler barındırdığından bu proje için Confidential Computing değerlendirilmelidir. Sigorta yazılımları ve otomotiv tarafında da müşteri bilgileri ve finansal verileri güvende tutmak için kullanılabilir.

Ayrıca, finans, sağlık, e-ticaret gibi sektörlerin yazılımlarında, KVKK, BTK, BDDK düzenlemeleri gibi hükümet programları dahilindeki regülasyonlara tabii tüm projelerde de değerlendirilmelidir.

Confidential Computing Kullanan Yazılım Çözümleri

Enarx

Enarx, Trusted Execution Environtment'ın platform bağımsız şekilde özel,esnek ve serverless mimariye kullanılması için üretilmiştir. Tamamen open source olan bu proje, uygulamaların yeniden düzenlenmesine ihtiyaç duymadan Confidential Computing teknolojisine uygun şekilde deploy edilmesine olanak sağlar. Rust, C/C++, C#, Go, Java, Python, Haskell gibi pek çok dili destekler.

Gramine

İşletim sistemi tabanlı esneklik sağlamak amaçlı oluşturulmuş bir uygulamadır. Intel, Software Guard Extensions (SGX) modeli için Confidential Computing yapısını Gramine ile ortaklaşa kurmuştur.

Occlum

Open source ve kullanımı ücretsiz olan Occlum, SGX gibi enclave teknolojilerinin kullanımını kolaylaştırmak için oluşturulmuş özel bir yazılımdır. Mevcut bir uygulamayı ve datalarını kendi bünyesi içerisinde korumaya alır, bu sayede Confidential Computing kullanımı için uygulamanın özel olarak gözden geçirilmesinin önüne geçmiş olur.

Confidential Computing Olası Kullanım Alanları

Confidential Computing, veriyi işlerken bile koruyabilme yeteneği sayesinde pek çok sektör için cazip bir çözüm sunmaktadır. Aşağıda birkaç farklı sektör ve kullanım alanları örnekleri verilmiştir.

Sağlık

Hastane ve hasta kayıtları, tıbbi araştırmalar gibi hassas verilerin işlendiği sağlık sektöründe verinin gizliliği büyük önem taşımaktadır.

Finans

Bankalar, finansal kuruluşlar ve sigorta şirketleri, müşteri bilgilerini, işlem detaylarını ve diğer kritik finansal verileri güvende tutmak için Confidential Computing'den faydalanabilir.

Devlet Yapıları

Devlet daireleri ve kamu kurumları, kişisel bilgileri, vergi kayıtlarını ve diğer pek çok hassas bilgiyi işlerken bu teknolojiyi kullanabilir.

Eğitim

Öğrenci kayıtları, notlar ve diğer kişisel bilgilerin, akademide yapılan araştırmaların ve bunların sonuçlarının güvenli bir şekilde işlenmesi için eğitim sektöründe kullanılabilir.

Perakende ve E-ticaret

Müşteri bilgileri, satın alma geçmişi ve ödeme bilgileri gibi kritik verilerin korunması için bu sektörde kullanılabilir.

Telekomünikasyon

Kullanıcı verileri, arama kayıtları, internet kullanımları, altyapı bilgileri ve diğer iletişim bilgilerini güvenli bir şekilde işlemek için Cloud Computing teknolojisini kullanabilir.

Enerji

Akıllı şebekeler, enerji tüketimi verileri ve altyapı bilgileri gibi, ülke yapısı için kritik seviyede olan verilerin işlenmesinde kullanılabilir.

Araştırma ve Geliştirme

Özellikle rekabetçi endüstrilerde, araştırma ve geliştirme verilerinin korunması büyük önem taşımaktadır. Bu araştırmaların tutulduğu sistemlerin mimarilerinde Cloud Computing'den faydalanılabilinir.

EDGE Lokasyonlarında Kullanımı

Cloud Servis Sağlayıcıları, EDGE lokasyonlarında confidential computing çözümlerinden faydalanmaktadır. Edge computing, veri işleme görevlerini merkezi bir bulut altyapısından daha yaygın bir şekilde dağıtılmış konumlara, trafiğin daha hızlı yönetilmesi için EDGE lokasyonları üzerinden taşımaktadır. Bu, veriyi kaynağında işleyerek gecikmeyi azaltır ve bant genişliği kullanımını optimize eder.

Bu tür yaygın ve dağıtılmış lokasyonlarda, veri güvenliği ve gizliliği büyük bir endişe haline gelir. Özellikle, EDGE lokasyonlarının fiziksel güvenliği her zaman merkezi veri merkezleri kadar sıkı olmadığı için, bu lokasyonlarda çalışan uygulamalar ve servisler için ekstra güvenlik katmanlarına ihtiyaç duyar.

Confidential computing, EDGE lokasyonlarında çalışan uygulamaların ve servislerin verilerini işlerken ve EDGE trafiğini yönetirken gizli tutmalarına yardımcı olabilir. Bu, hem verinin hem de işleme algoritmalarının yetkisiz erişimlere veya gözetimlere karşı korunmasını sağlar.

Özetle, EDGE computing'in getirdiği güvenlik zorluklarına yanıt olarak, birçok bulut sağlayıcısı ve teknoloji şirketi, Confidential Computing çözümlerini EDGE lokasyonlarına da entegre etmektedir.

2022'nin başlarına kadar, birçok büyük teknoloji şirketi confidential computing'i kendi platformlarına entegre etmeye başladı. Bu firmalar arasında Microsoft, Google, IBM, Intel ve Alibaba gibi devler bulunmaktadır.

Bu büyük teknoloji firmalarının dışında, birçok diğer şirket ve kuruluş da confidential computing teknolojisini kendi altyapılarında ve ürünlerinde kullanmaktadır. Ancak, EDGE lokasyonlarına spesifik olarak bu teknolojinin uygulandığına dair net örnekler, zamanla daha belirgin hale gelecektir, çünkü Confidential Computing'in yaygınlaşması ve uygulama alanlarının genişlemesi sürekli bir evrim içindedir.

Quantum Computing'in Gelişimi ve Sektöre Olası Etkileri

Quantum computing'in gelişimi, kriptografi ve bilgi güvenliği üzerinde derin etkilere sahip olabilecek potansiyelde, çığır açıcı bir teknolojik gelişimdir. Özellikle, quantum bilgisayarların bazı klasik kriptografik şemaları kırma potansiyeli, mevcut güvenlik yaklaşımlarının ve teknolojilerinin nasıl oluşturulduğunun ve kullanıldığının sektör tarafından yeniden değerlendirilmesini gerektirebilir.

Mevcut şifreleme algoritmaların birçoğu, quantum bilgisayarların saldırılarına karşı savunmasız olabilir. Özellikle, RSA ve ECC gibi halka açık anahtar kriptografisi şemaları, etkili bir quantum algoritması olan Shor'un algoritmasıyla tehdit altında olabilir. Confidential computing, donanımsal seviyede veri gizliliği

sağlayabilme özelliği sayesinde, quantum-dirençli kriptografiye geçiş için, bu alanda kritik bir rol oynama fırsatı yakalayabilir.

Quantum Computing'in gelişimi, bilgi güvenliği alanında radikal değişikliklere neden olacak gibi görünmektedir. Ancak bu, sektörün bu tehditlere karşı proaktif bir şekilde hazırlık yapmasını ve yeni güvenlik stratejileri geliştirmesini teşvik edecektir. Confidential Computing bu noktada sektörün ihtiyaç duyduğu seviyede güvenliği sağlayabilir.

Kuantum bilgisayarlara karşı dirençli yeni kriptografik şemaların geliştirilmesi, Confidential Computing'in gelecekteki uygulamaları için önemlidir. Bu algoritmalara geçiş, mevcut sistemlerin güvende kalmalarına yardımcı olacaktır.

Quantum-dirençli kriptografik algoritmalar, klasik algoritmalara göre daha fazla hesaplama kaynağına ihtiyaç duyabilir. Bu, Confidential Computing çözümlerinin performansı ve etkinliği üzerinde olumsuz bir etkiye sahip olabilir.

Şu anda Quantum Computing üzerinde aktif olarak çalışılmaya devam etmektedir. Honeywell firmasının yeni modeli olan “System Model H1” quantum volume ölçeğini (Quantum Volume: IBM tarafından oluşturulan bu tanım, 2017 yılında quantum bilgisayarlarının performansını ölçmek için firmanın ortaya koyduğu bir konsepttir.) %400 arttırarak 512’ye çıkartmıştır. Bu gelişmeyle beraber en geç 10-15 yıl içerisinde quantum bilgisayarların hayatımıza gireceği tahmin edilmektedir.

Quantum -dirençli şifrelemeler üzerine çalışmaların hızlanmasının sebebi ise, Quantum bilgisayarlar devreye girdiği anda geleneksel şifreleme yöntemleri geçersiz kalacak olmasıdır. Bu sebeple pek çok yeni şifreleme konseptleri ortaya çıkmaya devam etmektedir.

National Institute of Standards and Technology(NIST)’te çalışan matematikçi Dustin Moody’e göre; firmalar, mümkün olan en hızlı şekilde quantum-dirençli şifrelemelere geçmelidir. Moody, büyük ölçekli kuantum bilgisayarların bugün kullanılan kriptografik sistemleri kırabilecek saldırılarda kullanılabileceğini belirtiyor -- bu nedenle, bir saldırganın yapması gereken tek şey şimdiki bilgiyi toplamak ve gelecekte deşifre etmek üzere saklamaktır.

Moody bu konu üzerine şunları söylemiştir;

“It's important to make sure we can counter this threat now, There will be a transition with these algorithms, and it won't necessarily be easy. We are trying to prepare as much as we can and encourage others to do so.”

“Bu tehdidi şimdi karşılayabileceğimizden emin olmalıyız. Algoritmalar arasında geçiş yapılması gerekecek ve bu da kolay olmayacak. Elimizden geldiği kadar hazır olmaya çalışıyoruz ve herkesi de buna karşı hazırlanmaya teşvik ediyoruz.”

Quantum Computing'in getireceği tehditler, güvenlik uzmanlarını ve araştırmacıları, bilgi güvenliği için yeni modeller ve yaklaşımlar oluşturmaya teşvik edecektir. Bu, Confidential Computing'in evrimine ve nasıl uygulandığına yönlendirici olacaktır.

Sonuç

Bu çalışma, Confidential Computing’in bilgi güvenliği üzerinde nasıl bir potansiyeli olduğunu inceledi. Quantum Computing’in getireceği tehditlerin varlığı, güvenlik uzmanları ve araştırmacıları, mevcut güvenlik yöntemlerini sorgulamaya ve bilgi güvenliği için yenilikçi modeller ve yaklaşımlar oluşturmaya teşvik ediyor. Bu yenilikçi düşünme biçimi, Confidential Computing'in gelecekteki yönünü de şekillendirecektir. Özellikle, bu teknolojinin evrimi ve uygulama metodolojisi, Quantum Computing'in sunduğu potansiyel tehditler ışığında yeniden değerlendirilmelidir. Sonuç olarak, Confidential Computing'in yükselişi, bilgi güvenliğindeki proaktif ve yenilikçi stratejilerin bir sonucu olarak ortaya çıkmıştır.

Referanslar

https://www.aquasec.com/cloud-native-academy/cspm/top-7-risks-of-cloud-computing/
https://www.dataversity.net/10-cloud-computing-risks-every-business-should-know/
https://en.wikipedia.org/wiki/Confidential_computing
https://www.ibm.com/topics/confidential-computing
https://confidentialcomputing.io/about/
https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-vm-overview
https://profian.com/white-paper/an-introduction-to-confidential-computing/
https://www.researchgate.net/publication/372801790_Confidential_Computing
https://www.zdnet.com/article/the-future-of-tech-confidential-computing-quantum-safe-cryptography-take-center-stage/