2025 Yılında Dosya Bütünlüğü: Sağlam Veri Koruması için En Son ve En Etkili 10 Gelişmiş Teknik ve Eğilim

I. Yönetici Özeti

Dosya bütünlüğü, yani verinin yetkisiz değişikliklere veya bozulmalara karşı korunmuş olduğunun güvence altına alınması, siber güvenliğin temel direklerinden biridir. Günümüzün giderek dijitalleşen dünyasında, verinin en değerli varlıklardan biri haline gelmesiyle birlikte, bireyler, kurumlar ve devletler için dijital varlıkların korunması hayati önem taşımaktadır.[1] Fidye yazılımları, kötü amaçlı yazılımlar ve gelişmiş kalıcı tehditler gibi siber tehditlerin artan karmaşıklığı, dosya bütünlüğüne yönelik geleneksel yaklaşımların ötesine geçen proaktif ve çok katmanlı bir stratejiyi zorunlu kılmaktadır.[1]

Bu rapor, 2025 yılında dosya bütünlüğünü yeniden tanımlayacak on çığır açan teknik ve eğilimi detaylandırmaktadır. Bu teknikler arasında, anomali tespiti için yapay zeka (YZ) ve makine öğreniminden (ML) yararlanan gerçek zamanlı izleme, blok zinciri aracılığıyla değişmez veri kökeni sağlama, kuantum sonrası kriptografi (PQC) ile geleceğe yönelik güvenlik, homomorfik şifreleme ve sıfır bilgi ispatları (ZKP'ler) kullanılarak gizliliği koruyan doğrulama yer almaktadır. Bu ilerlemeler, tespit yeteneklerini geliştirmeyi, yanıtları otomatikleştirmeyi, doğrulama sırasında veri gizliliğini sağlamayı ve bütünlüğün sağlam, yasal olarak kabul edilebilir kanıtlarını sunmayı vaat ederek, dijital güveni ve siber tehditlere karşı dayanıklılığı önemli ölçüde artıracaktır.

II. Giriş: Dosya Bütünlüğünün Gelişen Manzarası

Dosya bütünlüğü, bir verinin son yetkili değişikliğinden bu yana bozulmadığı veya üzerinde oynanmadığına dair güvenilirlik anlamına gelir. Gizlilik ve erişilebilirlik ile birlikte bilgi güvenliğinin temel bir bileşenidir.[1] Veri ihlallerinin gizlilik kaybına, mali zararlara ve itibar zedelenmesine yol açabileceği günümüz dijital çağında, dosya bütünlüğünün önemi sadece veri korumanın ötesine geçerek operasyonel sürekliliği, yasal uyumluluğu ve kurumsal itibarı doğrudan etkilemektedir.[1] Kişisel verilerin hukuka aykırı işlenmesini ve erişimini önlemek, uygun güvenlik düzeyini temin etmek için teknik ve idari tedbirlerin alınması zorunludur.[2]

Veri Bütünlüğüne Yönelik Artan Tehdit Ortamı (2025)

Dijital ortam, her gün ortaya çıkan yeni çevrimiçi tehditlerle karakterize edilmektedir. Virüsler, solucanlar, fidye yazılımları, oltalama saldırıları ve DDoS saldırıları gibi yaygın tehditler, kişisel veri hırsızlığından kurumsal faaliyetlerin aksamasına kadar geniş bir yelpazede zararlar verebilmektedir.[1] Siber suçlardaki artış, dosya bütünlüğü izleme (FIM) pazarının hızla büyümesini tetiklemektedir; pazar büyüklüğünün 2024'te 1,07

milyar dolardan 2025'te 1,24 milyar dolara çıkması beklenmektedir.[3] Siber saldırıların artan karmaşıklığı, sürekli gelişen siber güvenlik önlemlerinin dinamik olmasını gerektirmektedir.[1] İşletmelerin dijital teknolojilere artan bağımlılığı ve siber suçlular tarafından kullanılan gelişmiş teknikler, dosya bütünlüğünü sağlamak için dinamik ve uyarlanabilir yaklaşımlara olan kritik ihtiyacın altını çizmektedir.[1]

Geleneksel Hash ve Sağlama Toplamlarının Sınırlılıkları

Geleneksel olarak, dosya bütünlüğünü doğrulamak için hash algoritmaları ve sağlama toplamları kullanılmıştır. MD5 gibi hash algoritmaları, hızları ve verimlilikleri nedeniyle dosya aktarımları sırasında bütünlük kontrolleri ve sağlama toplamları için popüler bir seçim olmuştur.[5] Ancak, iki farklı girdinin aynı hash değerini üretebildiği çakışma saldırılarına karşı güvenlik açıkları nedeniyle, MD5 artık kriptografik amaçlar için güvenli kabul edilmemektedir.[5] SHA-256 ve SHA3-256 gibi daha yeni algoritmalar, MD5'e kıyasla daha yüksek güvenlik seviyeleri sunmakta ve daha güçlü saldırılara karşı dirençli olarak modern uygulamalar için tercih edilmektedir.[5]

Döngüsel Artıklık Kontrolü (CRC) gibi sağlama toplamları, dosya aktarımları sırasında veya depolama sırasında kazara veri bozulmalarını tespit etmede etkilidir.[7] Ancak, CRC'ler kötü niyetli kurcalamalara karşı korunmak için tasarlanmamıştır; bir CRC hatası, dosyanın bozuk veya eksik indiğini veya depolandığı alanda bir sorun olduğunu gösterir.[7] Bu geleneksel yöntemlerin sınırlılıkları, 2025 ve sonrasında dosya bütünlüğü doğrulaması için daha sağlam, kriptografik olarak güvenli ve akıllı yaklaşımlara duyulan ihtiyacı ortaya koymaktadır.

III. 2025 Yılında En Son ve En Etkili 10 Dosya Bütünlüğü Tekniği ve Eğilimi

1. Çekirdek Seviyesi ve Olay Odaklı Sistemlerle Gerçek Zamanlı Dosya Bütünlüğü İzleme (FIM)

Gerçek zamanlı Dosya Bütünlüğü İzleme (FIM) çözümleri, dosya sistemlerindeki yetkisiz değişiklikleri sürekli olarak denetleyerek tespit üzerine anında uyarılar sağlar.[3] Bu yetenek, güvenlik olaylarına hızlı yanıt vermek için kritik öneme sahiptir. Uç noktalara veya sunuculara ajanların kurulmasını içeren ajan tabanlı FIM, çevrimdışı dosyalardaki değişiklikleri bile izleme yeteneği de dahil olmak üzere ayrıntılı, gerçek zamanlı ve son derece doğru izleme sunar.[4] Bu ajanlar genellikle, değişikliği kimin yaptığı ve hangi sürecin kullanıldığı gibi meta verileri yakalayarak dosya sistemi olaylarına derinlemesine görünürlük sağlamak için çekirdek seviyesi sürücüleri kullanır.[3] Bu yaklaşım, hızlı hareket eden tehditlere karşı daha az etkili olan yoklama tabanlı

FIM'in aksine, üstün bir koruma katmanı sağlar.[12]

Gerçek zamanlı FIM ve çekirdek seviyesi izlemeye yapılan vurgu [3], siber güvenlikte reaktif olay yanıtından proaktif tehdit önleme ve anında hafifletmeye doğru stratejik bir dönüşü ifade etmektedir. Geleneksel FIM genellikle periyodik kontrollere dayanır [15], bu da değişikliklerin tespit edilmeden gerçekleşebileceği bir zaman penceresi bırakır. Fidye yazılımı gibi modern siber tehditler son derece hızlı hareket eder.[16] Buna karşı koymak için gerçek zamanlı tespit esastır. Çekirdek seviyesi izleme, en derin görünürlüğü ve anında olay yakalamayı sağlayarak neredeyse anında uyarılar gönderir. Bu, güvenlik ekiplerinin fidye yazılımı gibi tehditleri önemli bir hasar oluşmadan önce tespit etmesini ve yanıtlamasını mümkün kılar, böylece "tespit et ve kurtar" duruşundan "önle ve hafiflet" duruşuna geçişi sağlar.

FIM'in Güvenlik Bilgi ve Olay Yönetimi (SIEM) ve Uç Nokta Tespit ve Yanıt (EDR) çözümleriyle entegrasyonu [4] sadece veri konsolidasyonu ile ilgili değildir; FIM uyarılarının otomatik yanıtları tetiklediği, genel güvenlik duruşunu ve operasyonel verimliliği artıran bir ekosistem yaratmakla ilgilidir. FIM, dosya değişiklikleri hakkında uyarılar üretir. Bu uyarılar izole edilirse, manuel inceleme gerektirir, bu da yavaş ve insan hatasına açıktır. FIM'i SIEM ile entegre etmek, FIM olaylarının diğer güvenlik günlükleriyle (ağ trafiği, kullanıcı etkinliği vb.) ilişkilendirilmesine olanak tanıyarak daha zengin bir bağlam sağlar.[4] EDR entegrasyonu, tehlikeye atılmış sistemleri izole etme veya kötü amaçlı süreçleri sonlandırma gibi otomatik eylemleri mümkün kılar.[16] Bu sinerji, ham FIM verilerini eyleme dönüştürülebilir istihbarata ve otomatik savunma mekanizmalarına dönüştürerek, tehditleri tespit etme ve yanıtlama ortalama süresini (MTTD/MTTR) önemli ölçüde azaltır. FIM'in değeri, daha geniş, entegre bir güvenlik çerçevesinin parçası olduğunda artırılır.

Tablo 1: Gerçek Zamanlı FIM Çözümlerinin Karşılaştırması (2025 Görünümü)

Çözüm Adı	Satıcı	Fiyatlandırma Modeli (Varsa)	Temel Özellikler	Derecelendirmeler/Yorumlar (Varsa)
Paessler PRTG	Paessler GmbH	PRTG 500 için 2149 $	Kapsamlı izleme, esnek uyarı, küme yük devretme, dağıtılmış izleme, derinlemesine	696-698 Derecelendirme [9]

			raporlama, SIEM yetenekleri [9]	
ManageEngine EventLog Analyzer	ManageEngine	595 $ / yıl	SIEM yetenekleri (log analizi, konsolidasyon, kullanıcı etkinliği izleme, FIM), gerçek zamanlı uyarı, veri ihlali önleme [9]	155 Derecelendirme [9]
ManageEngine ADAudit Plus	Zoho	595 $ / yıl	Gerçek zamanlı izleme, kullanıcı ve varlık davranış analizi (UEBA), AD değişiklik denetim raporları, ayrıcalık kötüye kullanımını azaltma [9]	408 Derecelendirme [9]
Microsoft Defender for Cloud	Microsoft	Ücretsiz Deneme Mevcut	CSPM ve CWPP, Azure, şirket içi ve çoklu bulut kaynakları için FIM, anahtar güvenlik ve uyumluluk standartları için yerleşik destek [17]	8.4/10 (99 Yorum) [17]
CrowdStrike Falcon	CrowdStrike	Ücretsiz Deneme Mevcut	Uç nokta koruma paketi, tehdit tespiti, ML kötü amaçlı yazılım tespiti, imza içermeyen güncelleme [17]	9/10 (319 Yorum) [17]

Netwrix Change Tracker	Netwrix	Yok	Güvenlik yapılandırma yönetimi, yetkisiz değişiklikleri vurgulama, risk yönetimi yetenekleri, uyumluluk kanıtı [17]	10/10 (1 Yorum) [17]

2. Dosya Sistemlerinde Anomali Tespiti için Yapay Zeka ve Makine Öğrenimi

Yapay Zeka (YZ) ve Makine Öğrenimi (ML), geleneksel FIM yöntemlerini aşarak gelişmiş anomali tespiti yetenekleri sunarak dosya bütünlüğü izlemeyi dönüştürmektedir.[3] Geleneksel imza tabanlı tespit yöntemlerinin aksine, YZ/ML algoritmaları normal ağ trafiği ve kullanıcı davranış kalıplarını öğrenir.[18] Bu öğrenilmiş temellerden herhangi bir önemli sapma, anomali olarak işaretlenebilir ve böylece yeni, "sıfır gün" tehditlerinin tespiti sağlanır.[13] Bu yaklaşım, yanlış pozitifleri önemli ölçüde azaltır ve tehdit tespitinin doğruluğunu artırır.[4] Python kütüphaneleri PyOD ve scikit-learn, bu tür anomali tespit sistemlerini uygulamak için uygun çeşitli algoritmalar (örn. Isolation Forest, One-Class SVM, K-means) sunmaktadır.[26]

YZ/ML'in dosya bütünlüğünde anomali tespiti için artan kullanımı, statik, imza tabanlı tehdit tespitinden dinamik, davranış tabanlı analize doğru temel bir dönüşü ifade etmektedir. Geleneksel antivirüs ve FIM genellikle imza veritabanlarına dayanır.[18] Bu, bilinen tehditlere karşı etkilidir ancak yeni, polimorfik veya sıfır gün saldırılarına karşı yetersiz kalır. YZ/ML, özellikle denetimsiz öğrenme teknikleri, dosya sistemi etkinliği, kullanıcı davranışı ve ağ kalıplarının "normal" bir temelini oluşturabilir.[18] Bu öğrenilmiş normalden herhangi bir sapma, bilinen bir imzası olmasa bile kötü amaçlı etkinliği gösterebilir.[20] Bu, daha önce görülmemiş tehditlerin tespitini mümkün kılar ve daha dayanıklı bir savunma sunar.

YZ/ML tespiti artırırken, YZ/ML modellerine yönelik "düşmanca saldırılar" ve "veri zehirlenmesi"nin yükselişi [30] yeni bir zorluk teşkil etmekte ve sürekli öğrenme ve uyarlanabilir güvenlik duruşlarını gerekli kılmaktadır. YZ/ML modelleri veriler üzerinde eğitilir. Eğer bu eğitim verileri manipüle edilirse (veri zehirlenmesi) veya saldırganlar tespitten kaçmak için özel olarak tasarlanmış girdiler oluştururlarsa (düşmanca saldırılar), YZ modeli kendisi bir güvenlik açığı haline gelebilir.[30] Bu durum, YZ odaklı FIM sistemlerinin statik olamayacağı; yeni verilerden ve denenmiş saldırılardan sürekli olarak öğrenmesi ve gelişmesi gerektiği anlamına gelir.[16] Bu, sağlam model doğrulama,

güvenli veri işleme ve potansiyel olarak YZ savunma sistemlerinin "kırmızı takım" değerlendirmelerini gerektirir.[31] YZ modelinin güvenliği, dosya bütünlüğünün kritik bir bileşeni haline gelmektedir.

Tablo 2: Dosya Anomali Tespiti için Python Kütüphaneleri (YZ/ML)

Kütüphane Adı	Birincil Kullanım Durumu	Desteklenen Temel Algoritmalar	Güçlü Yönler	Sınırlılıklar	FIM Bağlamında Örnek Kullanım
PyOD	Genel anomali tespiti	Isolation Forest, Local Outlier Factor (LOF), AutoEncoders [26]	Kapsamlı algoritmalar, ölçeklenebilirlik, küçük ve büyük veri kümeleri için optimizasyonlar [28]	Daha uzmanlaşmış, daha fazla algoritma seçeneği [28]	FIM günlüklerindeki sıra dışı dosya değişikliklerini veya erişim kalıplarını tespit etmek [27]
Scikit-learn	Genel makine öğrenimi, basit anomali tespiti	One-Class SVM, Isolation Forest [26]	Geniş ML araç setiyle sorunsuz entegrasyon, kullanıcı dostu [28]	PyOD'a göre daha az özel anomali tespiti algoritması [28]	Normal dosya sistemi davranışının bir temelini oluşturmak ve sapmaları belirlemek [26]
Prophet	Zaman serisi verileri	Trend, mevsimsellik ve tatil modellemesi [28]	Zaman serisi verileri için özel olarak tasarlanmış, sunucu trafiği gibi metrikleri izlemek için kullanışlı [28]	Zaman serisi dışındaki veriler için uygun değil [28]	Dosya değişiklik sıklığındaki veya boyutundaki zaman içindeki anomalileri izlemek
Watchdog	Dosya	N/A (izleme	Platformlar	Doğrudan	Şüpheli

	sistemi olay izleme	aracı) [32]	arası (Windows, macOS, Linux), gerçek zamanlı olay yakalama, özel olay işleyicileri [32]	anomali tespiti algoritması sağlamaz, YZ/ML ile entegrasyon gerektirir [32]	dosya oluşturma, değiştirme veya silme olaylarını anında tetiklemek için bir FIM sisteminde temel olarak kullanılır [27]
PyCrypto/PyCryptodome	Kriptografik fonksiyonlar	Şifreleme, şifre çözme, dijital imzalar, hash fonksiyonları [34]	Veri gizliliğini ve bütünlüğünü korur, güvenli iletişim ve depolama [34]	Anomali tespiti için doğrudan kullanılmaz, ancak FIM'de hash oluşturma ve doğrulama için temeldir [34]	Dosya hash'lerini oluşturmak ve doğrulamak, değiştirilmemiş olduklarından emin olmak [34]

3. Değişmez Dosya Kökeni ve Doğrulaması için Blok Zinciri

Blok zinciri teknolojisi, dijital varlık işlemlerini depolamak için merkezi olmayan, doğrulanabilir ve değişmez bir defter hizmeti sunar.[36] Kriptografik hashing'den yararlanarak, dosyaların "parmak izleri" (hash'leri) bir blok zincirine güvenli bir şekilde kaydedilebilir.[38] Bu, dosyada yapılacak herhangi bir sonraki değişikliğin hash'ini değiştirmesini sağlayarak, blok zincirindeki değişmez kayıtla karşılaştırılarak anında tespit edilmesini sağlar.[38] Bu süreç, kurcalamaya karşı dayanıklı bir denetim izi ve değişmezlik kanıtı oluşturur.[37]

Blok zincirinin değişmezliği ve merkezi olmayan yapısı, güven modelini tek, merkezi bir otoriteden dağıtılmış bir ağa temelden kaydırarak dosya bütünlüğü için şeffaflığı ve denetlenebilirliği artırır. Geleneksel sistemlerde, günlük dosyaları ve bütünlük kayıtları genellikle merkezileştirilmiştir ve içeriden kötü niyetli kişiler veya sofistike saldırganlar tarafından kurcalanmaya karşı savunmasızdır.[42] Tehlikeye atılmış merkezi bir otorite kayıtları tahrif edebilir. Blok zinciri, defteri birden çok düğüm arasında dağıtarak ve bloklar arasında kriptografik bağlantılar kullanarak, geçmiş kayıtların tespit edilmeden değiştirilmesini pratik olarak imkansız hale getirir.[36] Bu doğal kurcalamaya karşı dayanıklılık, herhangi bir değişikliğin tüm ağ katılımcıları tarafından görünür olacağı anlamına gelir [46], daha yüksek bir güven düzeyi oluşturur ve denetim izleri için

doğrulanabilir orijinallik sağlar.[42]

Blok zinciri veri bütünlüğünü artırırken, değişmezliği GDPR gibi veri koruma düzenlemelerine uyum konusunda önemli zorluklar yaratmaktadır, özellikle veri silme ("unutulma hakkı") ile ilgili olarak.[36] Bu, bütünlük için tasarlanmış bir teknolojinin gizlilik gereklilikleriyle çeliştiği bir paradoks yaratır. GDPR Madde 17, bireylere kişisel verilerinin silinmesini talep etme hakkı tanır. Blok zincirinin temel ilkesi değişmezliktir; veriler bir kez kaydedildiğinde kolayca değiştirilemez veya silinemez.[46] Bu doğrudan çelişki, kişisel olarak tanımlanabilir bilgilerin (PII) doğrudan halka açık bir blok zincirinde depolanmasının sorunlu olduğu anlamına gelir. Çözümler, yalnızca verilerin kriptografik hash'lerinin zincir üzerinde depolanmasını, asıl verilerin zincir dışında tutulmasını veya blok zinciri ile birlikte Sıfır Bilgi İspatları veya Homomorfik Şifreleme gibi gizlilik artırıcı teknolojilerin kullanılmasını içerebilir.[46] Bu, blok zincirinin hassas veri bütünlüğü kullanım durumlarında daha geniş çapta benimsenmesi için ele alınması gereken kritik bir yasal ve etik hususu vurgulamaktadır.

4. Hash Fonksiyonlarının Geleceğe Hazırlanması için Kuantum Sonrası Kriptografi (PQC)

Yeterince güçlü kuantum bilgisayarların ortaya çıkışı, RSA ve ECC gibi birçok açık anahtarlı kriptosistem de dahil olmak üzere mevcut kriptografik sistemler için önemli bir tehdit oluşturmaktadır.[48] Kuantum Sonrası Kriptografi (PQC) algoritmaları, hem klasik hem de kuantum bilgisayarlardan gelen saldırılara dayanacak şekilde tasarlanmıştır.[48] Hash fonksiyonlarının kendileri genellikle asimetrik şifrelemeye göre kuantum saldırılarına karşı daha dirençli olsa da, Grover algoritması kaba kuvvet saldırılarını hızlandırabilir ve bu da güvenlik seviyelerini korumak için hash boyutunun artırılmasını (örn. SHA3-256'dan SHA3-512'ye yükseltme) gerektirir.[50] Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), PQC algoritmaları için çok yıllı bir standardizasyon sürecine öncülük etmektedir; ilk standartlar 2024'te (ML-KEM, ML-DSA, SLH-DSA) yayınlanmış ve HQC gibi diğer seçimlerin 2027'ye kadar kesinleşmesi beklenmektedir.[49]

PQC'nin benimsenmesinin aciliyeti, yalnızca acil tehditten değil, aynı zamanda hassas verilerin bugün şifrelenmiş olsa bile gelecekteki kuantum bilgisayarlar tarafından depolanıp şifresi çözülebileceği "şimdi topla, sonra şifresini çöz" senaryosundan kaynaklanmaktadır.[53] Yeterince güçlü bir kuantum bilgisayar, mevcut şifreleme standartlarını geriye dönük olarak kırabilir.[53] Bu, veriler bugün güvenli bir şekilde şifrelenmiş olsa bile, uzun süre gizli kalması gerekiyorsa (örn. devlet sırları, tıbbi kayıtlar), gelecekte savunmasız kalabileceği anlamına gelir. Bu durum, hataya dayanıklı kuantum bilgisayarlar yaygınlaşmadan önce bile, uzun vadeli hassas bilgileri korumak

için PQC'ye proaktif bir geçişi zorunlu kılmaktadır. Özellikle arşiv verileri için dosya bütünlüğü, bu uzun vadeli kriptografik dayanıklılığı dikkate almalıdır.

PQC algoritmaları genellikle daha büyük anahtar boyutları ve daha karmaşık hesaplamalar gerektirir, bu da geleneksel yöntemlere kıyasla daha yüksek işlem gücü ve bellek gereksinimlerine yol açar.[50] Bu, eski sistemler ve IoT cihazları gibi kaynak kısıtlı ortamlar için önemli entegrasyon zorlukları yaratır. PQC gelecekteki güvenliği sunarken, pratik uygulaması önemsiz değildir. Kıyaslamalar, Kyber gibi algoritmaların, PQC adayları arasında verimli olsa da, hala performans değerlendirmeleri olduğunu göstermektedir.[57] Bu performans yükü, gerçek zamanlı sistemleri ve IoT cihazlarını etkileyebilir.[50] Ayrıca, mevcut sistemlerin taşınması, kriptografik kütüphanelerin yeniden yazılmasını, protokollerin güncellenmesini ve geriye dönük uyumluluğun sağlanmasını gerektirir; bu da potansiyel güvenlik açıkları yaratır ve uzmanlık gerektirir.[50] Bu, karmaşık, aşamalı bir geçiş stratejisi ve iş gücü eğitimi ile satıcı hazırlığına önemli yatırımı gerektirmektedir.[48]

Tablo 3: NIST PQC Standardizasyon Durumu ve Algoritma Özellikleri (2025)

Algoritma Adı	Tür (KEM/Dijital İmza)	Durum (Standartlaştırıldı/ Taslak)	Temel Matematiksel Problem	Anahtar/Şifre Metni Boyutları (Bayt)	Performans (ms) (Anahtar Üretimi / Kapsülleme / Kapsülleme Çözme)	Bellek Kullanımı (RAM, KB)
CRYSTALS-Kyber (ML-KEM)	Anahtar Kapsülleme Mekanizması (KEM)	Standartlaştırıldı (FIPS 203, 2022)	Kafes Tabanlı (MLWE) [56]	Genel: 1184 (Ortak Anahtar), 1088 (Şifre Metni) [57]	~0.04 / ~0.05 / ~0.06 [57]	~4 [57]
HQC	Anahtar Kapsülleme Mekanizması (KEM)	Taslak (2025, 2027'de kesinleşecek) [49]	Kod Tabanlı (Hata Düzeltme Kodları) [49]	Genel: 2254 (Ortak Anahtar), 4482	~0.10 / ~0.18 / ~0.22 [57]	~10 [57]

				(Şifre Metni) [57]		
CRYSTALS-Dilithium (ML-DSA)	Dijital İmza Algoritması (DSA)	Standartlaştırıldı (FIPS 204, 2022) [53]	Kafes Tabanlı [56]	N/A	N/A	N/A
FALCON (FN-DSA)	Dijital İmza Algoritması (DSA)	Taslak (FIPS 206, yakında) [49]	Kafes Tabanlı [56]	N/A	N/A	N/A
SPHINCS+ (SLH-DSA)	Dijital İmza Algoritması (DSA)	Standartlaştırıldı (FIPS 205, 2022) [53]	Hash Tabanlı [50]	N/A	N/A	N/A

5. Gelişmiş Dijital İmzalar ve Sertifika Yönetimi

Dijital imzalar, e-posta iletileri, makrolar veya elektronik belgeler gibi dijital bilgiler üzerinde kimlik doğrulamasının elektronik, şifrelenmiş bir damgasıdır.[59] Bilgilerin imzalayan kişiden geldiğinin ve değiştirilmediğinin kanıtını sunarak orijinallik, bütünlük ve inkar edilemezlik sağlar.[59] 2025 yılında, odak noktası NIST tarafından standartlaştırılmış ML-DSA (CRYSTALS-Dilithium) ve SLH-DSA (SPHINCS+) gibi PQC uyumlu dijital imza algoritmalarına kaymaktadır.[49] Bu imzaların güvenilirliğini sürdürmek için düzenli sertifika yaşam döngüsü yönetimi, yani sertifika verme, iptal etme ve doğrulama süreçleri kritik öneme sahiptir.[59]

Dijital imzalar, sadece teknik kimlik doğrulamasının ötesine geçerek, özellikle zaman damgası ve PQC entegrasyonu ile dijital işlemlerin yasal geçerliliğinin ve güven zincirlerinin temel taşı haline gelmektedir. Dijital imzanın tanımı, orijinallik, bütünlük ve inkar edilemezlik özelliklerini vurgular.[59] "Geçerli bir zaman damgasına" sahip olma ifadesi [59], imzanın ne zaman atıldığını belirlediği için kritik öneme sahiptir ve temel sertifika daha sonra sona erse bile yasal bağlayıcılığını korur. PQC dijital imzalarının standartlaştırılması [49], bu bütünlük kanıtlarının kuantum bilişim çağında bile geçerliliğini korumasını sağlar. Bu, dijital imzaların yasal uyumluluk, güvenli yazılım dağıtımı ve fiziksel imzaların eskimeye başladığı bir dünyada sağlam güven zincirleri oluşturmak için giderek daha hayati hale geldiği anlamına gelir.

Gelişmiş dijital imzaların yaygın olarak benimsenmesi, yazılım tedarik zincirini güvence

altına almak, dağıtılmış yazılımın bütünlüğünü sağlamak ve kaynaktan dağıtıma kadar kötü niyetli kurcalamaları önlemek için kritik öneme sahiptir. Yazılım dağıtımı genellikle karmaşık tedarik zincirlerini içerir ve bu da onu kurcalanmaya karşı savunmasız hale getirir.[60] Yazılım paketleri ve güncellemelerindeki dijital imzalar [52], orijinal geliştiriciye doğrulanabilir bir bağlantı sağlayarak, kodun aktarım veya depolama sırasında kötü niyetli bir şekilde değiştirilmediğini garanti eder. Bu, özellikle kritik altyapı ve kurumsal sistemler için önemlidir. Yazılımın yürütülmeden önce bütünlüğünü ve kökenini doğrulama yeteneği, 2025 yılında artan bir tehdit olan tedarik zinciri saldırılarına karşı önemli bir savunmadır.[60]

6. Gizliliği Koruyan Dosya İşlemleri için Homomorfik Şifreleme (HE)

Homomorfik Şifreleme (HE), şifrelenmiş veriler üzerinde şifre çözmeye gerek kalmadan doğrudan hesaplamalar yapılmasına olanak tanıyan güçlü bir kriptografik yöntemdir.[58] Bu, hassas dosya verilerinin yaşam döngüsü boyunca, işleme veya analiz sırasında bile şifreli kalabileceği anlamına gelir ve gizliliği önemli ölçüde artırır.[65] FHE (Tam Homomorfik Şifreleme), sınırsız toplama ve çarpma işlemlerini destekleyerek bulut bilişim ve YZ uygulamalarındaki karmaşık işlemler için uygun hale gelir.[64] Hesaplama yoğunluğu yüksek olsa da, performans önemli ölçüde iyileşmiştir.[58]

HE'nin şifrelenmiş veriler üzerinde hesaplama yapma yeteneği, farklı varlıklar arasında bireysel veri gizliliğinden ödün vermeden güvenli çok taraflı hesaplama ve işbirlikçi veri analizini temelden mümkün kılar. Geleneksel olarak, birden fazla tarafın birleştirilmiş hassas veri kümelerini (örn. sağlık hizmetleri, finans) analiz etmesi için, verilerin şifresinin çözülmesi ve paylaşılması gerekirdi, bu da önemli gizlilik riskleri ve uyumluluk engelleri yaratırdı.[58] HE, şifrelenmiş veriler üzerinde doğrudan hesaplamalara izin vererek bu ihtiyacı ortadan kaldırır.[62] Bu, kuruluşların YZ modeli eğitimi veya istatistiksel analiz için şifrelenmiş verileri bir araya getirebileceği, böylece hiçbir tarafın diğerlerinden gelen ham, hassas bilgileri görmeden toplu içgörüler elde edebileceği anlamına gelir.[58] Bu, katı gizlilik düzenlemeleri olan endüstriler için çığır açıcıdır.

Gizlilik açısından sunduğu büyük faydalara rağmen, HE'nin hesaplama yükü, yaygın olarak benimsenmesinin önünde önemli bir engel olmaya devam etmekte ve verimlilik iyileştirmeleri ve özel donanım üzerine araştırmaları teşvik etmektedir. HE'de dramatik performans iyileştirmeleri görülse de (çarpma başına 30 dakikadan milisaniyelere - [64]), hala "yerel CPU tamsayı çarpma talimatlarından yedi kat daha yavaş"tır.[64] Bu "daha yavaş performans" [58], gerçek zamanlı uygulamaları ve büyük ölçekli YZ/ML iş yüklerini etkiler. Buradaki zorluk, sağlam güvenliği pratik hesaplama verimliliğiyle dengelemektir.[69] Bu, HE'nin dosya bütünlüğü doğrulamasında ana akım haline gelmesi için algoritmalar (FAS gibi - [69]) ve özel donanım hızlandırmasında [70] daha fazla

ilerlemenin kritik olduğu anlamına gelir. Odak noktası, genel bir "tek boyutlu" çözüm yerine, belirli kullanım durumları için HE'yi optimize etmek olacaktır.

7. Gizli Dosya Doğrulaması için Sıfır Bilgi İspatları (ZKP'ler)

Sıfır Bilgi İspatları (ZKP'ler), bir tarafın (kanıtlayıcı) bir sırrın bilgisine veya bir ifadenin geçerliliğine dair diğer tarafa (doğrulayıcı) sırrın kendisini veya ifadenin doğruluğunun ötesinde ek bilgi ifşa etmeden kanıtlamasına olanak tanıyan kriptografik yöntemlerdir.[63] Dosya bütünlüğü bağlamında, ZKP'ler bir dosya hakkındaki özellikleri (örn. hash'i bilinen bir değerle eşleşiyor, belirli verileri içeriyor veya bir şemaya uyuyor) dosyanın içeriğini ifşa etmeden doğrulamak için kullanılabilir.[47] NIST, ZKP'leri 2025'te standartlaştırmayı hedeflemekte, bu da onların artan önemini vurgulamaktadır.[72]

ZKP'ler, veri doğrulamasında "hepsi ya da hiç" veri paylaşımından "yeterince" bilgi ifşasına doğru bir paradigma kaymasını sağlayarak, dosya bütünlüğü doğrulamasında ayrıntılı gizlilik kontrolüne olanak tanır. Geleneksel dosya bütünlüğü kontrolleri genellikle dosyanın tamamına veya hash'ine erişim gerektirir; bu da, dosya hassas ise, özel bilgileri ifşa edebilir. ZKP'ler, bir tarafın bir dosya hakkında belirli bir özelliği (örn. "bu dosyanın hash'i X'tir" veya "bu dosya Y koşulunu karşılayan verileri içerir") dosyanın içeriğini veya hatta hash'in kendisini doğrulayıcıya ifşa etmeden kanıtlamasına olanak tanır.[72] Bu "seçici açıklama" [73], gizliliğe duyarlı uygulamalar için dönüştürücüdür ve veri ifşası olmadan bütünlük veya uyumluluk doğrulamasına olanak tanır.

ZKP'ler, veri gizliliği düzenlemelerinin (GDPR gibi) ve doğrulanabilir uyumluluk veya denetlenebilirlik ihtiyacının genellikle çelişen taleplerini uzlaştırmak için benzersiz bir çözüm sunar. GDPR gibi düzenlemeler, veri minimizasyonu ve gizliliği zorunlu kılar.[46] Aynı zamanda, işletmelerin denetimler için kayıtların uyumluluğunu veya bütünlüğünü kanıtlaması gerekir. ZKP'ler, kuruluşların kurallara uyduklarını (örn. bir kullanıcının yaşını doğruladıklarını, verileri doğru bir şekilde işlediklerini, dosya bütünlüğünü koruduklarını) denetçilere veya düzenleyicilere temel hassas verileri ifşa etmek zorunda kalmadan kriptografik olarak kanıtlamalarına olanak tanır.[47] Bu, denetimler sırasında veri ihlali riskini önemli ölçüde azaltır ve uyumluluk süreçlerini kolaylaştırır, blok zincirinin değişmezliğinde belirlenen önemli bir zorluğu ele alır.[46]

Tablo 4: Sıfır Bilgi İspatlarının Temel Özellikleri

Özellik	Tanım	Dosya Bütünlüğü Doğrulaması için Anlamı

Tamlık (Completeness)	İfade doğruysa, dürüst bir kanıtlayıcı dürüst bir doğrulayıcıyı ikna edecektir.[71]	Dosya bütünlüğü gerçekten sağlamsa, ZKP sistemi bunu her zaman doğru bir şekilde doğrulayacaktır.
Sağlamlık (Soundness)	İfade yanlışsa, hile yapan hiçbir kanıtlayıcı dürüst bir doğrulayıcıyı bunun doğru olduğuna ikna edemez.[71]	Dosya bütünlüğü tehlikeye atılmışsa, kötü niyetli bir aktör, dosyanın sağlam olduğunu iddia ederek doğrulayıcıyı kandıramaz.
Sıfır Bilgi (Zero-Knowledge)	İfade doğruysa, doğrulayıcı ifadenin geçerliliğinin ötesinde hiçbir şey öğrenmez.[71]	Doğrulayıcı, dosyanın bütünlüğünün doğruluğunu öğrenir, ancak dosyanın içeriği veya diğer hassas bilgileri hakkında hiçbir şey öğrenmez.

8. Gelişmiş Konteyner Görüntüsü ve Çalışma Zamanı Dosya Bütünlüğü

Konteynerleştirme, bulutta yerel uygulamaların temel taşıdır, ancak görüntü güvenlik açıkları, yanlış yapılandırmalar ve çalışma zamanı tehditleriyle ilgili yeni güvenlik riskleri sunar.[60] 2025 yılında, konteynerleri güvence altına almak çok yönlü bir yaklaşım gerektirmektedir:

- **Görüntü Tarama:** CI/CD işlem hattının erken aşamalarında konteyner görüntülerini güvenlik açıkları, güncel olmayan kütüphaneler ve kötü amaçlı kod için sürekli olarak taramak.[60]
- **Gizli Veri Yönetimi:** Hassas verileri (örn. API anahtarları, parolalar) korumak ve bunların görüntülere sabit kodlanmasını önlemek.[60]
- **Çalışma Zamanı İzleme:** Çalışan konteynerlerdeki tehditleri (alışılmadık dosya erişimi, beklenmedik ağ bağlantıları veya ayrıcalık yükseltme girişimleri dahil) gerçek zamanlı olarak tespit etmek ve engellemek.[60] Bu genellikle çekirdek seviyesi uygulamayı (örn. KubeArmor) içerir.[60]
- **En Az Ayrıcalık:** Konteynerlerin ve kullanıcıların yalnızca gerekli izinlere sahip olmasını sağlamak için Rol Tabanlı Erişim Kontrolü (RBAC) ve ağ politikaları uygulamak.[60]
- **İş Yükü İzolasyonu:** Tehlikeye atılmış bir konteynerin "patlama yarıçapını" sınırlamak için mikro segmentasyon kullanmak.[60]

"Erken ve sık tarama"ya yapılan vurgu [60], güvenliğin yazılım geliştirme yaşam döngüsünün (SDLC) en başından itibaren, sonradan değil, entegre edildiği daha geniş "sola kaydırma" güvenlik eğilimini yansıtmaktadır. Geleneksel geliştirmede, güvenlik

testi genellikle döngünün geç aşamalarında gerçekleşir. Konteynerler için, hızlı dağıtım döngüleri ("haftada birden fazla sürüm" - [60]) ile güvenlik açıkları erken yakalanmazsa gözden kaçabilir. Bir kusuru derleme aşamasında düzeltmek, dağıtımdan sonra ele almaktan önemli ölçüde daha kolay ve daha ucuzdur.[60] Bu, güvenlik sorumluluklarını geliştirme hattının daha erken bir aşamasına iter, geliştiricileri konteyner güvenliğinin ayrılmaz bir parçası haline getirir ve görüntü oluşturmadan itibaren dosya bütünlüğünü sağlar.

Konteyner ortamlarının dinamik ve geçici doğası [78], geleneksel dosya bütünlüğü izleme araçları için benzersiz zorluklar sunmakta ve özel çalışma zamanı koruması ve gözlemlenebilirliği gerektirmektedir. Konteynerler kısa ömürlü ve oldukça dinamik olacak şekilde tasarlanmıştır.[78] Geleneksel FIM araçları, bu kadar hızlı sağlanan ve kaldırılan ortamlardaki değişiklikleri izlemekte zorlanabilir. Bu durum, konteynerin kısa ömrü ne olursa olsun, konteyner davranışını sürekli olarak izleyebilen ve gerçek zamanlı korumalar uygulayabilen konteyner çalışma zamanı güvenlik araçlarını gerektirir.[78] Ayrıca, uyumluluk ve adli tıp için konteyner içindeki her sistem etkileşimi, ağ bağlantısı ve dosya erişimi için ayrıntılı denetim günlükleri gerektirir [78], basit dosya hash'lerinin ötesine geçerek davranışsal telemetriye odaklanır.

Tablo 5: Konteyner Güvenliği için En İyi Uygulamalar (2025)

En İyi Uygulama	Açıklama	Dosya Bütünlüğü için Önemi
Erken ve Sık Tarama	Güvenlik açıklarını, güncel olmayan kütüphaneleri ve kötü amaçlı kodları CI/CD işlem hattının erken aşamalarında sürekli olarak tarayın.[60]	Güvenlik sorunlarının dağıtımdan önce tespit edilmesini ve düzeltilmesini sağlar, kötü niyetli kodun veya yanlış yapılandırmaların dosya sistemine girmesini önler.
Erişimi ve Ayrıcalıkları En Aza İndirme	Konteynerlerin ve kullanıcıların yalnızca görevlerini yerine getirmek için kesinlikle ihtiyaç duydukları erişime sahip olmasını sağlamak için en az ayrıcalık ilkesini uygulayın.[60]	Bir konteynerin tehlikeye atılması durumunda yetkisiz dosya değişiklikleri veya veri sızdırması riskini azaltır.
Çalışma Zamanı Davranışını İzleme	Çalışan konteynerlerde şüpheli davranışları (alışılmadık dosya erişimi,	Çalışma zamanında dosya bütünlüğüne yönelik tehditleri (örn. fidye yazılımı, kök kitler)

	beklenmedik ağ bağlantıları, ayrıcalık yükseltme girişimleri gibi) gerçek zamanlı olarak tespit edin ve engelleyin.[60]	anında tespit eder ve yanıt verir.
İş Yüklerini İzole Etme	Tehlikeye atılmış bir konteynerin "patlama yarıçapını" sınırlamak için ağ segmentasyonu ve mikro segmentasyon kullanın.[60]	Bir saldırının dosya sisteminin diğer bölümlerine veya diğer konteynerlere yayılmasını önleyerek, dosya bütünlüğü ihlallerinin etkisini sınırlar.
Güvenli Gizli Veri Yönetimi	Hassas verileri (örn. API anahtarları, parolalar) koruyun ve bunların konteyner görüntülerine sabit kodlanmasını önleyin; bunun yerine özel gizli veri yönetim hizmetlerini kullanın.[60]	Yetkisiz kişilerin hassas dosyalara veya yapılandırmalara erişmek için kimlik bilgilerini kullanmasını önleyerek dosya bütünlüğünü korur.

9. Sunucusuz Mimarilerde Güvenli Dosya Bütünlüğü

Geliştiricilerin temel altyapıyı yönetme endişesi duymadan yalnızca kod fonksiyonlarına odaklandığı sunucusuz bilişim, durum bilgisi olmayan, geçici ve dağıtılmış yapısı nedeniyle benzersiz dosya bütünlüğü zorlukları sunar.[79] Geleneksel izleme araçları, bu kısa ömürlü fonksiyonlar için genellikle yetersiz kalır.[79] 2025'te sunucusuz ortamlarda dosya bütünlüğünü sağlamak için en iyi uygulamalar şunları içerir:

- **Kod Koruması:** Birincil saldırı yüzeyi olduğu için fonksiyon kodunun kendisini güvence altına almaya odaklanmak.[79]
- **Girdi Doğrulaması:** Kötü amaçlı kod enjeksiyonunu veya yetkisiz erişimi önlemek için tüm girdileri titizlikle doğrulamak.[77]
- **Fonksiyonlar için En Az Ayrıcalık:** Sunucusuz fonksiyonlara görevlerini yerine getirmek için yalnızca minimum gerekli izinleri vermek.[77]
- **Gelişmiş Günlük Kaydı ve İzleme:** Şüpheli etkinlikler hakkında gerçek zamanlı uyarılar ve geleneksel araçların genellikle kaçırdığı API çağrılarını izlemek için özel araçlar kullanmak.[77]
- **Bağımlılık Yönetimi:** Güvenlik açıklarını azaltmak için üçüncü taraf kütüphaneleri ve SDK'ları düzenli olarak taramak ve güncellemek.[77]

Sunucusuz mimaride, güvenliğin geleneksel ağ çevresi daha az alakalı hale gelir; odak noktası, bireysel fonksiyon kodunu, yapılandırmalarını ve etkileşimlerini güvence altına almaya kayar. Sunucusuz, sunucuları ve ağları soyutlar.[79] Bu, güvenlik duvarları gibi

geleneksel çevre savunmalarının "dosyaların" (kod fonksiyonları) kendilerini korumada daha az etkili olduğu anlamına gelir. Güvenlik çevresi, kodun kendisine, yapılandırmasına (izinler, zaman aşımları) ve işlediği verilere etkin bir şekilde kayar.[77] Bu, her fonksiyon için güvenli kodlama uygulamalarına, titiz girdi doğrulamasına ve ayrıntılı erişim kontrolüne güçlü bir vurgu yapılmasını gerektirir, çünkü bunlar bütünlüğünün korunması gereken yeni "dosyalardır".

Sunucusuz fonksiyonların dağıtılmış ve geçici doğası, kapsamlı izleme ve hata ayıklamayı karmaşık hale getirerek, dosya bütünlüğü görünürlüğünü sürdürmek için özel araçlar ve stratejiler gerektirir. Sunucusuz fonksiyonlar kısa ömürlüdür ve talep üzerine, genellikle dağıtılmış altyapı üzerinde yürütülür.[79] Bu, "dosyaların" (fonksiyon kodu, geçici depolama) durumunu izlemeyi ve geleneksel izleme araçlarını kullanarak anomalileri tespit etmeyi zorlaştırır.[79] "Soğuk başlangıç" gecikmesi [79] de dinamik doğaya işaret eder. Bu durum, şüpheli etkinlikler için gelişmiş günlük kaydı, gerçek zamanlı uyarılar ve dağıtılmış fonksiyonlar arasında API çağrılarını ve kullanıcı davranışını izleyebilen özel araçları gerektirir.[77] Böyle bir ortamda dosya bütünlüğünü sürdürmek, birçok geçici bileşen arasında olayları ilişkilendirebilen sağlam bir gözlemlenebilirlik stratejisi gerektirir.

10. Dosya Bütünlüğü için Otomatik Uyumluluk ve Politika Uygulaması

Dosya Bütünlüğü İzleme (FIM) çözümleri, kuruluşların GDPR, HIPAA, PCI-DSS ve SOX gibi katı düzenleyici gerekliliklere uyumu göstermeleri için giderek daha önemli hale gelmektedir.[2] FIM araçlarındaki otomatik uyumluluk özellikleri, dosya değişiklikleri, kullanıcı etkinlikleri ve erişim kalıpları hakkında sürekli denetim, gerçek zamanlı risk değerlendirmeleri ve ayrıntılı raporların oluşturulmasını sağlar.[9] Bu, kuruluşları reaktif, manuel bir uyumluluk yaklaşımından proaktif, otomatik bir yaklaşıma doğru kaydırarak manuel hataları önemli ölçüde azaltır ve zaman kazandırır.[21]

FIM'in rolü, sadece güvenlik aracının ötesine geçerek, veri bütünlüğü ve erişim kontrolünün denetlenebilir kanıtını sağlayarak düzenleyici uyumluluk için kritik bir kolaylaştırıcı haline gelmektedir. GDPR ve HIPAA gibi düzenlemeler, veri koruma ve bütünlüğü için belirli önlemler zorunlu kılar.[2] FIM, dosya değişikliklerini sürekli olarak izleyerek ve kaydederek denetimler için gerekli kanıtları sağlar.[3] "Değişikliği kimin yaptığı ve kullanılan süreç" bilgisini takip etme yeteneği [3], hesap verebilirliği ve erişim kontrol politikalarına uyumu göstermekle doğrudan ilgilidir. Bu, FIM'in artık sadece bir güvenlik aracı değil, yasal ve endüstri standartlarını karşılamak için doğrulanabilir veriler sağlayan bir uyumluluk aracı olduğu anlamına gelir.

FIM'in otomatik uyumluluk araçları ve SIEM sistemleriyle entegrasyonu, seyrek, anlık denetimlerden sürekli, gerçek zamanlı uyumluluk izlemeye geçişi kolaylaştırmaktadır.

Geleneksel uyumluluk denetimleri genellikle periyodiktir ve uyumsuz değişikliklerin tespit edilmeden gerçekleşebileceği boşluklar bırakır. Otomatik FIM, özellikle SIEM [9] ve uyumluluk otomasyon platformlarıyla [80] entegre edildiğinde, politika uyumunun gerçek zamanlı olarak izlenmesine olanak tanır. Bu, uyumlu bir temelden herhangi bir sapmanın (örn. yapılandırma dosyalarında yetkisiz değişiklikler, hassas verilere alışılmadık erişim kalıpları) anında uyarıları ve otomatik düzeltmeyi tetikleyebileceği anlamına gelir, böylece düzenleyici gerekliliklere sürekli uyum sağlanır.[21] Bu proaktif duruş, uyumluluk riskini ve manuel raporlama yükünü önemli ölçüde azaltır.

IV. 2025 için Kapsamlı Değerlendirmeler

Çeşitli Sistemler Arasında Birlikte Çalışabilirlik ve Entegrasyon Zorlukları

Bu gelişmiş tekniklerin benimsenmesi, genellikle farklı sistemlerin ve teknolojilerin (örn. FIM'in SIEM/EDR ile, blok zincirinin geleneksel veritabanlarıyla, PQC'nin eski PKI ile) entegrasyonunu içerir. Bu durum, sorunsuz iletişim ve veri akışı sağlamak için açık standartlar, sağlam API'ler ve dikkatli mimari planlama gerektiren önemli birlikte çalışabilirlik zorlukları sunar.[16] Örneğin, PQC'ye geçiş, mevcut protokollere sorunsuz entegrasyonu sağlamak için karmaşık bir süreçtir.[48]

Gelişmiş Kriptografik Tekniklerin Performans ve Kaynak Yükü

FHE ve PQC gibi teknolojiler sağlam güvenlik sunarken, genellikle artan hesaplama ve bellek gereksinimleriyle birlikte gelir.[50] Bu yük, özellikle IoT cihazları veya gerçek zamanlı sistemler gibi kaynak kısıtlı ortamlarda dikkatli bir şekilde yönetilmelidir; bu da optimizasyon, donanım hızlandırma ve dikkatli parametre seçimi gerektirir.[50] Örneğin, FHE'deki çarpma işlemleri hala yerel CPU talimatlarından önemli ölçüde daha yavaştır.[64]

Beceri Açıklarını Giderme ve İş Gücü Eğitimi İhtiyacı

Yeni kriptografik yöntemlerin, YZ/ML modellerinin ve blok zinciri uygulamalarının karmaşıklığı, özel bilgi ve uzmanlık gerektirir.[50] Birçok işletme şu anda gerekli becerilere sahip değildir, bu da BT ve güvenlik ekiplerinin bu gelişmiş kavramlar ve en iyi uygulamalar konusunda yeteneklerini geliştirmeleri için kritik bir ihtiyacı vurgulamaktadır.[48] PQC'ye geçiş, güvenlik profesyonellerinin özel eğitim almasını ve uyum yeteneklerini artırmasını gerektirmektedir.[50]

Etik ve Yasal Sonuçlar

YZ/ML, blok zinciri, HE ve ZKP'leri içeren gelişmiş dosya bütünlüğü çözümlerinin uygulanması, önemli etik ve yasal soruları gündeme getirmektedir. Bunlar arasında veri gizliliği endişeleri (örn. blok zinciri değişmezliği ile GDPR uyumluluğu), yeni bütünlük

kanıtlarının yasal kabul edilebilirliği ve kullanıcı etkinlikleri kaydedilirken veya analiz edilirken bilgilendirilmiş onam ihtiyacı yer almaktadır.[42] Örneğin, blok zincirinin değişmez mimarisi, GDPR'ın veri silme ve değiştirme ile ilgili maddeleri açısından benzersiz zorluklar ortaya koymaktadır.[46]

V. Uygulama ve Geleceğe Hazırlık için Öneriler

Kuruluşlar, gelişmiş dosya bütünlüğü tekniklerinin uygulanması için risk tabanlı bir yaklaşım benimsemeli, kritik sistemleri ve hassas verileri önceliklendirmelidir.[48] Bu, kriptografik varlıkların envanterini çıkarmayı, mevcut güvenlik açıklarının etkisini değerlendirmeyi ve aşamalı bir geçiş stratejisi geliştirmeyi içerir.[48]

Acil etki için, YZ/ML anomali tespiti ile gerçek zamanlı FIM, kritik sistemler için önceliklendirilmelidir. Kuantum tehditlerine karşı geleceğe hazırlık için, NIST tarafından standartlaştırılmış PQC algoritmalarına aşamalı bir geçiş esastır.[48] Blok zinciri ve gizliliği koruyan teknikler (HE, ZKP), değişmez köken veya gizli veri paylaşımı gerektiren belirli kullanım durumları için, mevcut performans yükleri ve uyumluluk karmaşıklıkları dikkate alınarak araştırılmalıdır.

Gelişen tehdit ortamı, sürekli izleme ve uyarlanabilir güvenlik duruşlarını zorunlu kılmaktadır. Kuruluşlar, geleneksel güvenlik kontrollerini gelişmiş tekniklerle birleştiren hibrit yaklaşımları benimsemeli ve yeni tehditlere ve güvenlik açıklarına karşı koymak için sistemlerini ve politikalarını sürekli olarak güncellemelidir.[1] Düzenli güvenlik denetimleri ve endüstri konsorsiyumlarıyla etkileşim de kritik öneme sahiptir.[48]

VI. Sonuç

Dosya bütünlüğü alanı, dijital varlıkları giderek daha karmaşık hale gelen siber tehditlere karşı koruma zorunluluğuyla derin bir dönüşüm geçirmektedir. YZ odaklı gerçek zamanlı izleme ve blok zincirinin değişmezliğinden kuantum dirençli kriptografiye ve gizliliği koruyan ispatlara kadar tartışılan gelişmiş teknikler ve eğilimler, veri güvenilirliğini sağlamak için benzeri görülmemiş yetenekler sunmaktadır.

2025 yılında dijital güveni sürdürmek, dosya bütünlüğüne çok katmanlı, uyarlanabilir ve akıllı bir yaklaşıma bağlıdır. Bu, yalnızca teknolojik benimsemeyi değil, aynı zamanda stratejik planlamayı, insan sermayesine yatırımı ve veri güvenliğinin gelişen yasal ve etik boyutlarına ilişkin keskin bir farkındalığı da gerektirmektedir. Bu son teknoloji teknikleri benimseyerek, kuruluşlar bilgiyi koruyan, operasyonel sürekliliği sağlayan ve dijital alanda kamu güvenini koruyan dayanıklı dijital altyapılar inşa edebilirler.

Alıntılanan çalışmalar

1. Siber Güvenlik Nedir ve Neden Bu Kadar Önemlidir? - Zayıf Akım, erişim tarihi Haziran 5, 2025, https://zayifakim.com/siber-guvenlik-nedir-ve-neden-bu-kadar-onemlidir.html
2. Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) - KVKK, erişim tarihi Haziran 5, 2025, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf
3. File Integrity Monitoring Global Market Report 2025 - GII Research, erişim tarihi Haziran 5, 2025, https://www.giiresearch.com/report/tbrc1704345-file-integrity-monitoring-global-market-report.html
4. File Integrity Monitoring Market Size, Statistics Report 2025-2034, erişim tarihi Haziran 5, 2025, https://www.gminsights.com/industry-analysis/file-integrity-monitoring-market
5. MD5 vs SHA3-256 - A Comprehensive Comparison - MojoAuth, erişim tarihi Haziran 5, 2025, https://mojoauth.com/compare-hashing-algorithms/md5-vs-sha3-256
6. MD5 vs SHA1 vs SHA2 vs SHA3 - Compare Hashing Algorithms - SignMyCode, erişim tarihi Haziran 5, 2025, https://signmycode.com/blog/md5-vs-sha1-vs-sha2-vs-sha3
7. Winrar crc hatası düzeltilir mi - DonanımHaber Forum, erişim tarihi Haziran 5, 2025, https://forum.donanimhaber.com/winrar-crc-hatasi-duzeltilir-mi--72187267
8. CRC Artıklık Denetimini Anlamak: Yeni Başlayanlar İçin Veri Bütünlüğü - Wray Castle, erişim tarihi Haziran 5, 2025, https://wraycastle.com/tr/blogs/bilgi-tabani/crc-redundancy-check
9. Top File Integrity Monitoring Software in 2025 - Slashdot, erişim tarihi Haziran 5, 2025, https://slashdot.org/software/file-integrity-monitoring/
10. Top File Integrity Monitoring Software for Enterprise in 2025 - Slashdot, erişim tarihi Haziran 5, 2025, https://slashdot.org/software/file-integrity-monitoring/f-enterprise/
11. The Definitive Guide to File Integrity Monitoring - Wallarm, erişim tarihi Haziran 5, 2025, https://www.wallarm.com/what/file-integrity-monitoring
12. Enabling Real-time File Integrity Monitoring in Intrusion Detection for Agents, erişim tarihi Haziran 5, 2025, https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/data-center-security-(dcs)/6-10/configuring-features-through-console/about-policies-v127947623-d3608e175973/creating-a-detection-configuration-v95156843-d3608e14539/enabling-the-real-time-file-integrity-monitoring-f-v127947548-d3608e175301.html
13. LKIM: The Linux Kernel Integrity Measurer - Johns Hopkins University Applied Physics Laboratory, erişim tarihi Haziran 5, 2025, https://www.jhuapl.edu/Content/techdigest/pdf/V32-N02/32-02-Pendergrass-McGill.pdf
14. File Integrity Monitoring - osquery - Read the Docs, erişim tarihi Haziran 5, 2025, https://osquery.readthedocs.io/en/stable/deployment/file-integrity-monitoring/

15. File Integrity Checker (Monitor) – IJERT, erişim tarihi Haziran 5, 2025, https://www.ijert.org/file-integrity-checker-monitor
16. Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions, erişim tarihi Haziran 5, 2025, https://www.scirp.org/journal/paperinformation?paperid=134347
17. Best File Integrity Monitoring Software 2025 | TrustRadius, erişim tarihi Haziran 5, 2025, https://www.trustradius.com/categories/file-integrity-monitoring
18. Yapay Zeka ve Makine Öğrenimi ile Güvenlik Tehditlerini Tespit Etmek - Secure Fors, erişim tarihi Haziran 5, 2025, https://www.securefors.com/yapay-zeka-ile-guvenlik-acikliklarini-tespit-etmek/
19. Full article: Current trends in AI and ML for cybersecurity: A state-of-the-art survey, erişim tarihi Haziran 5, 2025, https://www.tandfonline.com/doi/full/10.1080/23311916.2023.2272358
20. Integrating Machine Learning and Behavioral Analytics for Next-Gen Cyber Threat Prediction and Mitigation - ResearchGate, erişim tarihi Haziran 5, 2025, https://www.researchgate.net/publication/390897384_Integrating_Machine_Learning_and_Behavioral_Analytics_for_Next-Gen_Cyber_Threat_Prediction_and_Mitigation
21. Open Source UEBA Tools & Commercial Alternatives in 2025 - Research AIMultiple, erişim tarihi Haziran 5, 2025, https://research.aimultiple.com/open-source-ueba/
22. AI-powered threat detection: Zscaler's defense against cyberattacks - SiliconANGLE, erişim tarihi Haziran 5, 2025, https://siliconangle.com/2025/05/01/ai-powered-threat-detection-zscaler-fighting-next-gen-cyberattacks-rsac/
23. ITDR: Mastering Identity Threat Detection and Response in 2025 - DoControl, erişim tarihi Haziran 5, 2025, https://www.docontrol.io/blog/itdr-mastering-identity-threat-detection-and-response-in-2025
24. AI-Driven Anomaly Detection in Cybersecurity - RIT Digital Institutional Repository, erişim tarihi Haziran 5, 2025, https://repository.rit.edu/cgi/viewcontent.cgi?article=13138&context=theses
25. "AI-Driven Anomaly Detection in Cybersecurity" by Mohamed Almansoori, erişim tarihi Haziran 5, 2025, https://repository.rit.edu/theses/12015/
26. Introduction to Anomaly Detection with Python - GeeksforGeeks, erişim tarihi Haziran 5, 2025, https://www.geeksforgeeks.org/introduction-to-anomaly-detection-with-python/?ref=oin_asr5
27. The File Integrity Monitoring (FIM) System continuously monitors multiple directories for unauthorized changes, ensuring data integrity and security. It logs modifications, detects anomalies using AI, and provides alerts for suspicious activities. - GitHub, erişim tarihi Haziran 5, 2025, https://github.com/AdityaPatadiya/File-Integrity-Monitor-FIM
28. What are open-source libraries for anomaly detection? - Milvus, erişim tarihi Haziran 5, 2025,

https://milvus.io/ai-quick-reference/what-are-opensource-libraries-for-anomaly-detection
29. Anomaly Detection in Machine Learning Using Python | The PyCharm Blog, erişim tarihi Haziran 5, 2025, https://blog.jetbrains.com/pycharm/2025/01/anomaly-detection-in-machine-learning/
30. En Önemli 16 Cloud Güvenliği Sorunu - Riskler, Tehditler, Zorluklar - OPSWAT, erişim tarihi Haziran 5, 2025, https://turkish.opswat.com/blog/top-cloud-security-issues-risks-threats-and-challenges
31. Conference Themes - ICACSDF2025, erişim tarihi Haziran 5, 2025, https://www.icacsdf.org/theme.html
32. Mastering File System Monitoring with Watchdog in Python - DEV Community, erişim tarihi Haziran 5, 2025, https://dev.to/devasservice/mastering-file-system-monitoring-with-watchdog-in-python-483c
33. da4nyy/ANTIVIRUSxML: File integrity monitor with malware detection using machine learning - GitHub, erişim tarihi Haziran 5, 2025, https://github.com/da4nyy/ANTIVIRUSxML
34. Top 10 Python Libraries For Cybersecurity | GeeksforGeeks, erişim tarihi Haziran 5, 2025, https://www.geeksforgeeks.org/top-10-python-libraries-for-cybersecurity/
35. Hashing and Validation of Grøstl in Python Implementation - MojoAuth, erişim tarihi Haziran 5, 2025, https://mojoauth.com/hashing/grstl-in-python
36. BLOKZİNCİR UYGULAMASINDA KİŞİSEL VERİLERİN TUTULMASI - Akademik Veri Yönetim Sistemi, erişim tarihi Haziran 5, 2025, https://avesis.marmara.edu.tr/dosya?id=00614607-a519-4f57-b2de-a82dd73bd0b6
37. Kripto Sözlüğü | Tangem, erişim tarihi Haziran 5, 2025, https://tangem.com/tr/glossary/
38. 13 V May 2025 https://doi.org/10.22214/ijraset.2025.70255, erişim tarihi Haziran 5, 2025, https://www.ijraset.com/best-journal/blockchain-solution-for-document-integrity-and-forgery-mitigation
39. Blockchain ensuring academic integrity with a degree verification prototype - PMC, erişim tarihi Haziran 5, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11920411/
40. Secure Access Control and Certificate Validation Using Blockchain and Python, erişim tarihi Haziran 5, 2025, https://ijsred.com/volume8/issue3/IJSRED-V8I3P9.pdf
41. Blockchain-Enabled Supply Chain Management: A Review of Security, Traceability, and Data Integrity Amid the Evolving Systemic Demand - MDPI, erişim tarihi Haziran 5, 2025, https://www.mdpi.com/2076-3417/15/9/5168
42. A Framework for Blockchain-Based Access Logs and Tamper-Proof Audit Trails, erişim tarihi Haziran 5, 2025, https://www.researchgate.net/publication/392312120_A_Framework_for_Blockcha

in-Based_Access_Logs_and_Tamper-Proof_Audit_Trails
43. Decentralized and Secure Blockchain Solution for Tamper-Proof Logging Events, erişim tarihi Haziran 5, 2025, https://ideas.repec.org/a/gam/jftint/v17y2025i3p108-d1603190.html
44. Data Integrity - WEF Blockchain Toolkit, erişim tarihi Haziran 5, 2025, https://widgets.weforum.org/blockchain-toolkit/data-integrity/index.html
45. Blockchain for High Performance Data Integrity and Provenance - OSTI, erişim tarihi Haziran 5, 2025, https://www.osti.gov/servlets/purl/1497843
46. Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways | Journal of Cybersecurity | Oxford Academic, erişim tarihi Haziran 5, 2025, https://academic.oup.com/cybersecurity/article/11/1/tyaf002/8024082
47. A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System, erişim tarihi Haziran 5, 2025, https://www.mdpi.com/1424-8220/25/11/3450
48. NIST PQ Standards 2025: What's Finalised - OnlineHashCrack, erişim tarihi Haziran 5, 2025, https://www.onlinehashcrack.com/guides/post-quantum-crypto/nist-pq-standards-2025-what-s-finalised.php
49. NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption, erişim tarihi Haziran 5, 2025, https://thequantuminsider.com/2025/03/11/nist-selects-hqc-as-fifth-algorithm-for-post-quantum-encryption/
50. Industry News 2025 Post Quantum Cryptography A Call to Action - ISACA, erişim tarihi Haziran 5, 2025, https://www.isaca.org/resources/news-and-trends/industry-news/2025/post-quantum-cryptography-a-call-to-action
51. What Is Quantum-Resistant Cryptography? Explained for 2025 - Cloudwards.net, erişim tarihi Haziran 5, 2025, https://www.cloudwards.net/quantum-resistant-cryptography/
52. 2024-2025 CRA Quad Paper: The Post-Quantum Cryptography Transition: Making Progress, But Still a Long Road Ahead - Computing Research Association, erişim tarihi Haziran 5, 2025, https://cra.org/wp-content/uploads/2025/01/2024-2025-CRA-Quad-Paper_-The-Post-Quantum-Cryptography-Transition_-Making-Progress-But-Still-a-Long-Road-Ahead.pdf
53. Research on Development Progress and Test Evaluation of Post-Quantum Cryptography, erişim tarihi Haziran 5, 2025, https://www.mdpi.com/1099-4300/27/2/212
54. NIST advances post-quantum cryptography standardization, selects HQC algorithm to counter quantum threats - Industrial Cyber, erişim tarihi Haziran 5, 2025, https://industrialcyber.co/nist/nist-advances-post-quantum-cryptography-standardization-selects-hqc-algorithm-to-counter-quantum-threats/
55. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography

Standardization Process, erişim tarihi Haziran 5, 2025, https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process
56. Selected Algorithms - Post-Quantum Cryptography | CSRC, erişim tarihi Haziran 5, 2025, https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms
57. PQC Benchmark 2025: Kyber vs BIKE vs HQC - OnlineHashCrack, erişim tarihi Haziran 5, 2025, https://www.onlinehashcrack.com/guides/post-quantum-crypto/pqc-benchmark-2025-kyber-vs-bike-vs-hqc.php
58. Moving Beyond Traditional Data Protection: Homomorphic Encryption Could Provide What is Needed for Artificial Intelligence - Journal of AHIMA, erişim tarihi Haziran 5, 2025, https://journal.ahima.org/page/moving-beyond-traditional-data-protection-homomorphic-encryption-could-provide-what-is-needed-for-artificial-intelligence
59. Microsoft 365 dosyaları için dijital imza ekleme veya kaldırma, erişim tarihi Haziran 5, 2025, https://support.microsoft.com/tr-tr/office/microsoft-365-dosyalar%C4%B1-i%C3%A7in-dijital-imza-ekleme-veya-kald%C4%B1rma-70d26dc9-be10-46f1-8efa-719c8b3f1a2d
60. Container Security And How To Secure Containers In 2025 - AccuKnox, erişim tarihi Haziran 5, 2025, https://accuknox.com/blog/container-security
61. The Container Security Best Practices You Need To Be Using in 2025 - SUSE, erişim tarihi Haziran 5, 2025, https://www.suse.com/c/container-security-best-practices/
62. Mathematical Proposal for Securing Split Learning Using Homomorphic Encryption and Zero-Knowledge Proofs - MDPI, erişim tarihi Haziran 5, 2025, https://www.mdpi.com/2076-3417/15/6/2913
63. Advanced Cryptography - NCSC.GOV.UK, erişim tarihi Haziran 5, 2025, https://www.ncsc.gov.uk/whitepaper/advanced-cryptography
64. Pyfhel: PYthon for Homomorphic Encryption Libraries - Research Collection, erişim tarihi Haziran 5, 2025, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/522339/pyfhel.pdf?sequence=3&isAllowed=y
65. Homomorphic Encryption: Definition, Types, Use Cases - phoenixNAP, erişim tarihi Haziran 5, 2025, https://phoenixnap.com/kb/homomorphic-encryption
66. Security Guidelines for Implementing Homomorphic Encryption - Cryptology ePrint Archive, erişim tarihi Haziran 5, 2025, https://eprint.iacr.org/2024/463.pdf
67. Privacy Preservation in Federated Market Basket Analysis using Homomorphic Encryption, erişim tarihi Haziran 5, 2025, https://aclanthology.org/2024.nlpaics-1.13/
68. Privacy-Enhancing and Privacy- Preserving Technologies in AI: - Centre for Information Policy Leadership, erişim tarihi Haziran 5, 2025, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_pets_and_ppts_in_ai_mar25.pdf

69. A Selective Homomorphic Encryption Approach for Faster Privacy-Preserving Federated Learning - arXiv, erişim tarihi Haziran 5, 2025, https://arxiv.org/html/2501.12911v1
70. intel/pailliercryptolib_python: Intel Paillier Cryptosystem Library is an open-source library which provides accelerated performance of a partial homomorphic encryption (HE), named Paillier cryptosystem, by utilizing Intel® IPP-Crypto technologies on Intel CPUs supporting the AVX512IFMA instructions. The library is written in modern standard C++ and provides the essential API for - GitHub, erişim tarihi Haziran 5, 2025, https://github.com/intel/pailliercryptolib_python
71. Zero-Knowledge Proof Frameworks: A Survey - arXiv, erişim tarihi Haziran 5, 2025, https://arxiv.org/html/2502.07063v1
72. Why Zero-Knowledge Proofs Are the Future of Blockchain Security | Built In, erişim tarihi Haziran 5, 2025, https://builtin.com/articles/zero-knowledge-proof-blockchain-security
73. Zero-Knowledge Proofs: A Beginner's Guide - Dock Labs, erişim tarihi Haziran 5, 2025, https://www.dock.io/post/zero-knowledge-proofs
74. Zero-Knowledge Proof Frameworks: A Systematic Survey - arXiv, erişim tarihi Haziran 5, 2025, https://arxiv.org/pdf/2502.07063
75. Zero-Knowledge Proof (ZKP) Python Implementation - GitHub, erişim tarihi Haziran 5, 2025, https://github.com/codeesura/Zero-Knowledge-Proof-Python-Implementation
76. Zero Knowledge Proof Identity Management - IAM Concept, erişim tarihi Haziran 5, 2025, https://identitymanagementinstitute.org/zero-knowledge-proof-identity-management/
77. Serverless Security Pitfalls: A 2025 Checklist | sanj.dev, erişim tarihi Haziran 5, 2025, https://sanj.dev/post/serverless-security-pitfalls-2025
78. Top 10 Container Runtime Security Tools for 2025 - SentinelOne, erişim tarihi Haziran 5, 2025, https://www.sentinelone.com/cybersecurity-101/cloud-security/container-runtime-security-tools/
79. Serverless Computing in 2025: Complete Guide & Best Practices - BuzzClan, erişim tarihi Haziran 5, 2025, https://buzzclan.com/cloud/serverless-computing/
80. Identity Verification Trends to Watch in 2025: The Future of Secure Onboarding, erişim tarihi Haziran 5, 2025, https://www.idenfodirect.com/articles/identity-verification-trends-to-watch-in-2025-the-future-of-secure-onboarding/
81. Decentralized Identity: The Ultimate Guide 2025 - Dock Labs, erişim tarihi Haziran 5, 2025, https://www.dock.io/post/decentralized-identity