Güvenli Veri Depolama

Hira Beril KÜÇÜK
AISECLAB
(Artificial Intelligence Security & Defense Lab)
aiseclab.org

Güvenli Veri depolama, yöntemler, teknikler ve algoritmalar konusunda derleme içermektedir.

I. GÜVENLİ VERİ DEPOLAMA

Güvenli veri depolama, verilerin yetkisiz erişim, değiştirme veya kaybolma riskine karşı korunduğu bir depolama yöntemidir. Verilerin güvenli bir şekilde depolanması, gizlilik, bütünlük ve erişilebilirlik gibi önemli hususları kapsamaktadır. Güvenli veri depolama amacıyla veri şifreleme, erişim kontrolü, yedekleme ve geri dönme, fiziksel güvenliği sağlamak gibi önemler alınabilmektedir.

II. ŞİFRELEME TABANLI VERİ DEPOLAMA

Şifreli depolama olarak da bilinen şifreleme tabanlı depolama, verileri depolanmadan önce şifreleyerek ve erişildiğinde veya alındığında şifresini çözerek güvenli bir şekilde depolama yöntemini ifade eder. Yöntemin amacı, saklanan verilerin gizliliğini ve bütünlüğünü korumak, yalnızca yetkili kişilerin veya sistemlerin verilere erişebilmesini ve okuyabilmesini sağlamaktır. Şifreleme tabanlı depolama, şifreleme anahtarlarını kullanarak verileri şifreli metin olarak bilinen okunamaz bir forma dönüştürmek için şifreleme algoritmalarına dayanır. Simetrik ve Asimetrik şifreleme olmak üzere iki temel şifreleme algoritması vardır. Simetrik şifreleme, verileri hem şifrelemek hem de şifresini çözmek için tek bir anahtar kullanır. AES (Gelişmiş Şifreleme Standardı) ve 3DES (Üçlü Veri Şifreleme Standardı) gibi algoritmalar, simetrik şifreleme için yaygın olarak kullanılır. Aynı anahtar hem şifreleme hem de şifre çözme için kullanıldığından anahtar güvenli tutulmalı ve yalnızca yetkili taraflarca bilinmelidir. Açık anahtarlı şifreleme olarak da bilinen asimetrik şifrelemede şifreleme için bir genel anahtar ve şifre çözme için bir özel anahtar olmak üzere bir çift anahtar kullanır. Bu yöntemde genel anahtar serbestçe dağıtılabilirken, özel anahtar gizli tutulmalıdır. RSA (Rivest-Shamir-Adleman) ve ECC (Elliptic Curve Cryptography) yaygın olarak kullanılan asimetrik şifreleme algoritmalarıdır. Şifreleme tabanlı depolama, hassas verileri korumak için sağlam bir güvenlik katmanı sağlar. Güvenli dosya depolama, veritabanı şifreleme, bulut depolama şifreleme ve tam disk şifreleme gibi çeşitli uygulamalarda yaygın olarak kullanılır. Ancak, şifrelemeye dayalı depolamanın kapsamlı bir güvenlik stratejisinin yalnızca bir yönü olduğunu ve verilerin genel olarak korunmasını sağlamak için diğer güvenlik önlemleriyle birleştirilmesi gerektiğini unutmamak önemlidir.

III. GÜVENLİ VERİ DEPOLAMA ALGORİTMALARI

Saklanan verilerin güvenliğini sağlamak için özel olarak tasarlanmış kriptografik algoritmalar, depolama boyunca verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumayı amaçlar. Yaygın olarak kullanılan güvenli veri depolama algoritmalarından bazıları; AES, RSA, 3DES, Blowfish, SHA olarak verilebilir.

AES (Gelişmiş Şifreleme Standardı) hassas bilgilerin güvenliğini sağlamak için ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından onaylanan simetrik bir şifreleme algoritmasıdır. Veri blokları üzerinde çalışan algoritma 128, 192 ve 256 bitlik anahtar boyutlarını desteklemektedir. AES, verimliliği, çok yönlülüğü ve çeşitli kriptografik saldırılara karşı direncinden dolayı güvenli veri depolama amacıyla yaygın olarak kullanılmaktadır.

RSA (Rivest-Shamir-Adleman), şifreleme ve şifre çözme için büyük asal sayıların matematiksel özelliklerine dayanan, güvenli anahtar yönetimi ve veri depolama için yaygın olarak kullanılan asimetrik bir şifreleme algoritmasıdır. RSA, şifreleme için bir genel anahtar ve şifre çözme için bir özel anahtar kullanır. RSA, şifreleme anahtarlarını şifrelemek ve korumak veya güvenli iletişim kanalları oluşturmak için kullanılmaktadır.

3DES (Üçlü Veri Şifreleme Standardı), bir şifre blok zincirleme (CBC) modunda veri Şifreleme Standardı (DES) algoritmasını üç kez uygulayan simetrik bir şifreleme algoritmasıdır. Üç adet 56 bitlik alt anahtardan oluşan 168 bitlik bir anahtar kullanmaktadır. 3DES, DES ile geriye dönük uyumluluğun gerekli olduğu eski sistemlerde yaygın olarak kullanılmaktadır. Ancak, AES ile karşılaştırıldığında nispeten yavaş hızı nedeniyle, yavaş yavaş yerini daha modern algoritmalara bırakmaktadır.

Blowfish, hızlı ve güvenli veri depolama için tasarlanan simetrik bir şifreleme algoritmasıdır. Değişken uzunluklu bloklarda çalışarak 32 bit ile 448 bit arasında değişen anahtar boyutlarını desteklemektedir.

Basit ve verimliliği nedeniyle kısıtlı kaynaklara sahip ortamlar için tercih sebebi olmaktadır. Henüz AES kadar yüksek güvenlik seviyesi vaad etmemektedir.

SHA (Güvenli Karma Algoritmalar), SHA-256 ve SHA-3 gibi SHA algoritmaları, veri bütünlüğü doğrulaması ve sabit boyutlu karma değerleri oluşturmak için kullanılmaktadır. Bu algoritmalar, isteğe bağlı uzunluktaki

girdi verilerini alarak 256 veya daha yüksek bitte sabit boyutta bir karma değer üretir. SHA algoritmaları, saklanan verilerin bütünlüğünü doğrulamak ve kurcalanmadığından emin olmak için yaygın olarak kullanılmaktadır.

Güvenli veri depolama amacıyla algoritma seçiminde verilerin hassasiyeti, performans gereklilikleri, mevcut sistemlerle uyumluluk, ilgili güvenlik standartları ve düzenlemelerine uygunluk gibi faktörlerin göz önünde bulundurulması esastır. Ek olarak, kapsamlı veri koruması sağlamak için şifreleme algoritmalarının yanı sıra sağlam anahtar yönetimi uygulamaları, güvenli depolama altyapısı, erişim kontrolleri ve güvenli protokoller uygulanmalıdır.

IV. Güvenli Depolama Yöntemleri ve Protokolleri

Verilerin güvenli bir şekilde depolanmasını sağlamak için tasarlanan protokoller verileri şifrelemek, kullanıcıların kimliğini doğrulamak ve veri bütünlüğünü korumak için kullanılmaktadır. SFTP, SSH, HTTPS, IPsec, CHAP ve ağa bağlı depolama protokolleri veri güvenliği açısından yaygın olarak kullanılan protokollerdir.

SFTP (Güvenli Dosya Aktarım Protokolü), bir ağ üzerinden güvenli dosya aktarımı sağlayan bir protokoldür. FTP'nin işlevselliğini SSH'nin (Secure Shell) güvenlik özellikleriyle birleştirir. SFTP, aktarım sırasında verileri korumak için şifreleme ve kimlik doğrulama mekanizmalarını kullanmakta ve dosyaların sistemler arasında güvenli bir şekilde aktarılmasını sağlamaktadır.

SSH (Güvenli Kabuk), güvenli iletişim ve veri aktarımı sağlayan ağ protokolüdür ve güvenli olmayan ağlarda kullanılabilmektedir. Veri gizliliğini ve bütünlüğünü korumak için şifreleme kullanmakta ve kullanıcıların ve sunucuların kimliğini doğrulamak için kimlik doğrulama mekanizmaları sağlamaktadır. SSH, sistemlerin güvenli uzaktan yönetimi ve güvenli dosya aktarımları için yaygın olarak kullanılmaktadır.

IPsec (İnternet Protokolü Güvenliği), bir ağda IP iletişimini güvence altına almak için kullanılan protokol paketidir. IP paketleri için kimlik doğrulama, şifreleme ve bütünlük doğrulaması sağlayarak ağ cihazları arasında güvenli veri aktarımı sağlamaktadır. Güvenli uzaktan erişim ve siteden siteye bağlantı için sanal özel ağlar (VPN'ler) oluşturmak için yaygın olarak kullanılmaktadır.

CHAP (Karşılıklı El Sıkışma Kimlik Doğrulama Protokolü) ile iSCSI (Internet Küçük Bilgisayar Sistemi Arayüzü): iSCSI, bir IP ağı üzerinden SCSI (Küçük Bilgisayar Sistemi Arayüzü) komutları göndermek için kullanılan bir protokoldür. CHAP ile birleştirildiğinde, iSCSI başlatıcı (istemci) ile iSCSI hedefi (depolama aygıtı) arasında güvenli kimlik doğrulama sağlar. CHAP, yalnızca yetkili başlatıcıların depolama aygıtına erişebilmesini sağlamaktadır.

Ağa Bağlı Depolama (NAS) Protokolleri, bir ağ üzerinden paylaşılan depolama kaynaklarına güvenli erişim sağlayarak istemcilerin dosyaları güvenli bir şekilde depolamasına ve almasına olanak tanımaktadır.

Veri güvenli depolama yöntemleri, verileri yetkisiz erişim, kurcalama, kayıp veya hırsızlığa karşı korumaya odaklanır. Şifreleme, bir şifreleme algoritması ve gizli bir anahtar kullanarak verileri bir şifreli metin formatına dönüştürme işlemidir. Şifrelenmiş veriler, karşılık gelen şifre çözme anahtarı olmadan okunamaz. Şifreleme, veri gizliliğini korur ve verilere erişilse veya ele geçirilse bile güvenli kalmasını sağlamaktadır. Erişim kontrolleri, saklanan verilere erişimi yetkili kişi veya kuruluşlarla sınırlamaktadır. Erişim denetimleri, kullanıcı kimlik doğrulaması, rol tabanlı erişim denetimi (RBAC) ve belirli kullanıcılara veya gruplara atanan erişim izinleri gibi mekanizmaları içerebilmektedir. Veri sınıflandırması, verilerin hassasiyetine, önemine veya düzenleyici gerekliliklere göre sınıflandırılmasını içermektedir. Veri segmentasyonu, erişimi sınırlamak ve bir veri ihlalinin etkisini en aza indirmek için verileri mantıksal veya fiziksel olarak ayırmayı içerir. Segmentasyon, ağ segmentasyonu, bölümleme veya veri setlerinin izolasyonu yoluyla yapılabilmektedir. Fazlalık ve yedeklemeler, saklanan verilerin kullanılabilirliğini ve dayanıklılığını sağlamaktadır. Fazlalık, verilerin yinelenen kopyalarını oluşturmayı ve bunları farklı konumlarda veya sistemlerde depolamayı içerir. Bu, bir kopya tehlikedeyse veya erişilemezse, başka bir kopyanın kullanılabilir olmasını sağlamaktadır. Düzenli yedeklemeler, veri kaybı, bozulma veya sistem arızası durumunda geri yüklenebilecek ek veri kopyaları oluşturmaktadır. Saklanan verilerdeki hassas veya kişisel olarak tanımlanabilir bilgileri (PII) korumak için veri maskeleme ve anonimleştirme teknikleri kullanılmaktadır. Veri maskeleme, hassas verileri gerçekçi ancak kurgusal verilerle değiştirirken, verilerin biçimini ve yapısını korur. Anonimleştirme, bireysel gizliliği korumak için tanımlayıcı bilgileri kaldırır veya şifreler. Bu teknikler, verileri test etme, analiz etme veya diğer amaçlarla kullanmasına ve paylaşmasına olanak tanırken, verilerin açığa çıkma riskini en aza indirmektedir. Depolanan verileri korumak için fiziksel depolama altyapısı güvenli olmalıdır. Buna erişim kontrolleri, gözetim sistemleri, çevresel kontroller ve yangın söndürme mekanizmaları içeren güvenli veri merkezleri veya sunucu odaları dahildir. Fiziksel güvenlik önlemleri, depolama aygıtlarına yetkisiz fiziksel erişimi önleyerek hırsızlığa, hasara veya yetkisiz kaldırmaya karşı koruma sağlamaktadır. Veri yaşam döngüsü yönetimi, verilerin oluşturulmasından elden çıkarılmasına kadar yönetilmesini içermektedir. Veri depolama, saklama, arşivleme ve güvenli silme işlemlerini içerir. Veri yaşam döngüsünü uygun şekilde yönetmek verilerin gerekli süre boyunca güvenli bir şekilde saklanmasını ve artık ihtiyaç duyulmadığında güvenli bir şekilde imha edilmesini sağlayabilmektedir. Güvenlik izleme ve denetimi, depolama sistemlerinin ve veri erişim faaliyetlerinin sürekli olarak izlenmesini içerir. Bu, erişim günlüklerinin günlüğe kaydedilmesini ve analiz edilmesini, şüpheli etkinliklerin tespit edilmesini ve bunlara yanıt verilmesini ve güvenlik açıklarının belirlenmesi ve güvenlik politikaları ve düzenlemelerine uygunluğun sağlanması için düzenli güvenlik denetimlerinin yürütülmesini içermektedir.

Saklanan verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamada güvenli depolama yöntemleri ve protokoller önemli rol oynamaktadır. Protokoller depolama, aktarım ve erişim işlemleri sırasında verileri korumak için şifreleme, kimlik doğrulama ve güvenli iletişim mekanizmaları sağlamaktadırlar. Protokollerin ve yöntemlerin seçimi seçimi, depolama altyapısının ve kullanılan uygulamaların özel gereksinimlerine, uyumluluğuna ve güvenlik hususlarına bağlıdır.

V. Anahtar Yönetimi ve Güvenli Depolama

Güvenli depolamada anahtar yönetimi, depolamadaki verilerin güvenliğini sağlamak için kullanılan şifreleme anahtarlarının oluşturulması, dağıtılması, saklanması ve korunması ile ilgili uygulamaları, süreçleri ve protokolleri ifade eder. Etkili anahtar yönetimi, saklanan verilerin gizliliğini ve bütünlüğünü korumak için kritik öneme sahiptir. Anahtar yönetiminin önemli unsurlarından biri olan anahtar üretiminde şifreleme için kullanılan anahtarlar, genellikle güvenli rasgele sayı üreteçleri kullanılarak oluşturulur. Anahtarların gücü ve rastgele oluşu, şifrelenmiş verilerin güvenliğini sağlamak için gereklidir. Şifreleme anahtarlarının yetkili taraflara güvenli bir şekilde dağıtılması çok önemlidir. Bu nedenle anahtar dağıtımı, güvenli dosya aktarım protokolleri, anahtar yönetim sistemleri veya donanım güvenlik modülleri (HSM'ler) gibi güvenli kanallar aracılığıyla gerçekleştirilebilmektedir.Anahtar dağıtım mekanizmaları, yalnızca yetkili kişilerin veya sistemlerin anahtarları almasını sağlamalıdır. Bu aşamada anahtarları yetkisiz erişime veya tehlikeye karşı korumak için uygun anahtar depolama hayati önem taşımaktadır. Anahtarlar güvenli bir şekilde, genellikle şifrelenmiş biçimde saklanmalı ve erişim yetkili personelle sınırlandırılmalıdır. Anahtarları güvenli bir şekilde depolamak ve yönetmek için donanım güvenlik modülleri (HSM'ler) veya güvenli anahtar yönetim sistemleri kullanılabilmektedir. Güvenliği artırmak için ise düzenli olarak anahtar döndürme yapılmalıdır. Bu, yeni şifreleme anahtarları oluşturmayı ve mevcut olanları değiştirmeyi içermektedir. Anahtar rotasyonu, uzun vadeli anahtar gizliliği riskini azaltmakta ve güvenliği ihlal edilmiş veya güncelliğini yitirmiş anahtarların, saklanan verilerin güvenliğini tehlikeye atmamasını sağlamaktadır. Bir anahtarın tehlikede olduğu veya artık gerekli olmadığı durumlarda, şifrelenmiş verilere yetkisiz erişimi önlemek için anahtar derhal iptal edilmelidir. İptal, anahtarın kullanımının devre dışı bırakılmasını ve verilerin şifresini çözmek için kullanılamayacağından emin olmayı içermektedir. Bazı durumlarda, bir anahtar emanet veya kurtarma mekanizmasının yürürlükte olması gerekebilir. Şifreleme anahtarlarının bir kopyasını güvenilir bir üçüncü tarafla güvenli bir şekilde saklamayı içeren bu yöntem, anahtar kaybı veya sistem arızası durumunda anahtarın kurtarılmasına izin vererek şifrelenmiş verilere erişim olanağı sağlamaktadır. Anahtarlara artık ihtiyaç kalmadığında veya ele geçirildiğinde, kurtarılamamalarını sağlamak için uygun anahtar imha önlemleri alınmalıdır. Yetkisiz kullanımı önlemek için anahtar materyalin saklanan kopyalarının güvenli bir şekilde silinmesini veya yok edilmesini içerebilmektedir. Uygun anahtar yönetimi uygulamaları, depolamadaki şifrelenmiş verilerin güvenliğini sağlamak için önemlidir.

VI. Fiziksel Güvenlik Önlemleri

Fiziksel güvenlik önlemleri, verilerin depolandığı fiziksel altyapıyı ve depolama cihazlarını korumak için tasarlanmıştır. Veri depolama alanlarına yetkisiz fiziksel erişimi önlemek için erişim kontrol mekanizmalarının uygulanması önemlidir. Bu; veri depolama alanlarına erişimi kontrol etmek ve sınırlamak için fiziksel engeller, çitler veya kapılar oluşturmak, depolama tesisine giren kişilerin kimliğini doğrulamak ve yetkilendirmek için kart okuyucular, biyometrik tarayıcılar veya PIN kodları gibi erişim kontrol sistemlerini kullanmak veya hassas alanlara yalnızca yetkili kişilerin girmesini sağlamak için ziyaretçi kayıt prosedürlerini ve eskort gerekliliklerini uygulamak olabilmektedir. Bir diğer önlem mekanizması ise gözetim sistemleridir. Gözetim sistemlerinin konuşlandırılması, veri depolama alanlarındaki etkinliklerin izlenmesine ve kaydedilmesine yardımcı olmaktadır. Bu süreç genel olarak; giriş ve çıkış noktalarını, depolama alanlarını ve kritik altyapıyı izlemek için kameraları stratejik olarak kurmak, gözetim akışlarının gerçek zamanlı olarak izlenmesi ve kaydedilen görüntülerin belirli bir süre boyunca saklanması, yetkisiz erişim girişimleri, kurcalama veya diğer güvenlik ihlalleri durumunda uyarıları tetikleyen entegre alarmlar şeklinde özetlenebilmektedir. Tüm bunların yanı sıra depolanan verilerin bütünlüğünü ve uzun ömürlü olmasını sağlamak için uygun çevresel koşulların sürdürülmesi esastır. Bu amaçla sıcaklık ve nem kontrolü, yangın söndürme sistemleri, güç yedekleme gibi sistemlerin kullanımı zorunlu hale gelmektedir.Sabit sürücüler vb gibi fiziksel depolama ortamlarını depolamak için güvenli kabinler veya raflar kullanmak, hırsızlığa veya yetkisiz erişime karşı ek bir koruma katmanı sağlar. Bu depolama birimleri kilitleme mekanizmalarına, erişim kontrollerine sahip olabilir ve hatta güvenli kasalar veya kısıtlı alanlar içinde yer alabilmektedir. Veriler bir veri merkezinde veya sunucu odasında saklanıyorsa, veri merkezi erişim kontrolleri, sunucu odası izleme, kablo yönetimi vb hususlar dikkat gerektirmektedir. Artık kullanılmayan veri depolama ortamları için güvenli imha prosedürlerinin uygulanması amacıyla verilerin atılan veya devre dışı bırakılan depolama aygıtlarından kurtarılamayacağından emin olmak için parçalama, manyetik ortamı giderme (manyetik ortam için) veya güvenli silme yöntemleri gibi fiziksel imha tekniklerini içermektedir. Tüm bu fiziksel güvenlik önlemleri, veri güvenliğine kapsamlı bir yaklaşım oluşturmak için diğer teknik ve idari güvenlik kontrolleriyle birlikte çalışmaktadır.

VII. Veri Erişim Kontrolleri

Güvenli veri depolamada, hassas verilere yalnızca yetkili kişi veya kuruluşların erişebilmesini sağlamak için veri erişim kontrolleri uygulanmaktadır. Kimlik ve Erişim Yönetimi (IAM) sistemleri, bir kuruluş içindeki kullanıcı kimliklerinin, rollerinin ve izinlerinin yönetilmesine yardımcı olur. Kullanıcı hesaplarının, kimlik doğrulama ve yetkilendirme süreçlerinin merkezi yönetimini sağlamaktadır. IAM, yalnızca kimliği doğrulanmış ve yetkili

kullanıcıların verilere erişebilmesini sağlamaktadır. Kullanıcı provizyonu, rol tabanlı erişim kontrolü (RBAC), çok faktörlü kimlik doğrulama (MFA) ve erişim politikası uygulaması gibi özellikler içermektedir. Ayrıcalıklı Erişim Yönetimi (PAM), kritik sistemlere ve verilere yükseltilmiş erişim haklarına sahip ayrıcalıklı hesapların güvenliğini sağlamaya ve yönetmeye odaklanmaktadır. PAM çözümleri, ayrıcalıklı erişimin sıkı bir şekilde kontrol edilmesini ve izlenmesini sağlar. Genellikle parola kasalama, oturum izleme, tam zamanında erişim ve ayrıcalıklı kullanıcı etkinliği günlüğü gibi özellikleri içermektedir. PAM çözümleri, genellikle verilerde veya sistem yapılandırmalarında önemli değişiklikler yapma yeteneğine sahip olan ayrıcalıklı kullanıcıların yetkisiz erişim riskini azaltır. Rol Tabanlı Erişim Kontrolü (RBAC), izinleri önceden tanımlanmış rollere göre atayan bir erişim kontrol modelidir. IAM sistemleri ise tipik olarak, yöneticilerin ilişkili erişim ayrıcalıklarına sahip rolleri tanımlamasına izin veren RBAC işlevselliğini içermektedir. Kullanıcılara daha sonra iş sorumluluklarına göre belirli roller atanmakta ve erişim hakları buna göre verilmektedir. RBAC, izinleri her kullanıcı için ayrı ayrı değil, rol düzeyinde yöneterek erişim denetimini basitleştirmektedir. Nitelik Tabanlı Erişim Kontrolü (ABAC), erişim kontrolü kararları vermek için kullanıcılar, veriler ve ortamla ilişkili çeşitli öznitelikleri dikkate alan bir modeldir. IAM sistemleri, erişim izinlerini belirlemek için kullanıcı öznitelikleri, kaynak özellikleri veya bağlamsal faktörler gibi öznitelikleri değerlendiren ABAC ilkelerini içerebilmektedir. ABAC, erişim izni verirken dinamik öznitelikleri ve koşulları göz önünde bulundurarak daha ayrıntılı kontrol sağlamaktadır. Güçlü veri erişim kontrolleri, erişim kayıt ve denetim mekanizmalarını içermektedir. Bu mekanizmalar erişim girişimlerini, etkinlikleri ve veri erişimiyle ilgili olayları izlemekte ve kaydetmektedir. IAM ve PAM çözümleri genellikle kullanıcı erişimi, gerçekleştirilen işlemler ve zaman damgaları gibi ayrıntıları yakalayan günlük kaydı ve denetim özellikleri sunmaktadır.

REFERANSLAR

[1] Stallings, W., & Brown, L. (2022). Computer Security: Principles and Practice (4th ed.). Pearson.

[2] Güney, T. (2018, 1 Ekim).Hashing ve Encryption nedir?[Blog yazısı]. Erişim adresi: https://atarikguney.medium.com/hashing-ve-encryption-nedir-de9ad799a2d4