SAYISAL İÇERİK GÜVENLİĞİ: UYGULAMA YÖNTEMLERİ

Alper Uğur[1] ve Murat Aydos[2]

[1] Ar. Gör. Pamukkale Üniversitesi Bilgisayar Mühendisliği Bölümü
Morfoloji Binası Kınıklı Kampüsü, 20017 DENİZLİ
augur@pamukkale.edu.tr

[2] Yrd. Doç. Dr., Pamukkale Üniversitesi Bilgisayar Mühendisliği Bölümü
Morfoloji Binası Kınıklı Kampüsü, 20017 DENİZLİ
maydos@pamukkale.edu.tr

Anahtar Kelimeler: Sayısal İçerik Güvenliği **Oturum Konusu:** Güncel Bilgisayar Bilimleri

1. GİRİŞ

Bilişim dünyasındaki teknolojik gelişmeler, görsel ve işitsel medyanın üretim ve dağıtımını örneksel ortamdan sayısal ortama kaydırmıştır. Örneksel medyanın üretiminde karşılaşılan birebir kopyalama sebebiyle gereken uzun imal zamanı, bir sonraki kopyadaki kalite düşüşü gibi mali negatif etkenler sayısal teknolojinin kullanılması ile ortadan kalkmıştır. Fakat sayısal içeriğin bu denli kolay çoğaltılabilir ve iletilebilir olması onu yasal olmayan biçimlerde paylaşılır ve tüketilir kılmıştır.

Dünyanın en büyük elektronik eşya üreticilerinden Sony, 2002 yılı Haziranı'nda yayınladığı raporda sayısal korsanlığın müzik dünyasına verdiği zararın 160 milyon dolar olduğunu belirtmektedir[1]. Bununla birlikte 1998 yılında 8,6 milyar dolar olan online satış ve B2B dağıtım piyasası 2003'te 193 milyar dolara yaklaşmıştır[2]. Bu ivmenin güvenli dağıtım sağlandığı takdirde daha da artması açıktır.

Ticari kâr paylarının düşüşü ve telif haklarının çiğnenmesi, piyasadaki ivmelenmenin korunması gereği üretici firmaları sayısal içeriğin korunması konusunda çalışmalar yapmaya yöneltmiştir.

2. GÜVENLİK YÖNTEMLERİ

Geliştirilen teknoloji ve önerilen çözümleri pasif koruma, yarı-aktif koruma ve aktif koruma başlıklarında gruplandırabiliriz.

2.1. Pasif Koruma

Sayısal içeriğin yasadışı kullanımının tespiti için kullanılan yöntemlerdir. Erişim engeli ve içerik gizliliği yoktur.

Lisanslama: Sayısal içerik ile son kullanıcının bir belge ile ilişkilendirilmesi. Genel olarak kullanıcı ya da cihaz kimliği, kullanım hakları, başlangıç ve bitiş sürelerini içerir.

Filigran (watermarking): Kullanılan yöntem, görsel medyaya görüntü işleme teknikleri kullanılarak; fark edilmemesi için gizlenmiş, ek veri yerleştirmektir. Yerleştirilen ek veri, lisans benzeri bilgileri taşır.

Bu yöntemlerde özel kurumlar (BSA) ya da yazılımlar (web-spider) vasıtasıyla yasadışı kullanım belirleme çalışmaları yapılmakta ve hukuki yollarla sonuca gidilmektedir.

2.2. Yarı-Aktif Koruma

Pasif korumadaki lisanslama yöntemine ek olarak teknik uygulamalarla içerik erişiminin sınırlandırılması esaslı çözüm önerileridir.

Sinyal-işleme tabanlı sistemler (Macrovision): Televizyonda yayınlanan görüntülerin VHS kayıt cihazlarınca kaydedilmesini engelleyen bir tekniktir Uygulama TV ve VHS kayıt cihazlarının teknik farklılıklarına dayanmaktadır. Yapılan yayınla beraber TV'lerin yok saydığı ama VHS kayıt cihazlarının dikey renk senkronizasyonunu karıştıran ek sinyalin gönderilmesini temel alıyor. Piyasadaki kayıt cihazlarının yaklaşık %90'ının buna duyarlı olduğu öne sürülmekte[3].

Yayın kodekleri ve sıkıştırma yöntemleri (MPEG-DVD): Sayısal içeriğin iletim güvenliğini sağlayan yöntemlerdir. Erişim sınırlaması sağlar. Verilerin sıkıştırma, şifreleme gibi bilimsel metotlarla işlenerek sadece yetkin programlarla çalışması sağlanır. Bu programlar aracılığıyla da lisans tespiti ve yasal kullanım belirlenmesi yapılabilmektedir.

Akıllı kartlar (SmartRight): Açık anahtarlı sertifikaya sahip taşınabilir mikro sistemlerdir. Cihazlar, akıllı kartlar ile sertifika değişimi yaparak ev-içi ağı için bir anahtar oluşturulmasını sağlar. Akıllı kartlar, kendi içeriklerini şifreleme ve deşifreleme işlevlerini yerine getirebilirler.

Sayısal Hak Yönetimi (DRM): Şimdiye kadar bahsedilen yöntemlerin tümleşik halidir. İçeriğin ek-programlar ya da veriler (plug-in/sertifika) yardımıyla cihazla ilişkilendirilmesi, lisanslamanın yapılması esasına dayanır. Ürün değil lisans satımı üzerine kurulmuş, dürüst kullanıcı temelli bir yöntemdir.

Bu çözüm genel olarak ev-içi ağ sistemi için sunulmaktadır. Kullanıcının sahip olduğu tüm cihazların uyumluluğu ve satın alınan hakların tek bir cihazla sınırlandırılmaması üzerine geliştirilmiştir

Kullanıcıya lisansını aldığı ürün kriptografik yöntemlerle (simetrik anahtarlı algoritma) şifrelenmiş olarak iletilir. Sayısal içerik lisanslı cihazda deşifrelenip kullanıma hazır duruma gelir. Kullanıcının sahip olduğu tüm cihazların anahtar değişimi ve kimlik doğrulama gibi kriptografi tabanlı teknikler ile uyumu sağlanır. Sayısal imza ve sayısal sertifika uygulamaları kullanım, doğrulama, yetkilendirme gibi islevlerde kullanılması önerilen destek yöntemlerdir[4].

2.3. Aktif Koruma

Daha önce değinilen sayısal içerik güvenliği uygulama yöntemleri; içerik gizliliği, donanımsal kısıtlamalar, tespit gerekliliği gibi eksiklikler ile sayısal içerik için istenilen verimlilikte tam güvenlik sağlayamamaktadırlar. Bu üretici firmaları özgün donanım tasarımları ve yazılım çözümlerinden oluşan uygulamalar geliştirmeye zorlamıştır. Tasarlanan bu uygulamalarda, sayısal içeriğin iletiminde kriptografik protokoller kullanılmakta ve sayısal içerik yine kriptografik yöntemlerle şifrelenip koruma altına alınmaktadır.

DDWG-HDCP: Sayısal Görüntü Çalışma Grubu (Digital Display Working Group) tarafından ana sunucu ve görüntü birimi arasında evrensel bir sayısal arayüz standardı olmak üzere geliştirilen ve kullanılan DVI arayüzü çıkışlarını kopyalamaktan koruyan bir sistemdir[5].

Görüntü kaynağı ve görüntü birimi arasında güvenli bir sayısal bağlantı sağlamayı amaçlamaktadır. IEEE1394 için geliştirilen DTCP ile yapısal paralellik gösterir. Uygulamalar, donanımsal olarak farklılık gösterir. (Sıkıştırılmamış yüksek-çözünürlüklü görüntüler için yeterli bant genişliği, parazitsiz sağlanabilen azami uzunluk, cihaz bağlantıları vs[6].)

5C-DTCP: Intel, Hitachi, Matsushita, Sony ve Toshiba şirketlerinin oluşturduğu 5C birlikteliğinin sunduğu çözüm önerisidir[7]. IEEE1394 bus standardı üzerine kurulan sistem, dört temel katmandan oluşmakta:

- Kimlik denetimi ve anahtar değişimi
- İçerik şifreleme
- Kopya Kontrol Bilgisi(CCI)
- Sistem yenilenebilirlik

Sistem iki güvenlik düzeyini esas almaktadır. Tam korunma gerektiren ve kopyalanma izni verilmeyen içerikler için Tam-Kimlik Denetimi ve bir tek kopya hakkı verilen Kısıtlı-Kimlik Denetimi.

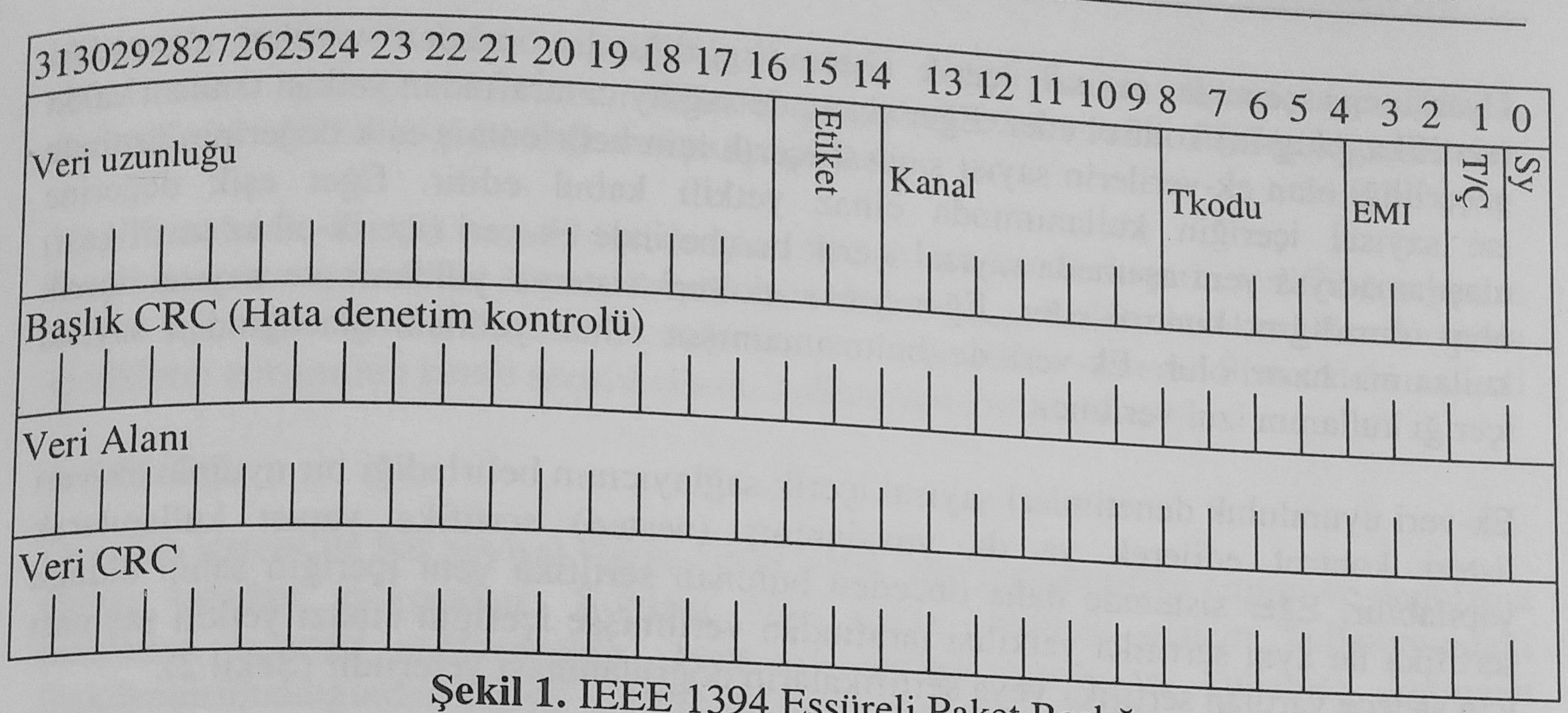
Bu denetim protokolleri veri bütünlüğü ve imzalama için Sayısal İmza Algoritması, iki ya da daha fazla tarafın ortak gizli anahtar oluşturma için Diffie-Hellman Anahtar-Değişim Algoritması kullanmaktadır. Her iki algoritmanın uygulamasında ayrık logaritma tabanlı sistemlerden daha performanslı Eliptik Eğri Kriptografisi kullanılmıştır.

İçerik şifreleme için Hitachi'nin permutasyon ve yerdeğişim tabanlı genel-anahtar blok şifreleme algoritması M6 (anahtar uzunluğu : 64 bit) kullanılmaktadır. İsteğe bağlı Değiştirilmiş Blowfish (anahtar uzunluğu : 56 ve 64 bit) ve DES (anahtar uzunluğu : 56 bit) şifrelemelerini de içermektedir.

İçeriğin çoğaltılmasıyla ilgili korumada Kopya Kontrol Bilgisi'nden yararlanılmaktadır. Eşsüreli paket başlığının en anlamlı iki ikilinde tutulan Şifreleme Mod Gösterge (EMI) değerleri şifreleme/deşifreleme modunu ayırt eder. Yine başlıkta tutulan Tek/Çift biti şifreleme yapılacak anahtarı belirler (0:Çift değer, 1: Tek değer). Tablo 1'de mod kodları, Şekil 1'de IEEE1394 eşsüreli paket başlığının yapısı gösterilmiştir.

Tablo 1. Şifrele Mod Göstergeleri ve Karşılıkları

Değer	Şifreleme Mod Göstergeleri	Gerekli Kimlik Denetimi
00	Kopya-korumasız	Yok, şifrelenmemiş
01	Daha fazla kopya yok	Tam ya da Kısıtlı
10	Tek-nesil-kopya	Tam ya da Kısıtlı
11	Kopyalanamaz	Tam



Şekil 1. IEEE 1394 Eşsüreli Paket Başlığı

Tam korumalı cihazlarda kullanılması önerilen sistem yenilenebilirlik işlevi uzun vadeli sistem bütünlüğü ve yetkisiz cihazları feshetme imkanı sağlamaktadır. İletilen içeriğe ek gönderilen sistem yenilebilirlik mesajları, Tam-Kimlik Denetimi uygulanan cihazlarda saklanan Sertifika İptal Listesini yenileyerek sistemi günceller.

3. YENİ BİR YAKLAŞIM: SAYISAL HAK YÖNETİMİNDE EŞİK ŞEMASI UYARLAMASI

Yukarıda bahsedildiği gibi Sayısal Hak Yönetimi'nde içeriğin güvenliği, sisteme yüklenen plug-inler ve sayısal sertifikalar ile sağlanmaktadır. Bunun yanında sistemin cihaz tabanlı olması, kullanıcının sahip olduğu sayısal içeriği kendisine ait farklı cihazlarda kullanabilmesi için her cihaza yeni bir sertifika edinmesini gerektirmektedir.

Bilindiği gibi mobil telefonlar, disk-çalarlar gibi düşük sistem hafızası ve az enerji tüketimi gibi uygulama kısıtlayıcı unsurları olan cihazlarda verilerin tutulması ve işlenmesi kullanılacak mimarilerde önem taşımaktadır.

Biz, söz konusu cihazlarda Shamir'in eşik şemasının SHY uyarlamasının sayısal içerik güvenliği için çözüm getireceği kanısındayız.

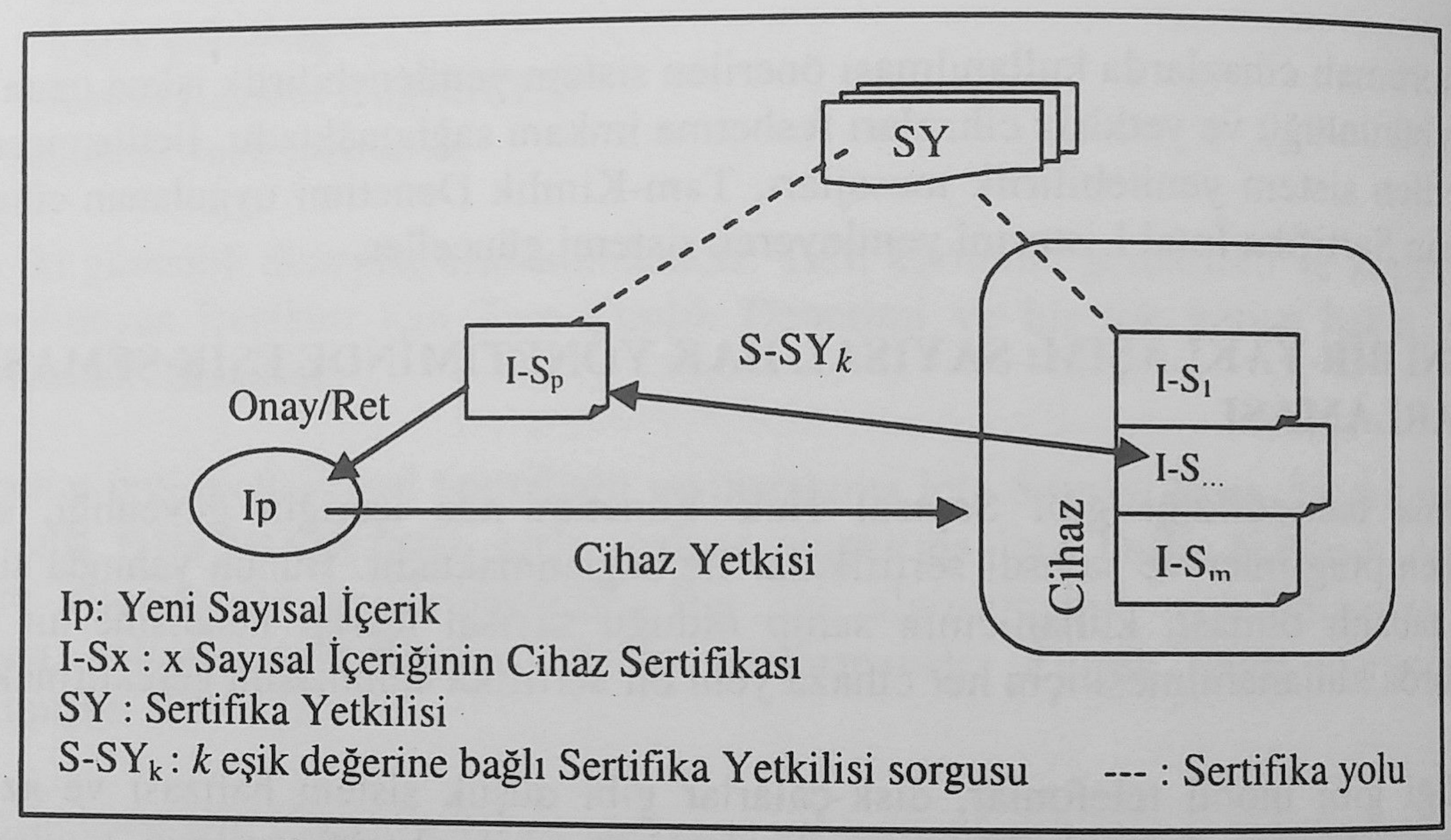
Eşik şeması ya da daha genel adıyla giz paylaşımı şeması, n adet paylaşım için k eşiği tanımlar. n paylaşımın oluşturacağı kümenin en az k elemanından oluşacak tüm alt kümeler gizi çözmeye yetecek bunun yanında $(k-1)$ adet paylaşıma karşı bile gizli bilgi açığa çıkmayacaktır. Bu (k,n) eşik şeması diye adlandırılır[8].

Eşik şemasının aşağıda yer alan bazı özellikleri de uyarlanan sistemin özelliklerinde belirleyici rol oynamaktadır.

- Gizliliği ihlal edilmiş paylaşımlar diğer paylar değiştirilmeden yeni paylaşımlar ile değiştirilebilir.
- Gizli bilgide hiçbir değişiklik yapılmadan yeni paylaşım kümeleri elde edilebilir.
- Bireylere farklı sayıda paylaşım verilerek hiyerarşik bir şema oluşturulabilir. Verilen paylaşım sayısı her bireyin sistemdeki önemini belirler.

Uyarlanmış şemada sayısal içerik sisteme girdiğinde önceden varolan ek-verileri (sertifika, plug-in) kontrol eder. Eğer sistemde sağlayıcı tarafından yetkisi tanınan ya da geçerliliği olan ek-verilerin sayısı sayısal içerik için belirlenmiş eşik değerinin üstünde ise sayısal içeriğin kullanımında cihaz yetkili kabul edilir. Eğer eşik değerine ulaşılamadıysa yeni aşamada sayısal içerik beraberinde ek-veri (içerik-cihaz sertifikası) olup olmadığını kontrol eder. Eğer varsa ek-veri sisteme yüklenir ve sayısal içerik kullanıma hazır olur. Ek-veri de bulunamamışsa cihaz yetkisiz olacağından sayısal içeriği kullanım izni verilmez.

Ek-veri uyumluluk denetimleri sayısal içerik sağlayıcının belirlediği bir uyumlu ek-veri listesi kontrol edilerek ya da yuvalanmış (nested) sertifika yapısı kullanılarak yapılabilir. Eğer sistemde daha önceden bulunan sertifika yeni içeriğin sahip olduğu sertifika ile aynı sertifika yetkilisi tarafından verilmişse içeriğin cihazı yetkili sayması için sadece varolan sertifika veya sertifikaların doğrulanması yeterlidir (Şekil 2).



Şekil 2. *k* eşik değerine bağlı sertifika sorgusu

Süresi dolan sertifikalar ya da üzerinde değişiklik yapılmış, şüpheli ek-veriler üzerinde denetim yöntemleri geliştirilebilir. Örneğin, DTCP yönteminde kullanılan bir sistem yenilenebilirlik mesajı ile sistemdeki ek-verilerin geçerlilikleri güncellenebilir ve geçerliliği iptal edilen veriler hariç tutularak sayısal içeriğin kullanımı için gerekli eşik değeri, diğer yetkili ek-veriler kullanılarak aşılacaktır. Eğer yeterli eşik değeri elde edilemezse cihaz yetkisiz kabul edilip sayısal içeriğin kullanımı engellenecektir. Dikkat edilmesi gereken nokta sayısal içeriğin kullanımının, öncelikle (varsa) kendine ait sertifika ile bağlı olduğudur. Başka bir deyişle içeriğe özel sertifika, gereken *k* eşik değerlerinin tamamını içerir. Kopya korumasız içerikler içinse *k* eşik değerinin 0 olarak belirtilmesi yeterlidir.

Cihaza bağlı ek-veri ile iletilen sayısal içeriğin, uyarlanmış eşik şeması uygulamasınca depolanmaması; sadece, sistemde eşik değerini sağlayacak yeterli sayıda depolanmış ek-verinin bulunmaması (ilk yüklemedeki ek-verilerin geçerliliğini yitirmesi) durumunda sayısal içeriğe ait cihaza bağlı ek-verinin geri yüklenmesi ek işlemini gerektirmektedir. Tasarım aşamasında sayısal içerik ile birlikte tespit için bir bitlik bilgi (0: ek-veri yok 1: ek-veri ile iletildi) tutulması buna yardımcı olacaktır.

Sistemde, önem arz eden sayısal içerik, eşik değeri *k*, ve ek-veri tespit bitinin şifrelenmesi yeterli olacaktır. Bunun yanında kriptografik hash algoritmaları kullanılarak veri bütünlüğü doğrulaması yapılabilir.

Uygulamalarda, m adet sayısal içerik için cihazda tutulacak ek-veri (sertifika) sayısı m iken bizim şemamızda bu sayı en büyük eşik değeri k_{max} kadar olacaktır. Her durumda $m >= k_{max}$ olacağından sunulan çözümün avantajı açıktır. (m=k: Sistemdeki sayısal içeriklerin tamamının kendi sertifikalarını kullanması durumudur.)

4. SONUÇ

Önerilen sistem ile her sayısal içerik-cihaz ikilisi için ayrı sertifika temini ve depolama gereği ortadan kalkacaktır. Böylece hem cihaz üzerinde sistem kullanımındaki hafızadan tasarruf sağlanacaktır, hem de sayısal içerik ve kullanıcı doğrudan ilişkilendirilmediğinden kişisel gizlilik de sağlanmış olacaktır. Sistemin yetkisi dağıtıcı tarafından tanınan tek bir ek-veriye bağımlı olmayıp eşik değeri adedince ek-veri kullanımı güvenlik seviyesini arttırıcı rol oynamaktadır.

---

[1] European Industry Association, Content Protection Technologies, 2003

[2] ORBID Corp., 4DRM Digital Rights Management, 2003

[3] a.g.e.[1]

[4] Qiong Liu, Digital Rights Management for Content Distribution, AISW2003, 2003

[5] Silicon Image, High-bandwith Digital Content Protection White Paper, 2000

[6] Bob Perry, IEEE1394 vs. DVI A Comparative Perspective, MDEA,2003

[7] 5C, Digital Transmission Content Protection White Paper, Rev.1.0, 1998

[8] A. Shamir, "How to Share a Security", Communications of the ACM 22, 1979