

A3D3M : AÇIK ANAHTAR ALTYAPISI DESTEKLİ DİJİTAL DELİLLERİ DOĞRULAMA MODELİ

Yusuf UZUNAY

Orta Doğu Teknik Üniversitesi
Enformatik Enstitüsü
Ankara TÜRKİYE
yuzunay(at)ii.metu.edu.tr

Kemal BIÇAKCI

Vrije Üniversitesi
Bilgisayar Bilimleri Bölümü
Amsterdam HOLLANDA
kemal(at)few.vu.nl

Anahtar sözcükler: Bilişim Suçları, Dijital Delil, Dijital Delillendirme, Dijital Delilleri Doğrulama

ABSTRACT

Digital evidences have a paramount importance in the prosecution of a cyber crime however their legal acceptance in the courtroom has some fundamental prerequisites. This is because of their fragile structure enabling the adversary to delete, to modify as well as to corrupt them before the prosecution takes place.

In this paper we present A3D3M as a system model that provides the security of the process for capturing digital evidences in the cyber crime scene. Public key cryptography and digital signatures are among the tools A3D3M employs to establish an integrated solution. As a part of our work, we also try to tackle some of the inherent problems public key technology has when it is applied to the verification of digital evidences.

1. GİRİŞ

Bilişim suçları, son zamanlarda karşılaşılan önemli suç tipleri arasında yer almaktadır. Özellikle bilişim teknolojilerinin kullanımındaki artış, bilişim suçlarının etkisini arttırmakta ve büyük riskler oluşturmaktadır.

Bir suçun aydınlatılmasında ve failinin tespitinde kullanılan en önemli mekanizma delillendirmedir. Bilişim suçları kapsamındaki deliller ise üçe ayrılabilir [1]:

- *Dijital Deliller:* Bir bilişim suçu ile ilgili, dijital biçimde kayıt edilen veya aktarılan bilgiler.
- *Veri Nesnelere:* Bir bilişim suçunun aydınlatılmasında yararlı olabilecek, fiziksel öğelerle ilintili bilgiler.
- *Fiziksel Öğeler:* Üzerine dijital veri kayıt edilmiş veya üzerinden veri iletimi gerçekleştirilmiş fiziksel medyalar.

Bilişim suçları araştırılırken, bu delil tiplerinden en çok dijital delillere ihtiyaç duyulmaktadır. Dijital deliller, yapı itibarıyla bozulmaya ve kolay bir şekilde değiştirilmeye müsait oldukları için, hukuki yönden kabul edilebilirlikleri konusunda bazı sıkıntılar ile karşılaşmaktadır. Bu delillerin mahkeme esnasında gerçek delil özelliği gösterebilmeleri için, delillerin ilk

alındığı andan itibaren değişmediğinin, hangi tarihte, nereden ve kimlerden alındığının doğrulanması büyük önem arz etmektedir.

Literatür incelendiğinde, konunun bazı boyutları üzerine geçmişte yapılmış çalışmalar olmasına rağmen, sorunu çözmeye yönelik entegre bir çözüme rastlanılmamaktadır. Bu makale kapsamında, ilk olarak dijital deliller ile ilgili problemlere göz atılacak ve arkasından makalede kullanılacak bazı tekniklerle ilgili ön bilgi verilecektir. Bölüm 4'te dijital delillendirmede açık anahtar altyapısı ile ilgili sorunlar vurgulanacak olup bölüm 5'de geçmişte yapılan çalışmalar incelendikten sonra bölüm 6'da özellikle olay yerinden alınan dijital delillerin, güvenilir bir şekilde doğrulanmasında büyük kesinlik sağlayacak ve bu alanda ilk olacak bir model (A3D3M) oluşturulmaya çalışılacaktır. Bölüm 7'de modelin faydalarına değinildikten sonra sonuç bölümüyle makale tamamlanacaktır.

2. DİJİTAL DELİLLERLE İLGİLİ PROBLEMLER

Bir suçun araştırılmasındaki amaçlardan bir tanesi suçlu, mağdur ve olay yeri arasındaki bağlantıları ortaya çıkararak suçun failine ulaşmaktır. Locard'ın değişim prensibine göre, suç sahnesine giren bir şey veya bir kişi, olay yerinden bazı şeyleri yanına alırken, bir takım şeyleri de olay yerinde bırakır [2]. Bilişim sistemleri üzerinde ise, iz bırakmadan işlem yapmak neredeyse imkansızdır. Önemli olan bu izleri doğru bir şekilde tespit edip, sonuca götürücü verilere ulaşmaktır.

Dijital deliller, bir çok tipte karşımıza çıkmaktadır. Bunlar veri dosyaları, kurtarılmış silinmiş dosyalar, kayıp alanlardan kurtarılmış veriler, dijital fotoğraf ve videolar, sunucu kayıtları, e-posta, internet geçmişi, web sayfaları, abone kayıtları gibi doğrudan bilgisayar sistemleriyle alakalı deliller olabileceği gibi, günümüzde gömülü bilgisayar sistemlerine sahip bir mikro dalga fırından elde edilebilecek ve bir kundakçılık olayında fırının belirli bir zamanda yangın çıkarmak için programlandığını ortaya çıkarabilecek

veriler de dijital deliller olarak karşımıza çıkmaktadır [1,3].

Dijital deliller, dijital verilerden oluşur. Bu veriler ise bilişim sistemleri üzerine kayıt edilmiş bir ve sıfır ikililerine verilen anlam sonucunda ortaya çıkar. Dolayısıyla doğrudan elle tutulabilir ve gözle görülebilen bir yapının olmayışı, dijital verileri soyut hale getirmektedir. Soyut kavramlardan kesinlik çıkartmak ise çok zordur. Fakat deliller, işlevi itibariyle bir suçu ispat edici nitelikte kesin bulgular barındırmalıdır. Bu nedenle dijital verilerin yüzde yüz delil olarak kullanılması yönünde, büyük problemler meydana gelmektedir. Bu problemler şu ana başlıklar altında toplanabilir :

1. Yapısal Problemler

- Dijital veriler çok kolay bir şekilde değiştirilebilmektedir.
- Dijital verilerin bire bir aynı oluşturulabilmektedir.
- Dijital veriler hassas bir yapıdadır ve manyetik alan, sıcaklık, çarpma gibi çeşitli çevresel etkenler yüzünden kolay bir şekilde bozulabilmektedir.
- Dijital veriler, nasıl kodlandıklarına bağlı olarak anlam kazanabilirler. Günümüzde virüs, truva atı gibi zararlı kodlar sayesinde verilere değişik anlamlar yüklemek mümkündür.

2. Yapısal Problemler Sonucu Oluşan Problemler:

- Dijital Delillerin Bütünlüğü: Dijital veriler üzerinde çok kolay bir şekilde değiştirme, silme ve yenisini oluşturma gibi işlemlerin yapılabilmesi bu delillerin bütünlüğünü sağlamayı çok zorlaştırmaktadır.
- Dijital Delillerin Doğrulanması: Bir kişiyi dijital delillerle birlikte yakaladıktan sonra, mahkeme sürecinde o verilerin gerçekten o kişiye ait olduğunun ispatı gerekmektedir. Fakat delil olarak ele geçirilen verilerin aynı her hangi bir kişi tarafından da oluşturulabilir.
- Dijital Delillerin İnkâr Edilememesi: Dijital delillendirme işlemindeki dijital delilin sahibi, onu ele geçiren şahıslar (Ör: Polis), delilin alındığı medya, delilin ele geçirildiği zaman, delilin içeriği gibi bütün unsurların daha sonradan inkâr edilememesi gerekmektedir.
- Dijital Delillerin Doğruluğu: Dijital delillerin ele geçirilmesi esnasında kullanılan teknikler ve yararlanılan bilgilerin (Örneğin delilin ele geçirilme zamanı) doğruluğunun ispatı gerekir.
- Dijital Delillerin Daha Sonradan Ele Alınabilirliği: Dijital deliller oluşturulduktan sonra, bu delilleri üçüncü bir şahıs inceleyebilmektedir.

Bu problemler dışında, bilişim suçlarındaki örneğin ulusal ve uluslar arası kanunlar ve ortak tanımların

eksikliği gibi genel anlamdaki bazı sıkıntılar dijital deliller için de geçerli olup, bu makale kapsamında, olayın daha çok teknik yöndeki sıkıntılarına değinilecektir.

3. ÖN BİLGİ

Dijital deliller, bilişim hukuku alanındaki önemli problemlerden bir tanesidir. Aslına bakılacak olursa problemin temelinde dijital delillerin, klasik deliller gibi ele alınamamasındaki teknik sorunlar yatmaktadır. En İyi Delil Kuralı'na göre zarar görmediği müddetçe, bir suç ile ilgili orijinal delillerin sunulması zorunludur. Fakat deliller ile ilgili ABD Federal Kurallarına göre bilgisayar verilerinin gerçekten o veriler olduğunun doğruluğu sağlandığı müddetçe bilgisayar çıktıları ve verilerin görüntüleri de orijinal delil olarak kabul edilmektedir. Dolayısıyla dijital delillerin doğrulanması ve inkâr edilememesi, bu bağlamda büyük önem arz etmektedir [1,2].

Dijital veriler ile ilgili doğrulama, bütünlüğün sağlanması, inkâr edememe gibi hususlar aslında yeni gündeme gelmiş konular değildir. Uzun süredir bilişim güvenliğinde özellikle kriptografi bilimi altında çok yoğun tartışılmaktadır.

Doğrulama iki bölümde ele alınabilir. Birincisi göndericinin doğrulanması, ikincisi mesaj içeriğinin doğrulanması. Doğrulama, basit olarak simetrik kriptografi kullanılarak yapılabilir. Örneğin Mesaj Doğrulama Kodu olarak bilinen ve mesaj içeriğinin gizli anahtar ile şifrelenmesi sonucu oluşan bir veri bloğunu gönderilen mesaja eklemek suretiyle hem gönderenin kimliğinden, hem de mesajın içeriğinin değişip değişmediğinden emin olabiliriz. Simetrik kriptografide, ortak kullanılan bir tane anahtar (gizli anahtar) bulunur. Anahtarın sadece gönderici ve alıcıda olduğunu düşünürsek, göndericiden başkası ilgili mesajı bu şekilde şifreleyemeyecektir. Simetrik kriptografideki en önemli sorunlardan bir tanesi iletişime geçilecek kişilere gizli anahtarın dağıtılması ve anahtar değişimidir [4].

Anahtar değişimine gerek kalmadan doğrulama yapabileceğimiz ve günümüzde sık kullanılan başka bir kriptografi çeşidi de asimetrik kriptografidir. Asimetrik kriptografi ilk defa 1976 yılında **Diffie** ve **Hellman** tarafından ortaya atılmış olup binlerce yıldan sonra kriptografi alanında gerçekten devrim sayılabilecek ilk ilerleme olmuştur [5]. Açık-anahtar algoritmaları basit bit işlemleri yerine matematiksel fonksiyonları temel almıştır. Daha da önemlisi açık-anahtar, asimetrik yani sadece bir anahtar kullanan simetrik kriptolamanın tersine iki ayrı anahtarın (Açık ve özel anahtar) kullanılmasını öngörür.

Asimetrik kriptografi bir çok farklı alanda kullanılmakla birlikte, günümüzde en sık tartışılan uygulaması **dijital imzadır**. Dijital imza sistemlerinde gönderici, mesajı kendi özel anahtarıyla

imzalar ve alıcı da göndericinin açık anahtarını kullanarak ilgili mesajı onaylar. İmzalamaktan kasıt mesajın özel anahtar ile işleme tabi tutulması sonucu bir özet çıkarılarak, bu özeti imza niteliğinde gönderilen mesaja eklenmesi anlamına gelir. Günümüze kadar bir çok dijital imza sistemi önerilmiştir. Bir elektronik dökümanı imzalamada kullanılan ilk dijital imza sistemi olan RSA, hala en geniş kullanım alanı gören asimetrik kriptografi algoritmalarından biridir [6].

Dijital imza, özellikle elektronik delillendirmede büyük önem arz etmektedir. Dijital imza kullanımında makaleyi daha iyi anlama adına söz edilebilecek iki önemli kavram vardır. Bir tanesi Dijital Sertifika, diğeri de Açık Anahtar Altyapısı (AAA)'dır.

Dijital sertifikaların çıkış nedeni, dijital imzalarda kullanılan ve herkesin ulaşabileceği bir formatta bulunan açık anahtarın, gerçekten sahibine ait olup olmadığını ispatıdır. Bir **dijital sertifika**, bir açık anahtar, bu açık anahtarın sahibinin kimliğiyle ilgili bilgiler ve bütün bu bilgilerin güvenilir bir kurum tarafından imzalanmasıyla oluşturulur. Bu kuruma **Sertifika Otoritesi (Certificate Authority-CA)** denir. Dijital sertifikaların işleme için gerekli olan alt yapıya verilen isim ise **Açık Anahtar Altyapısı**'dır.

Simetrik ve asimetrik kriptografi kullanılarak mesajın içeriğinin ve mesajı gönderenin doğrulanması gerçekleştirilebilir. Sadece mesajın içeriğinin doğrulanmasına ihtiyaç duyulduğu durumlarda, anahtar kullanmadan doğrulama yapabilen bir yöntem olan **Tek Yollu Özet (Hash) Fonksiyonları** da kullanılabilir. Tek yönlü özet fonksiyonlarında bir x değerinden $H(x)$ 'i hesaplamak çok kolay olmakla birlikte, $H(x)=h$ eşliğinde, bilinen h kodundan x 'i hesaplamak matematiksel açıdan mümkün olamamaktadır. Özet fonksiyonlarının en önemli özelliği değişken uzunluklardaki mesajları alıp işleme tabi tuttukten sonra, sabit uzunlukta bir çıktı üretmeleridir. Dolayısıyla özet fonksiyonları içeriğin doğrulanması dışında, simetrik ve asimetrik kriptografide çok büyük boyuttaki dosyaları sabit uzunluğa çekerek algoritmanın verimliliğinin artmasına da katkı sağlamaktadırlar.

Bu makale çerçevesinde olay yerinden alınan dijital delillerin doğrulanması için kullanacağımız model, açık anahtar altyapısı üzerine inşa edilecek olup, asimetrik kriptografiye dayanacaktır.

4. AAA İLE İLGİLİ PROBLEMLER

Dijital imza ve dijital sertifikaların asıl kullanım alanı, doğrulama ve inkar edememe gibi bilişim güvenliğindeki çok önemli mekanizmaların sağlanmasıdır.

Günümüzde dijital imza kullanımı, e-ticaret, e-sözleşme gibi bir çok e-uygulamanın da temelini teşkil etmektedir. Bu yüzden ülkelerin çoğu, dijital imzanın kabul edilebilirliği konusunda kanunlarında bir takım yasal düzenlemeler yapmıştır. Fakat dijital imza sisteminin dijital delillendirmede tek başına kullanılması, ne yazık ki bu delillere yüzde yüz kesinlik ve doğruluk kazandıramamaktadır. Başlıca nedenler şu şekilde sıralanabilir [7,8]:

- Kapalı anahtarın başka bir kişi tarafından ele geçirilmesi, sistemi tamamen etkisiz kılmaktadır. Dolayısıyla başka birinin kapalı anahtarını ele geçiren birisi onun adına bir takım imzalar atabilir ve dijital imzaya yüzde yüz güvenen bir sistemde kişinin gerçekte ilgili imzayı atmadığını ispatlaması çok zordur.
- Bir dosya sistemi üzerine kayıt edilmiş anahtar, dosya sisteminin güvenliği ölçüsünde güvenlidir. Dosya sistemindeki herhangi bir güvenlik güncellemesinin geç yapılması, saldırganın sisteme sızıp anahtarını çalabilmesi anlamına gelir.
- Eğer anahtar şifreli halde saklanıyorsa, anahtar güvenliği şifreleme algoritmasının güvenliğine eşittir.
- Virüsler, Truva Atları, Arka Kapılar gibi zararlı kodlar bilgisayar üzerinde, kullanıcının bilgisi dışında işlemler gerçekleştirilmekte ve hatta kullanıcının kendi ekranından okuyup onayladığı dosyalar ile gerçekte imzalanan dosyalar birbirinden farklı olabilmektedir. Örneğin bir e-sözleşmeyi ele alırsak 100 000\$'lık bir e-sözleşme virüsler tarafından değiştirilip, kullanıcıya 100\$ şeklinde görüntülenebilir ama asıl imzalanan sözleşme 100 000\$'dır.
- Sertifikanın iptalini gerektiren bir durum oluştuğunda veya süresi dolduğunda sertifikanın efektif bir şekilde nasıl geçersiz kılınacağı da hala tartışılan konulardan biridir [9,10,11]. Mevcut uygulamaların çoğunda sertifika iptali göz önüne alınmamaktadır. Dolayısıyla kullanılan bir dijital sertifikanın o anda geçerli sertifika olup olmadığı bilinmemekte ve bu da dijital delillendirmede problemler oluşturmaktadır.

5. GEÇMİŞTEKİ ÇALIŞMALAR

Maurer dijital delillerle ilgili sıkıntıları gidermek için, 2004 yılında dijital bildirim kavramını vurgulamıştır [12]. Dijital bildirimler, normal kriptografik yöntemlere ek olarak, kişilerin kendileri tarafından oluşturulan ve kişinin olay hakkındaki farkındalığını açıkça belirten fiziksel bir olgunun dijital hale getirilmesidir. Örneğin bir elektronik sözleşmeyi imzalarken sözleşmede hangi tutara imza atıldığını sesli olarak kayıt altına alma veya bir şekilde imzalanacak olan belgeyi video görüntüsü şeklinde kayıt etmek suretiyle elde edilen dijital verilerin, imzalanacak dökümana eklenmesi düşünülebilir.

Beser, Duerr ve Staisiunas 2003 yılında, dijital video görüntülerinin mahkeme esnasında kabul

edilebilirliğini sağlamak adına bir çalışma başlatmışlar ve DVA (Digital Video Authenticator) isminde bir arayüz oluşturarak elde edilen görüntülerin daha sonradan doğrulanmasını ve bütünlüğünün korunmasını sağlamışlardır [13]. Bu arayüz bir dizüstü bilgisayara yerleştirilmiş olup, görüntüyü alacak olan kamera IEEE-1394 seri arayüzü üzerinden bilgisayara bağlanmıştır. Bu kamera bir yandan görüntüyü kasete kaydederken, diğer taraftan da bilgisayara gönderebilmektedir. Kamera görüntüyü kayıt ederken, aynı anda bilgisayara gelen görüntü de DVA programı tarafından ele alınıp, gerçek zamanlı olarak çerçeve çerçeve imzalanarak bilgisayara takılı bir medya üzerine aktarılmaktadır. Sistemde açık anahtar kriptografi kullanılmış olup, açık anahtar kriptografiden kaynaklanabilecek sorunlara ise şu şekilde çözümler düşünülmüştür:

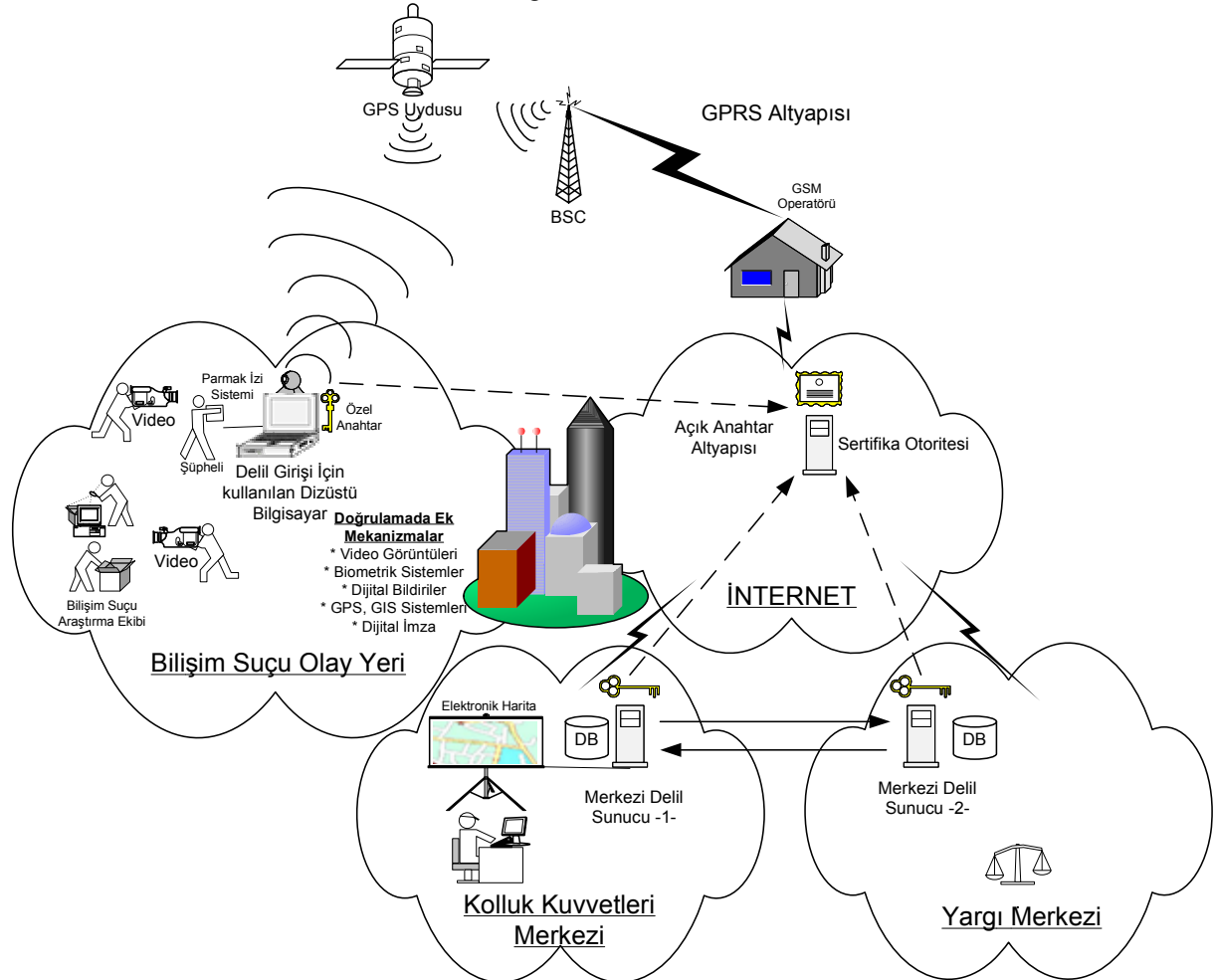
- Bir olay görüntüleneceğinde sistemde kullanılan anahtarlar olaydan hemen önce oluşturulup, olay sonrasında yok edilmekte ve ikinci kez kullanılmamaktadır. Böylelikle anahtarın çalınıp daha sonradan başka biri tarafından kullanılması da mümkün değildir.

Sistem hükümet tarafından oluşturulmuş özel bir AAA üzerine inşa edilmiştir.

- Sistem üzerinde sadece DVA programını çalıştıracak şekilde gömülü bir işletim sistemi hazırlanıp, tamamen güvenli ve virüslerden arındırılmış bir platform oluşturulmuştur.

Geçmişte yapılan bu çalışmalar, dijital delillerle ilgili bir takım meselelerin çözülmesinde oldukça faydalı olmalarına rağmen, olay yerinden toplanan dijital delillerin tümünü doğrulamada yetersiz kalmaktadırlar. Dolayısıyla bizim bu makaledeki amaçlarımız şunlar olacaktır:

- Geçmişteki çalışmalardan yararlanıp, olay yerinden alınan dijital delillerin tümünü doğrulamak için entegre bir çözüm üretilebilir.
- Ürettiğimiz çözümü, herkesin kullandığı bir açık anahtar altyapısı üzerinden fakat açık anahtar kriptografideki sorunların önüne geçerek oluşturabilmek.



Şekil-1. A3D3M – Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli

6. A3D3M MODELİ

Model adli kolluk birimlerini ve yargı mekanizmalarını içine almakta olup, açık anahtar altyapısı üzerine inşa edilmiştir. Fakat önemli özelliklerinden bir tanesi açık anahtar altyapısının dijital delillendirmede kullanılabilmesi için bazı ek mekanizmalarla desteklenmesidir. Bu mekanizmalar GPRS Sistemleri, GPS ve GIS Sistemleri, Biometrik Sistemler, Video Kayıt Sistemi ve Dijital Tutanaklar olacaktır. Şimdi A3D3M'deki bileşenlere ve modelin işleyişine biraz daha ayrıntılı bir şekilde giriş yapalım:

6.1. Altyapıda Kullanılacak Bileşenler

Model şekil 1'de görünen altyapı üzerine inşa edilmiş olup bir çok teknolojiyi içine almaktadır:

6.1.1. GPRS sistemi

GPRS (General Packet Radio Service), GSM'i temel alan, internet üzerinden hızlı veri transferi sağlayan dijital bir mobil telefon teknolojisidir. Modelimizde olay yerindeki dizüstü bilgisayar ile delillerin saklanacağı merkezi veritabanlarına gerçek zamanlı bilgi alış-verişi GPRS üzerinden gerçekleştirilecektir.

6.1.2. GPS ve GIS sistemleri

GPS (Global Positioning Systems) sistemleri, uydu tabanlı dolaşım sistemleri olmakla birlikte günümüzdeki uygulama alanları daha çok vericinin mevki tespiti şeklindedir. GIS (Geographical Information Systems) sistemleri ise, mekandaki konumu belirlenmiş verilerin kapsanması, yönetimi, işlenmesi, analiz edilmesi, modellenmesi ve görüntülenmesi işlemlerinde kullanılır [14]. GIS ve GPS sistemlerinin birlikte kullanılmasıyla, mekan bilgileri ile grafiksel ve sözel verilerin birleştirilmesi sağlanmaktadır.

Emniyet Genel Müdürlüğü bünyesinde yapılan MOBESE isimli projede de GIS ve GPS sistemlerinden yararlanılmıştır [14,15]. Proje çerçevesinde, polis araçlarına GPS modüller yüklenmiş olup, oluşturulan elektronik harita üzerinden araçların buldukları mevki tespit edilmekte, hatta ve hatta araçlar seyir halindeyken hangi hızla nereye doğru gittikleri bile merkezden saptanabilmektedir. Bizim modelimizde ise dijital delillerin toplandığı mevki tespitinde, buna benzer bir sistem kullanılacaktır. GPS modülü olay yerine götürülen dizüstü bilgisayara yerleştirilmiş olup, gelen sinyallere göre merkezde oluşturulan dijital harita yardımıyla mevki tespiti yapılarak elde edilen bilgiler delil bilgi veritabanına eklenecektir. GPS Sistemlerinde mevki tespitinin doğruluğu, kullanılan uydu sayısı ile orantılıdır. Şekil 1'de genel bir çerçevede olayı gösterebilmek adına temsili olarak bir uydu görünmesine rağmen, kesin tespit için (Ör: yaklaşık 1m) en az üç uyduya gerek duyulmaktadır.

Dijital deliller toplandığı anda, gerçek zamanlı olarak sunucu sistemleri üzerinde bulunan veritabanlarına kayıt edilebilecektir. Bizim modelimizde bir tanesi kolluk birimleri içerisinde, bir tanesi de yargı birimlerinde bulunmak üzere iki adet merkez noktası düşünülmüştür. Projeye göre bu merkez noktalarının sayısı artırılabilir.

Delillerin birden fazla veritabanına kayıt edilmesinin amacı, veritabanlarından birinde oluşabilecek herhangi bir sıkıntı (Ör: delil bilgilerinin değiştirilmesi, delillerin bozulması, veritabanının çökmesi) durumunda, diğer veritabanlarından orijinal delil bilgilerine ulaşılabilmesidir.

6.1.3. Biometrik sistemler

Model çerçevesinde kimlik doğrulamada kullanılmak üzere biometrik sistemlerden yararlanılacaktır. Örneğin olay yerindeki dizüstü bilgisayara monte edilmiş yüz tanıma sistemleri veya parmak izi sistemlerinin kullanımı düşünülebilir.

Yüz tanıma sistemleri, bir kişinin görüntüsünden yüz özelliklerini seçebilen ve bu özellikleri daha önceden veritabanına kayıt edilmiş verilerle karşılaştırabilen sistemlerdir. Başarı yüzdeleri kişinin kullandığı aksesuar (gözlük, atkı v.b), ışık, kameranın yüzü görüş açısı gibi bir çok faktöre bağlı olarak değişmektedir. A3D3M'de bu sistemler istemli olarak kullanılacağı için, kişinin yüzünden istenilen açıdan ve istenilen şekilde görüntü alınabilecektir. Dolayısıyla başarı oranı da %100'e çok yakın olacaktır denilebilir [16]. Yinede tamamen garanti sonuçlara ulaşmak için parmak izi sistemleri tercih edilebilir.

6.1.4. Video kayıt sistemi

Operasyon sürecinde olay yerine girilmesinden bitime kadar olan her şey, olay yeri kameramanları vasıtasıyla videoya alınacak ve aynı zamanda alınan bu görüntüler gerçek zamanlı olarak imzalanarak bilgisayara aktarılacaktır (Bu mekanizmada [13] benzeri bir sistem düşünülmüştür).

6.1.5. Zaman sunucusu

Delillerin toplanma zamanına ilişkin doğru zaman bilgisi girebilmek için kullanılacak, güvenilir bir zaman sunucuya ve üretilen zaman damgasının yine AAA çerçevesinde imzalanmış olmasına ihtiyaç vardır [17]. Bu zaman sunucu kendini Greenwich gibi güvenilir bir yerden devamlı senkron halde tutmalıdır.

6.1.6. Dijital sertifika

Bilişim suçları ile mücadelede ve bu suçların yargılama sürecinde yer alan her bireyin ve imzalama yapacak her sistemin açık anahtar alt yapısı çerçevesinde açık ve özel anahtar çifti ve bir sertifika otoritesi (sertifika otoritesinin güvenilirliği konusunda şüphelere yer vermemek için farklı sertifika yolları-certificate paths kullanarak açık anahtar birden fazla

noktadan onaylanabilir) tarafından onaylanmış bir dijital sertifikası olduğunu varsayıyoruz.

6.1.7. Dijital tutanaklar

A3D3M çerçevesinde olay yerinden elde edilen dijital delillere, Maurer'in öne sürdüğü dijital bildirim benzeri görevlilerin kendi tuttıkları olay yeri tutanaklarını da eklenecektir. Yapılan bütün işler, elde edilen tüm deliller bu tutanaklara el ile yazılacaktır. Daha sonra ilgili tutanaklar tarayıcı vasıtasıyla taramıp imzalanacak olan nesnelere eklenecektir. Böylelikle dijital imza kullanılarak doğrulanmış deliller, tutanaklar vasıtasıyla da onaylanmış olacaktır.

6.1.8. Delil giriş programı

Modeldeki çekirdek nokta, dizüstü bilgisayar üzerine yerleştirilmiş olan delil giriş programıdır. Bu programın arayüzünde delillerle ilgili, delili bulan görevlinin bilgileri, delilin tipi, özellikleri, delilin ait olduğu operasyon bilgileri gibi bir takım verilerin girişi yapılır. Giriş esnasında ilgili kişilerin özel anahtarları vasıtasıyla delillerin kriptografik olarak özetleri alınarak, gönderilecek diğer bilgilere eklenmek suretiyle, bütün veriler GPRS bağlantısı üzerinden merkezi veritabanlarına aktarılır.

6.2. Modelin İşleyişi

Olay yerine girişten itibaren, yapılan bütün işlemler olay yeri kameramanları vasıtasıyla videoya alınırken bir taraftan da görüntüler kriptografik olarak imzalanarak (kameramanların özel anahtarları vasıtasıyla) bilgisayara aktarılmaya başlar. Bilişim suçu olay yeri araştırma ekibi, delillerin toplanması için gerekli çalışmalarını başlatır.

Olay yerine götürülen dizüstü bilgisayar gerekli olan bütün aparatlarıyla birlikte çalışır hale getirilir. Delilleri toplamada kullanılacak olan program başlatılır. Programda yeni bir suç olayı oluşturulduktan sonra, şüpheli özellikleri bölümüne gelinerek o anda olay yerinde bulunan şüphelilerin bilgisayara takılı parmak izi alım cihazı kullanılmak suretiyle teker teker parmak izleri alınır.

Bilişim suçları araştırma ekibi, delillere zarar gelmemesi için gerekli bütün işlemleri yaptıktan ve o anda delil olarak alınabilecek materyalleri tespit ettikten sonra, delillerin programa giriş aşaması başlar.

Deliller fiziksel veya dijital formatta bulunabilir. Bu yüzden delillerin giriş aşaması dijital ve fiziksel delillerin girişi olarak iki farklı alanda ele alınabilir:

Dijital Delillerin Girişi: O anda olay yerinde doğrudan ele geçirilen dijital deliller (Ör: Bilgisayar sistemleri üzerindeki uçucu bilgiler v.b.) dizüstü bilgisayarda bulunan programa giriş yapılır. Delillerin girişinden önce program, delili toplayan görevliden çeşitli girdiler alır. Örneğin giriş yapacak olan görevli

öncelikle sisteme parmak izini verir, daha sonra akıllı kartını sisteme bağlar ve son olarak bir kullanıcı adı ve şifre girebilir. Bu esnada yapılan bütün işlemler olay yeri kameramanları vasıtasıyla kayıt altına alınmaya devam etmektedir (Şekil 1: Bilişim suçları olay yeri). Giriş yapacak olan kişinin doğrulanması için gerekli işlemler bittikten sonra, deliller ve delillerle ilgili bilgiler programa giriş yapılır.

Fiziksel Delillerin Girişi: Delillerin bir çoğu olay yerinde incelenmeyip, delilleri barındıran materyaller daha sonradan uygun ortam koşullarında incelenmek üzere alınır. Ama sonuç olarak bütün delillerin nereden, ne zaman, kimlerden ve kim tarafından alındığının doğrulanması gerekmektedir. Bu yüzden fiziksel olarak ele geçirilen delillere yönelik dijital bilgiler oluşturularak sisteme giriş yapılır. Öncelikle delil olarak kullanılacak fiziksel öğelerin (Örneğin Harddisk) yakın plandan teker teker fotoğrafları çekilir. Fotoğraf aşaması bittikten sonra, ele geçirilen materyallerin teknik olarak özetleri (Hash) alınabiliyorsa, olay yerine getirilmiş olan ekipmanlar vasıtasıyla materyallere en ufak bir müdahale olmadan özetleri alınır. Bu esnada video kaydının da devam ettiği unutulmamalıdır. Video kaydındaki dikkat edilecek olan nokta fiziki deliller üzerindeki seri numarası gibi özel yerlerin büyütülerek, net bir şekilde kayıt altına alınabilmesidir. Görevlilerin tuttıkları tutanakların, fiziksel delillerin toplanmasında ayrı bir önemi vardır. Programa girişten önce yine delilleri ele geçiren görevliye ait bazı girdiler (parmak izi) alınır. Daha sonra delile ait fotoğraflar, varsa delillin teknik olarak özeti, seri numarası, markası gibi bütün özellikler, programa giriş yapılmalıdır.

Deliller ile ilgili bilgiler, programa aktarıldıktan sonra giriş düğmesine tıklanıldığında, sistem ilk olarak tanımlı olan zaman sunucuya bağlanarak o anki zamanı alır ve ilgili delilin toplandığı zaman olarak hafızasına kaydeder, daha sonra programa giriş yapılan bütün bilgileri (Delilin niteliği, hangi operasyonda toplandığı, kim tarafından toplandığı v.b.), zaman bilgisi, delilleri giriş yapan görevlinin parmak izi ve dijital hale getirilmiş fiziksel veriler (fotoğraf, delil ile ilgili video görüntüleri, dijital tutanaklar) ile birleştirir. Dedektifin akıllı kartında bulunan özel anahtar vasıtasıyla, birleştirilmiş olan bütün bu verilerin özeti alınır ve girilen bilgiler ile birlikte GPRS üzerinden merkeze iletilir. Akıllı kart içerisinde bulunan ve özet almada kullanılacak olan özel anahtarın güvenlik açısından dışarıya çıkarılmaması gerekir. Günümüzde, bazı akıllı kartlar sayesinde imzalama işlemi bizzat akıllı kart içerisinde gerçekleştirilebilmektedir [18].

Merkeze gelen verilerin giriş yapıldığı mevkinin adresi, GPS sistemi vasıtasıyla tespit edilir (Yer bilgisi ayrı yeten program üzerinden olay yerinde kayıt altına alınmıştır.) ve delille ilgili diğer bütün bilgiler ile birlikte hem kolluk kuvvetlerinde bulunan merkezi

sunucuya, hem de yargı tarafında bulunan merkezi sunucuya olay ismi ve sistem tarafından atanan olay numarasından ulaşılabilecek şekilde kayıt edilir.

Delillerin teker teker gönderilmesi bittikten sonra olay yerinde elde edilen bütün delillerin özelliklerinin yazılı olarak bulunduğu imzalı tutanaklar da tarayıcı vasıtasıyla dijital hale getirilip, olay esnasında çekilen video görüntülerine eklenmek suretiyle programa giriş yapılır. Program son olarak bu görüntüleri ve tutanakları, daha önceden giriş yapılan şüphelilerin parmak izleri, olaya katılan bütün görevlilerin parmak izleri ile birleştirir ve hepsini birden programın kendi özel anahtarıyla son defa özetini alarak merkeze giriş yapar. Böylelikle hem delillerin teker teker özetleri, hem de operasyona ait genel bir özet alınmış olur.

Delillerin dijital olarak sisteme girişi tamamlandıktan sonra, bütün deliller (fiziki ve dijital) uygun şekilde paketlenip, her hangi bir zarara uğramayacak şekilde merkeze iletilir. Merkezde, ele geçirilen delillerin incelenmesi esnasında olay yerinde gerçekleştirilen mekanizmanın aynısı kullanılır ve elde edilecek yeni delillerin sisteme girişi yapılır.

Alt yapıda aynı zamanda bütün uç birimler ile merkezler arasında bir VPN (Virtual Private Network) inşa edilmiştir. Doğrulamanın dışında, merkezi veritabanına gönderilecek kritik bilgiler VPN tüneli içerisinden şifreli bir şekilde merkeze iletelebilmektedir. Ayrıca unutulmaması gereken diğer bir husus da modelin kendi güvenliğidir. Örneğin merkezi veritabanlarının güvenliği, kullanılan programların, işletim sisteminin, metotların, prosedürlerin ve kriptografik algoritmaların güvenliği de mutlaka ele alınmalıdır.

7. MODELİN SAĞLADIKLARI

Modelin sağladığı faydalar, şu başlıklar altında incelenebilir:

7.1. Delillerin Kimlerden ve Kim Tarafından Toplandığının Doğrulaması ve İnkâr Edilememesi

A3D3M'de delillerin kimlerden ve kim tarafından toplandığının doğrulanması ve inkâr edilememesi için bir çok doğrulama mekanizması iç içe kullanılmıştır. Örneğin olay yerindeki şüphelilerin parmak izleri (yüz özellikleri de olabiliyordu) sisteme girilmiştir. Parmak izlerinin alınma safhası, kamera vasıtasıyla kayıt altına alınmıştır. Elde edilen delillerdeki özetlerden, toplayan dedektifin açık anahtarı ile bu bilgilerin değişip değişmediği anlaşılabilir. Dolayısıyla bu şartlar altında şüphelinin o esnada orada olmadığını savunacak bir durum bulmak çok zor olacaktır.

Yine delilleri toplayan ve sisteme giriş yapan görevliler de, hem parmak izi, hem açık anahtarları (akıllı kart vasıtasıyla özel anahtarlarını

kullanmışlardı.) hem de sisteme giriş kayıtları vasıtasıyla doğrulanabileceklerdir¹. Yine bu doğrulama hem video görüntüleriyle, hem de kişilerin el yazısıyla oluşturdukları tutanaklar vasıtasıyla daha da desteklenmiş olacaktır. Doğrulamada dijital imzalara birden fazla fiziksel nesne de katıldığından kapalı anahtarın her olaydan sonra silinip tekrar oluşturulmasına gerek kalmayacaktır. Bu şartlar altında delili sisteme giriş yapan görevlinin de olayı inkâr etmesi çok zordur.

7.2. Delillerin Nereden ve Ne Zaman Toplandığı

Delillerin toplandığı yer GPS ve GIS sistemlerinin kullanımı ile otomatik olarak tespit edilmekle birlikte, tutanaklarda ve delillerin giriş yapıldığı programda da bulunmaktadır.

Delillerin toplanma zamanı, zaman sunucu kullanılarak otomatik bir şekilde delil bilgilerine eklenmektedir. Bunun dışında yine hazırlanan tutanaklarda ve programa yapılan manuel girişlerde zaman bilgisi mevcuttur.

7.3. Delillerin Toplandığı Andan İtibaren Değişmediğinin İspatı

Toplanan bütün deliller, olay yerinde özetleri alınmak suretiyle, merkezi veritabanlarına kayıt edilmektedir. Örneğin olay yerinde bulunan bir harddisk'in doğrudan özeti alındığı gibi, o anda elde edilen dijital verilerin de bilgisayara giriş yapmak suretiyle özetleri alınır. Özetleri alma işlemi esnasındaki video görüntüleri ve tutanaklar da doğrulamayı pekiştirmesi açısından alınan delil bilgilerine eklenmektedir. Dolayısıyla bütün prosedürler fiziksel olarak izlenip, tutanaklardan takip edilebileceği için, açık anahtar altyapısı ile ilgili öne sürülebilecek herhangi bir iddia da yargılama esnasında çok geçerli olmayacaktır. Bu özetler daha sonradan tekrar alınmak suretiyle, deliller üzerinde herhangi bir değişiklik yapıp yapılmadığı ortaya çıkarılabilir.

Ayrıca elde edilen bütün deliller, delillerle ilgili bilgiler ve özetler hem kolluk kuvvetlerinde hem de yargı da olduğu için, polislin de elde edilen delilleri değiştirdiği iddiası incelenebilecektir.

7.4. Delillerin Doğruluğu

Dijital delillendirmedeki çok önemli noktalardan birisi de dijital delillerin ele geçirilmesi esnasında kullanılan teknikler, bilgiler, programlar ve uygulanan metot ve prosedürlerin doğruluğunun ispatıdır.

¹ Delil gönderme programı güvenilir ve özel oluşturulmuş bir işletim sistemi üzerine inşa edilmiş olup, girişler dedektiflerin akıllı kartı ve giriş için olay ile ilgili kendilerine verilen kullanıcı adı ve şifre ile sağlanmaktadır. Ayrıca bütün giriş ve işlemler programın kayıtlarına eklenmektedir.

Bunun için modeldeki bütün bileşenler, dünya çapında bilinen, güvenilen ve kabul görmüş bir kurum tarafından sertifikasyona tabi tutulmalıdır.

7.5. Delillerin Sonradan Ele Alınabilirliği

Modelde deliller gerçek zamanlı olarak iki ayrı sunucuya birden kayıt edilmektedir. Bu sunuculardan birisi kolluk kuvvetlerinde, diğeri de yargı birimindedir. Modeldeki bütün süreçler doğru bir şekilde yerine getirildiği takdirde, ele geçirilen deliller ve sistemin güvenilirliği çok kolay bir şekilde üçüncü bir şahıs tarafından incelenebilecektir.

8. SONUÇ

Bilişim suçlarındaki en sıkıntılı noktalardan birisi, bir olayda elde edilen dijital delillerin mahkeme esnasında kabul edilebilirliğidir. Dijital delillerin gerçek delil özelliği gösterebilmeleri için ilk toplandıkları andan itibaren hiçbir şekilde değiştirilmediğinin, kimlerden ve kim tarafından, nerede ve ne zaman toplandığının doğrulanması ve inkar edilememesi gerekmektedir. Günümüze kadar bu tip konular kriptografi bilimi altında incelenmiş olup, mevcut çözümler içerisinde dijital delillere kesinlik kazandıracak entegre bir mekanizmaya rastlanılmamıştır.

Dijital delillerin mahkeme esnasında kabul edilebilirliğini sağlamak için sadece doğrulamada kullanılacak teknik yöntemler yeterli değildir. Delillerin incelendiği laboratuvarın standartlarının delil incelemeye uygun olup olmadığı, kullanılan araç, gereç ve yöntemlerin uygunluğu gibi başka bir çok konunun da değerlendirilmeye alınması gerekmektedir. Bu yüzden bilişim suçlarıyla mücadele eden birimler için uluslar arası standartların belirlenerek, bu standartların uygulamaya konulması çok büyük önem arz etmektedir.

Aynı zamanda bilişim suçları kapsamında elde edilen deliller sadece olay yeri ile sınırlı değildir. Olay yerine gidilmeden de örneğin İnternet kullanılarak bir çok delil elde edilmektedir. Biz bu makalede dijital delillerin kabul edilebilirliği konusundaki bütün prosedürlere değil de, daha çok operasyon esnasında ve sonrasında elde edilen dijital delillerin teknik olarak doğrulanması, bütünlüğünün sağlanması ve inkar edilememesini sağlamak için bir model geliştirdik. Model iyi bir şekilde uygulandığı takdirde her ne kadar bütün dijital delillerin kabul edilebileceği anlamına gelmese de, operasyon esnasında ele geçirilen ve incelenen dijital delillerin kabul edilmesi yönünde büyük kesinlik sağlayacağı inancındayız.

A3D3M, dijital delillerin doğrulanmasında entegre bir çözüm olarak öne sürülmüş ilk modeldir ve geniş bir

topolojiye sahiptir. Konu olarak çok geniş boyutları mevcuttur. Bu makalede aslında geleceğe yönelik çalışmalara ışık tutabilmesi açısından bir giriş modeli oluşturulmaya çalışılmıştır. Model bir çok yönden geliştirilmeye açıktır. Özellikle modelin güvenliğini ve performansını daha da arttırmak adına farklı mekanizmalar sisteme entegre edilebilir.

KAYNAKLAR

- [1] Shinder, D. L., Scene of Cybercrime, USA, 2002
- [2] Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 2nd Ed., Academic Press, 2004
- [3] Uzunay, Y., Koçak M., "Bilişim Suçları Kapsamında Dijital Deliller", AB'05 Gaziantep, Şubat 2005
- [4] Stallings, W., Network Security Essentials Applications and Standarts, New Jersey, Prentice Hall, 2002
- [5] Diffie, W., Hellman, M.E., "New Directions in Cryptography", *IEEE Trans. Information Theory*, vol.22, no.6, 1976
- [6] Shamir, R.L., Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems", *ACM*, vol.21, 1978
- [7] Caloyannides, M.A., "Digital Evidence and Reasonable Doubt", IEEE Comp.Society, 2003
- [8] Oppliger, R., Rytz, R., "Digital Evidence: Dream and Reality", *IEEE Computer Society*, 2003
- [9] Kocher, P., "A quick introduction to certificate revocation trees (crts).
- [10] Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C., "X.509 internet public key infrastructure – online certificate status protocol - ocsps", IETF, RFC 2560, June 1999.
- [11] Bicakci, K., Crispo, B., Tanenbaum, A.S., "How to Incorporate Revocation Status Information into the Trust Metrics for Public-Key Certification", *SAC'05, ACM*, March 2005
- [12] Maurer, U., "New Approaches to Digital Evidence", *Proceedings of the IEEE* Vol. 92, No.6 June 2004
- [13] Beser, N.D., Duerr, T.E., Staisiunas, G.P., "Authentication of digital video evidence", *SPIE*, San Diego, California, August, 2003.
- [14] Demirci, S., "Emniyet Teşkilatında Coğrafi Bilgi Sistemlerinin Uygulanabilirliği", *1.Polis Bilişim Sempozyumu*, 2003
- [15] MOBESE Web Site, <http://www.mobese.com>
- [16] Kepenekci, B., Boray, F., "GAYE: a face recognition system", *Image Processing: Algorithms and Systems III*, San Jose, 2004
- [17] Hosmer, C., "Proving the Integrity of Digital Evidence with Time", *IJDE*, Spring 2002 Vol.1
- [18] Fratto, M., "Security Tokens", August, 2001