Sayısal Veri ve Kaynak Kodu Emanetçilik Sistemi

Meriç Yücel[1] Burak Berk Üstündağ[2]

[1]Ulusal Yazılım Sertifikasyon Merkezi, İstanbul Teknik Üniversitesi, İstanbul

[2]Bilgisayar Mühendisliği Bölümü, İstanbul Teknik Üniversitesi, İstanbul

[1]e-posta: mericyucel@gmail.com [2]e-posta: berk@berk.tc

Özetçe

Bu bildiride, İstanbul Teknik Üniversitesi Ulusal Yazılım Sertifikasyon Merkezi'nin (UYSM) hizmetlerinden biri olan sayısal veri ve kaynak kod emanetçiliği anlatılmaktadır. Kaynak kod emanetçilik sistemi doğası gereği güvenlik, güvenilirlik ve gizlilik koşulları altında fikri mülkiyet sahibi ve kullanıcı arasındaki ilişkinin bağımsız bir platformda yönetilmesi üzerine kuruludur. Bu amaçla uçtan uca kriptolu bir kayıt sistemi ile yüklenmiş dosyalar, çift anahtar mekanizması ile yönetilmekte ve hukuki bir sözleşme referansıyla eşleştirilmektedir.

1. Giriş

Yedieminlik, iki taraf arasındaki, yasal bir doküman ya da sözleşme ile bağlanan genel bir anlaşmanın, iki tarafında güvendiği bağımsız üçüncü bir tarafın güvencesi altında, sözleşmedeki koşullar gerçekleşene kadar saklanması olarak tanımlanabilir [1]. Sayısal kaynak kod emanetçiliği ise en basit tanımı ile bu anlaşmanın yazılım kaynak kodu için yapılmasıdır.

Bilgisayar programları temel olarak kaynak kodu ve derlenmiş koddan (çalıştırılabilir kod) oluşmaktadır [1]. Kaynak kod, programcı tarafından belirli bir dilde yazılan ve bir metin editörü ile açılıp, yazıldığı programlama dilini bilen biri tarafından okunabilen koddur. Derlenmiş kod ise, 0 ve 1'lerin kombinasyonu olan ve bilgisayar tarafından okunabilen koddur. Günümüzde açık kaynak kodlu yazılımlara rağbet hızla artsa da, yazılım piyasasındaki lisanslı ürünlerin birçoğu sadece derlenmiş kod olarak satılmaktadır. Birçok yazılım eser sahibi eserlerinin kaynak kodlarını korumak ister ve müşterileri ile paylaşmaz, yazılımlarını korumak için de ciddi önlemler alır. Ayrıca, yazılımların değişen donanım ve ihtiyaçlara cevap verebilmesi için sürekli güncellenmesi gereklidir. Birçok yazılım firması bu ihtiyacı karşılar ve sürdürülebilir yazılım üretmeye gayret eder [1,2].

Yazılım üretici firmaların bir sebepten dolayı işlerine devam edememesi durumunda, yazılım müşterisi satın aldığı yazılım için ihtiyaçları doğrultusunda güncellemelerden yararlanamaz, olası program hatalarına müdahale edemez vb. çeşitli sorunlarla karşılaşır. Bu gibi sorunlarla karşılaştığında yazılım kaynak koduna erişmek ister. Yedieminlik sayesinde güvenilir bir üçüncü tarafta saklı tutulan kaynak kodu yazılım müşterisi tarafından erişilir olur [1,2,3].

1.1. Amaç

Yazılım endüstrisinin gelişmesindeki en önemli etkenlerden biri, yazılım üreticisi ile müşterisi arasındaki karşılıklı güvenin sağlanarak, üretilen yazılımların satılabilmesine dayanır. Sayısal kaynak kod emanetçiliğinin zaruri bir ihtiyaç olmasının iki temel sebebi vardır. İlki, yazılım üreticilerinin fikri mülkiyetlerindeki yazılımları korumak istemeleri, diğeri ise yazılım müşterilerinin iş sistemlerini üzerine kurguladıkları yazılımların sürdürülebilirliğini garanti altına almak istemeleridir [3,4]. Özellikle, müşteriye özel yazılımların geliştirildiği ve sürdürülebilirliğin önemli olduğu finans sektörü, askeri uygulamalar vb. alanlarda kaynak kodu güvencesi çok önemlidir. UYSM, 256 bit kriptolu, çift anahtar korumalı, sayısal kaynak kod emanetçilik sistemini geliştirerek, ülke içinde yazılım piyasasındaki güvensiz ortamı ortadan kaldırmayı, yazılım müşterisinin olası mağduriyetlerini engellemeyi ve yazılım eser sahibinin fikri mülki haklarını güvence altına almayı hedeflemektedir.

2. Kaynak Kod Emanetçiliği

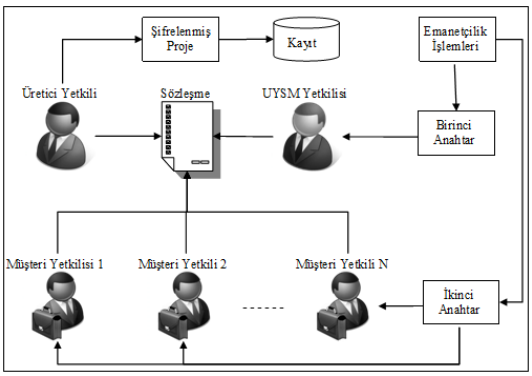
Kaynak kod emanetçiliğinin işleyişi, süreçleri, çözümleri ve çeşitleri bu bölümde anlatılmıştır.

2.1. Kaynak Kod Emanetçiliği Çeşitleri

UYSM'de kaynak kod emanetçiliği süreli ve/veya sözleşme denetimli olarak Kamu Kaynak Kod Emanetçiliği ve Özel Kaynak Kod Emanetçiliği olarak ikiye ayrılır.

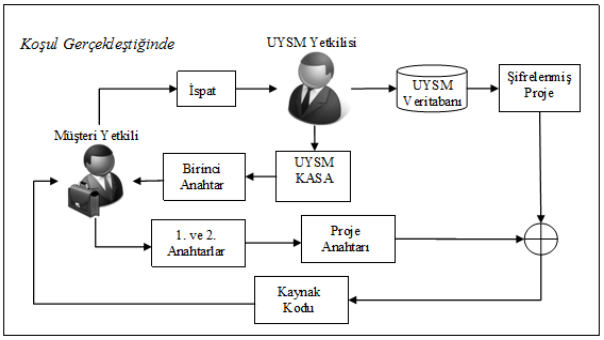
2.1.1. Kamu Kaynak Kod Emanetçiliği

Yazılım üreticisinin, özel bir müşteri için değil de, birden fazla müşteri için ürettiği programlar için kullanılan kaynak kod emanetçiliği biçimidir. Kaynak kod emanetçilik sözleşmesi, kağıt üzerinde UYSM ve yazılım üreticisi arasında yapılır. Yazılımı satın alan firmalar UYSM'ye Emanetçi müşterisi olarak kaydolurlar. Yazılım üreticisi tarafından yazılım eseri bir anahtar dosyası ile şifrelenir ve bu anahtar dosyasından iki alt anahtar oluşur. Bu alt anahtar dosya parçalarının biri UYSM'ye; diğeri ise yazılımı satın alan her müşteriye, yazılım üreticisi tarafından UYSM web sitesi aracılığı ile gönderilir.



Şekil 1: Kamu kaynak kodu emanetçiliği

Sözleşme koşullarındaki kaynak kod devir hallerinin gerçekleşmesi durumunda, müşteriler ilgili kanıt (mahkeme kararı) ile UYSM'ye başvurarak şifrelenmiş dosyayı ve UYSM'deki anahtar parçasını UYSM'den alırlar (Mahkeme tarafından atanan bilirkişi üzerinden de bu işlemler yapılabilir). Kendi anahtar parçaları ile bu anahtar parçasını UYSM tarafından özel olarak verilen bir program ile birleştirerek dosya anahtarını elde ederler. Elde edilen dosya anahtarı ile şifrelenmiş veriyi çözüp, kaynak koduna erişim sağlarlar.

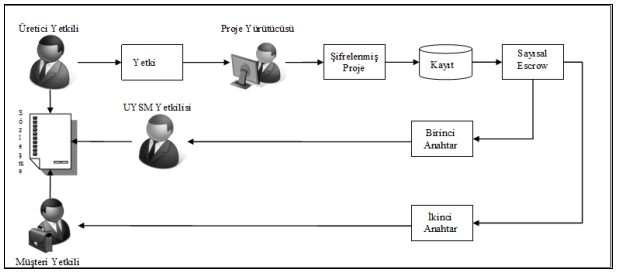


Şekil 2: Kamu kaynak kod emanetçiliği (koşul gerçekleştiğinde)

Kamu kaynak kod emanetçiliği, özel kaynak kod emanetçiliğin çok taraflı müşteri ile yapılmasıdır ve bölüm 2.1.2 ile başlayan bölümlerde anlatılan özel kaynak kod emanetçiliğini ve sistemin işleyişi ile ilgili tüm özelliklerini içermektedir.

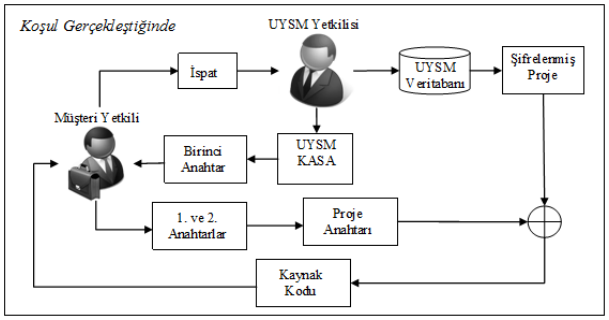
2.1.2. Özel Kaynak Kod Emanetçiliği

Özel kaynak kod emanetçiliği 3 taraflı ve 4 taraflı olarak yapılmaktadır. Sözleşme denetimi altında 3 taraflı özel kaynak kod emanetçiliğinde taraflar yazılım eser sahibi, yazılım müşterisi ve UYSM'dir. 4 taraflı sözleşmede, kaynak kodunun denetimi ve UYSM'de saklanan kaynak kodunun derleme sonucu oluşan çıktısının ürüne eşdeğerliğini belirlemek için tarafların üzerinde uzlaştığı, bağımsız bir denetçi sözleşme tarafı olarak seçilir. Bağımsız denetçiye yazılım eser sahibi tarafından yazılım anahtar dosyası verilir ve bu anahtar dosya ile denetçi kaynak koduna erişerek, eşdeğerlik analizi üzerine çalışma yapar.



Şekil 3: 3 taraflı özel emanetçilik

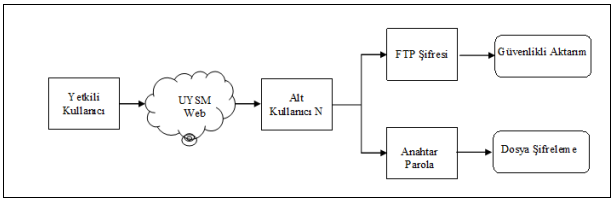
Şekil 3'de 3 taraflı özel emanetçilik süreci özetlenmiştir. Yazılım eser sahibi, yazılım müşterisi ve UYSM arasında kâğıt üzerinde yapılan bir sözleşmeden sonra yazılım üreticisi UYSM tarafından verilen bir program aracılığı ile bir anahtar dosya ile yazılım projesini şifreleyip UYSM veritabanında saklar. Bu anahtar dosyadan iki alt anahtar dosya parçası oluşur. Yazılım üreticisi tarafından bu anahtarlardan biri UYSM'ye, diğeri ise yazılım müşterisine gönderilir. Sözleşmedeki kaynak kodu devir hükümleri gerçekleştiğinde Şekil 2'deki gibi yazılım müşterisi sözleşme şartlarının gerçekleştiğini ispat ederek (mahkeme tutanağı) kaynak koduna erişim hakkı talep eder. UYSM veritabanından ilgili yazılım ve UYSM'deki anahtar parçası yazılım eser sahibine teslim edilir. Yazılım müşterisi elindeki anahtar dosya parçası ile UYSM'dekini birleştirerek dosya anahtarını elde eder ve bu dosya anahtarı ile şifrelenen veriyi çözerek yazılım kaynak koduna ulaşır.



Şekil 4: 3 taraflı özel emanetçilik (koşul gerçekleştiğinde)

2.2. İşlem Süreci

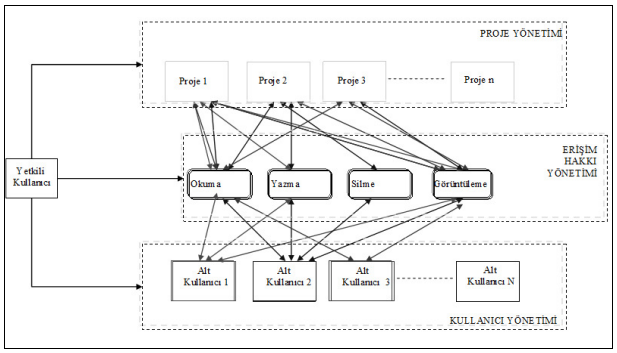
Kaynak kod emanetçiliğinde yazılım eser sahibi işlemleri, web sitesi işlemleri (Yetkili Kullanıcı) ve alt kullanıcı işlemleri olmak üzere iki ana bölüme ayrılır. Yetkili kullanıcı işlemleri web sitesi üzerinden gerçekleşir. Alt kullanıcı işlemleri ise UYSM tarafından web sitesi üzerinden indirilen özel bir yazılım ile gerçekleşir. Alt kullanıcı işlemleri tamamı yetkili kullanıcı tarafından verilen izinler ve kısıtlar çerçevesinde gerçekleşir.



Şekil 5: UYSM yetkili kullanıcı işlemleri

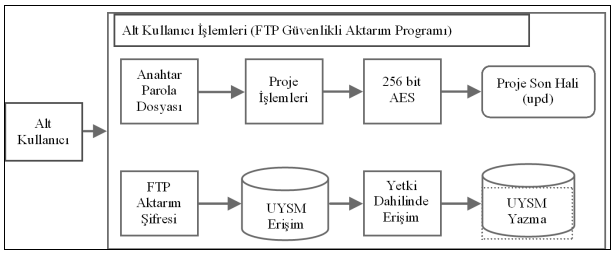
Şekil 5'de gösterildiği üzere yetkili kullanıcı web sitesi üzerinden alt kullanıcılarını oluşturur ve bu kullanıcıları için bir anahtar dosyası ve bir FTP şifresi tanımlar. FTP şifresi UYSM veritabanına güvenlikli olarak bağlanmak için; anahtar parola ise yazılım eserlerinin şifrelenmesi için kullanılır.

Yetkili kullanıcı web sitesi üzerinden proje dosyaları ve alt kullanıcılar tanımlar. Kullanıcılar ve projeler arasında Okuma, Yazma, Silme ve Görüntüleme haklarını atayarak, ayrık projelerde hiyerarşik bir düzende çalışanlarının yetki sınırlarını belirler. Şekil 6'da proje yönetimi, alt kullanıcı yönetimi ve erişim hakkı yönetimi gösterilmiştir.



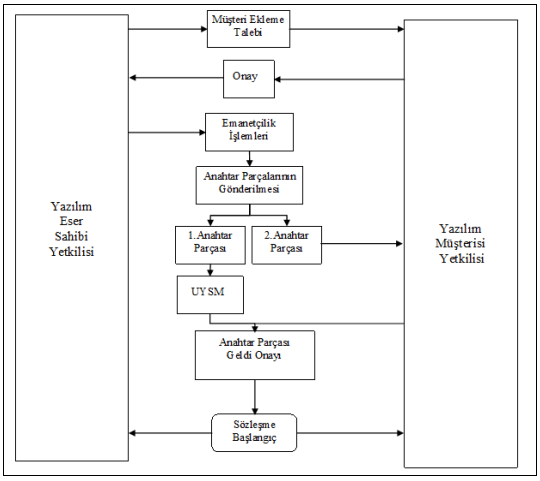
Şekil 6: Yetkili kullanıcı işlemleri

Alt kullanıcılar yetkili kullanıcı tarafından tanımlanan haklar çerçevesinde yerel bilgisayarlarında proje dosyaları oluşturabilir, bu proje dosyalarını UYSM veri tabanına kaydedebilirler. Dosya anahtarları ve FTP güvenlikli aktarım şifreleri ile bu işlemleri gerçekleştirirler. Alt kullanıcı işlemleri Şekil 7'de gösterilmiştir.



Şekil 7: Alt kullanıcı işlemleri

Alt kullanıcı, kaynak kodunu anahtar dosya ile şifreleyip UYSM veri tabanına yazdıktan sonra yetkili kullanıcı tarafından web üzerinden ilgili proje dosyası bir daha değiştirilmeyecek şekilde sonlandırılır. Sonlandırılan proje sadece oku şeklini alır ve hiçbir yetkideki kullanıcı tarafından içeriği değiştirilemez. Bu aşamadan sonra, kağıt üzerinde taraflarca imzalanan sözleşme referans alınarak web üzerinden yazılım eser sahibi, yazılım müşterisi ve UYSM taraflarınca paralel olarak yürütülen bir işlem ile kaynak kodu emanetçilik anlaşması geçerlilik kazanır.



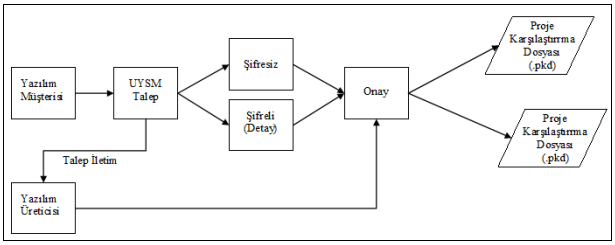
Şekil 8: Emanetçilik sözleşmesi web üzerinden 3 taraflı süreç

Şekil 8'de gösterildiği gibi yazılım eser sahibi yetkilisi web üzerinden, UYSM sistemine emanetçilik müşterisi olarak kayıt olan kullanıcılar arasından sorgu ile yazılım müşterisi firmayı bulur ve bu firmaya emanetçilik sözleşmesi için ilgili proje dosyasına dair müşteri ekleme talebi gönderir. Yazılım müşterisi firma yetkilisi web üzerinden bu isteği görür ve ancak talebe olumlu onay verdiği durumda yazılım eser sahibi tarafı işlemlere devam edebilir. Bir arayüz ekranında emanetçilik alt anahtar dosyalarını doldurur ve sistem tarafından otomatik atanan sözleşme referans numarası ile emanetçilik işlemlerini gerçekleştirir. Bu işlemler sonunda alt anahtarlardan biri UYSM'ye gelir, diğeri de UYSM'de kaydı tutulmaksızın yazılım müşterisi tarafına gönderilir. Anahtar parçalarını alan UYSM ve yazılım müşterisi web sitesi üzerinden ilgili anahtar parçalarını aldığına dair onay verdiği anda, emanetçilik sözleşmesi işlemleri sona erer ve sözleşme geçerli duruma gelir.

Anahtar dosyanın UYSM'de saklanmaması ilgili konu hakkındaki birçok patentten UYSM'nin sisteminin farkını göstermektedir. Çoğu sayısal kod emanetçilik sisteminde ve bu konudaki patentlerde çift anahtarlı korumadan ziyade şifrelenmiş verinin anahtarı sayısal emanetçi garantör tarafında kalmakta ve bu da yazılım üreticisinin, garantör tarafın kaynak koda erişim sağlayabiliyor olması bakımından güvenlik kaygısı duymasına sebep olmaktadır.[3,4]

2.3. Dosya İçerik Eşleme

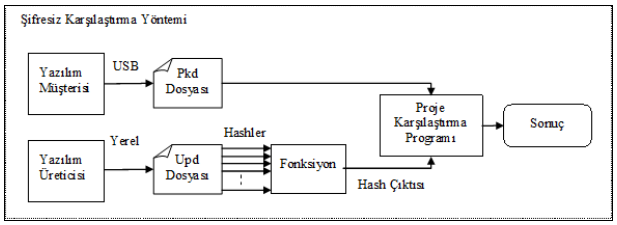
Şifrelenen ve emanetçilik için UYSM veritabanına kaydedilen verinin içeriğini sadece yazılım eser sahibinin bilmesinden ötürü, yazılım müşterisi, dosya içeriğinin eşliğini kontrol etmek istemesi olasıdır. Bu durumda yazılım müşterisi UYSM'ye talepte bulunur. Eşlik karşılaştırma işleminin şifreli ve şifresiz olarak iki yöntemi vardır.



Şekil 9: Dosya içerik eşleme talebi

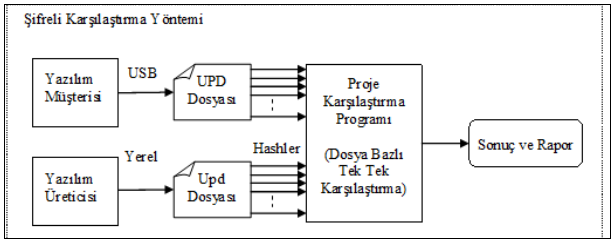
UYSM talebi yazılım eser sahibine iletir ve yazılım eser sahibinin onayı ile Şifreli karşılaştırma için UPD uzantılı veritabanında kayıtlı UYSM Proje Dosyasına erişim hakkı; şifresiz karşılaştırma için ise UYSM Proje Karşılaştırma Dosyası yazılım müşterisine verilir.

Şifresiz karşılaştırma işlemi, şifrelenmiş Ulusal Yazılım Sertifikasyon Merkezi Proje Dosyası'ndaki tüm dosyaların özütlerinin (Hash) fonksiyonu ile karşılaştırma yapar. UYSM'den alınan Proje Karşılaştırma Dosyası (pkd) ile yazılım eser sahibinin yanına gidilir. Yazılım eser sahibinin oluşturduğu projeyi tekrar oluşturması istenir. Yerel bilgisayarında ilgili kaynak kodları ile tekrar proje oluşturulduktan sonra Dosya Karşılaştırma Programı ile özüt fonksiyon çıktılarının iki dosya arasında aynılığı kontrol edilir. Tek bir dosyanın dahi farklı olması durumunda projenin aynı olmadığı sonucuna ulaşılır.



Şekil 10: Şifresiz eşlik karşılaştırma

Dosya bazlı detay karşılaştırma için yazılım eser sahibi tarafından bir anahtar dosya ile şifrelenen dosyaya müşterinin erişimi sağlanır. Yazılım eser sahibi yerel bilgisayarında tekrardan proje dosyasını oluşturup, her iki dosyanın da anahtar dosyasını girerek dosya içeriğine erişim sağlar. UYSM tarafından yazılım müşterisine verilen proje dosyası karşılaştırma programı ile proje içindeki her dosyanın boyut, tür, dosya adı gibi özellikleri ve özütleri tek tek karşılaştırılır. Program, detaylı bir karşılaştırma sonuç dosyasını çıktı olarak kullanıcılara verir.



Şekil 11: Şifreli eşlik karşılaştırma

4 taraflı özel emanetçilik anlaşmasında 4. taraf olarak atanan yazılım eser sahibi ve yazılım müşterisinin güvendiği bağımsız denetçi kişi anahtar dosya erişim hakkına sahip olarak bu işlemleri gerçekleştirebilmektedir.

2.4. Dosya Güncelleme

Emanetçilik anlaşmasındaki yazılım kaynak kodu, süreç başlamadan önce dosyanın değişmezliğinin sağlanması için sonlandırılarak, sadece oku haline getirilir. Yazılımlar genellikle ihtiyaçlara, teknolojik değişimlere ve donanım altyapısı değişikliklerine vb. göre güncellenmek zorunda kalırlar. Güncellenen kısmı yazılımdan ayırmak çoğu zaman oldukça güç bir iştir. Her güncellenen yazılım UYSM tarafından farklı bir proje olarak görülür çünkü UYSM dosya değişmezliğini ve güvenliğini garanti etmektedir. Güncellenen sürüm yeni bir proje dosyası olarak sisteme kaydolur ve kaynak kod emanetçilik işlem süreçleri baştan başlar.

2.5. Sözleşme Uzatma

Süre ile sınırlı emanetçilik sözleşmeleri, sözleşme süresi bitiminde emanetçilik anlaşması uzatılmak istenirse ve sözleşmede değişiklik yoksa taraflar web üzerinden sözleşmeyi, süresi biten sözleşme referans numarası ile uzatabilirler. Sözleşmede değişen maddeler var ise yeni bir sözleşme yapılmalı ve işlemler baştan başlamalıdır.

2.6. Kaynak Kodu Devir Hükümlerinin Gerçekleşmesi

Emanetçilik sözleşmesinde belirtilen kaynak kodu devir hükümlerinin gerçekleşmesi ile yazılım müşterisi kaynak koduna erişim hakkına sahip olur [1,2,3,4]. Yazılım müşterisinin, kaynak koda erişim sağlayabilmesi için hukuki yönden bu maddelerin gerçekleştiğini UYSM'ye ispat etmesi gerekmektedir. İlgili hükümlerin gerçekleştiğine dair kanıt (mahkeme kararı) UYSM tarafından hukuk müşavirliğine incelettirilir. Olumlu yanıt alınırsa, yazılım müşterisi kendinde saklı olan anahtar parçası ile UYSM'de saklı kalan anahtar parçasını birleştirir ve dosya erişim anahtarını elde eder. UYSM veritabanında saklı tutulan ilgili proje dosyası yazılım müşterisine verilir. Yazılım müşterisi elindeki anahtar dosya ile şifrelenmiş kaynak kodunun şifresini çözerek kaynak kodunu elde eder.

3. Sonuç

UYSM'de tasarlanan çift anahtarlı kaynak kodu emanetçilik sistemi ile yazılım eser sahiplerinin, yazılımları üzerindeki fikri mülkiyetlerinin koşullu olarak korunması, yazılım müşterilerinin yazılım eser sahiplerinin işlerine devam edememesi durumunda yazılım kaynak kodlarına erişerek ihtiyaçlarını giderebilmesi sağlanmıştır. Sözleşme referanslı elektronik kayıt sistemi ile yazılım üretici ve yazılım müşterisi arasında ilerde karşılaşılabilecek hukuki sorunların çözülebileceği bir yapı oluşturulmaktadır. Uygulanan sistem kriptolu kayıtların kripto öncesi özütlerini referans alarak aynılık ve güvenlik koşullarını sağlamakta, orijinin değişmezliğini garanti etmektedir. Ayrıca çoklu anahtar ile sözleşme denetimli, koşullu erişim imkanı bir arada olduğu göz önünde tutulursa sadece ülkemizde değil Dünya'da da giderek artan önemli bir ihtiyaca yeni ve uygulanabilirliği yüksek bir senaryo dahilinde cevap verdiği görülmüştür. Emanete alınacak kod ya da veri uçtan uca kriptolu olarak bir ucu 5 kademeli güvenlik sistemine sahip UYSM'nin en yüksek güvenlikli bölmesine dolaylı olarak aktarılmaktadır. Güvenlik nedeniyle bu kademeye doğrudan harici erişim mümkün değildir. 4. güvenlik kademesinden gönderenin elektronik onayı ve manuel kontrollü köprülemeyle aktarım sağlanmaktadır. Diğer bir deyişle yediemin hizmetleri yüksek güvenlikli sayısal kayıt sisteminin bir eklentisi olarak anahtar ve sözleşme yönetimine dayalı bir uygulama şeklinde gerçekleştirilmektedir.

4. Kaynakça

[1] Freeman E.H., ``Source Code Escrow", *Information Security Control: A global Perspective*., s.1-3, 2004.

[2] Han C., Zhao T., Tsung-Yen. ve Lee K., "Method and Apparatus for Providing to the conditional access to the source code of a program", *US Patents Publications*,

[3] Wood, G., "Protecting the Future", "*The Computer Bulletin*",May *2004*

[4] Lipner S. B., Balenson D.M., Ellisom C.M., Walker S.T. "System and Method For Key Escrow Encryption", *United States Patent*, 1996