# MERKEZİ DOSYA SAKLAMA ORTAMLARI İÇİN ERİŞİM DENETİMLİ KRİPTOGRAFİK BİR GÜVENLİK MİMARİSİ

**Tuğkan Tuğlular, Gürcan Gerçek, Ezgi Samanlı**
İzmir Yüksek Teknoloji Enstitüsü
tugkantuglular@iyte.edu.tr, gurcangercek@std.iyte.edu.tr, ezgisamanli@std.iyte.edu.tr

## ABSTRACT

Private and sensitive information is stored frequently in files, where secure storage becomes very important. This paper proposes a security architecture for central file repositories, where defense in depth is achieved through access control, cryptography and logging. The proposed architecture is composed of five servers; three are directly associated with security, the remaining two are a file server and a mediator. A client application is also an integral part of the architecture, which performs login, file upload / download operations. Cryptographic functions are embedded into all of these operations and their counterparts at the server side. The work includes experimental results obtained by execution of the software components of proposed architecture.

**Key words:** File security, Access control, Cryptograhy.

## 1. GİRİŞ

Kurumlar veritabanı güvenliği kadar dosya güvenliğine de önem vermek durumundadır. Önemli verilerin ve bilgilerin kayda değer bir kısmı dosyalar içinde saklanmakta ve sadece yetkili kişilerin bu dosyalara erişmeleri istenmektedir. Önemli dosyaların dağıtık olarak saklanması gerekli güvenlik önlemlerinin alınmasını güçleştirir. Dolayısıyla, bu tür dosyaların kurum denetiminde bulunan merkezi bir saklama ortamında toplanması güvenlik önlemlerinin etkisini arttıracaktır. Yetkisiz kişiler ya da programlar dosyaların saklandığı bu merkezi sanal ortama ulaşır ise, gizliliği ve mahremiyeti ihlal edecek şekilde dosya içindeki bilgileri okuyabilir, kopyalayabilir veya değiştirebilir. Böyle bir duruma düşmemek için kurumlar, gizli ve mahrem bilgi içeren dosyaların bulunduğu saklama ortamlarını katmansal güvenlik önlemleri alarak korumak zorundadır.

Kurumlar merkezi dosya saklama ortamı oluştururken erişim yaklaşımını belirlemelidir. Günümüzde en temel iki yaklaşım grup bazında erişim ve rol bazında erişimdir. Bu bildirinin yazarları dosyaların genellikle bir beraber iş yapma için kullanıldığı düşüncesinden yola çıkarak grup bazında erişim yöntemini çalışmaya temel almıştır. Yazarlar ayrıca, dosya içindeki veri ve bilgilerin gizliliği için hem simetrik hem de asimetrik şifreleme yöntemlerinin kullanıldığı bir yöntemi çalışmanın diğer ana unsuru olarak belirlemiştir. Bu çalışmada dosya saklama ortamlarının erişim denetimi, şifreleme ve günlük (log) tutma güvenlik önlemleri ile korunduğu bir uygulama geliştirilmiştir. Bu uygulama için kullanıcı, dosya ve sürüm yönetimi gibi özellikler kapsam dışı bırakılmıştır.

Bildiri; Giriş, Yöntem, Mimari, Uygulama, Deneysel Bulgular ve Sonuç olmak üzere altı bölümden oluşmaktadır. Yöntem bölümünde merkezi dosya saklama ortamı için önerilen dosya şifreleme yöntemi ve erişim denetimi yöntemi anlatılmıştır. Takip eden iki bölümde ise anılan yöntemlerin yazılım olarak tasarımı ve bu mimari doğrultusunda geliştirilen uygulama gösterilmiştir. Deneysel Bulgular bölümünde geliştirilen uygulamanın laboratuvar ortamında kurulup çalıştırılması ile elde edilen (ölçülen) operasyonel değerler verilmiş ve tartışılmıştır.

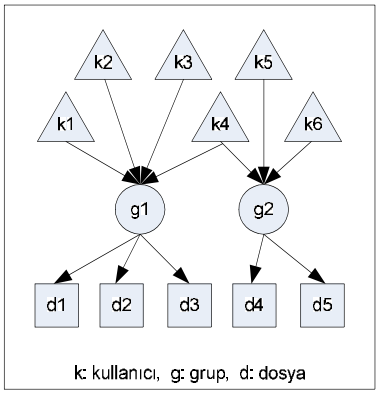
## 2. YÖNTEM

Merkezi dosya saklama ortamları için erişim denetimli kriptografik bir uygulama geliştirirken izlenen erişim denetimi yöntemi ile kriptografik yöntem bu bölümde açıklanmıştır. Tasarlanan ve geliştirilen uygulama; özgünlük denetimi, gizlilik ve doğruluk/bütünlük güvenlik hedeflerini tutturacak bir katmansal güvenlik yapısına sahiptir. Nitekim, literatürde yer alan benzer uygulamalara ait bir kıyaslama çalışmasında anılan katmansal yapının gerekliliğine dikkat çekilmektedir [1].

Bu çalışmada grup bazında erişim denetimi yöntemi temel alınmıştır. Bu yönteme göre bir dosyaya erişim hakkı sadece bir gruba aittir ve kullanıcılar kendi başlarına herhangi bir dosyaya erişemez. Bir grup bir ya da daha fazla kullanıcıdan oluşabilir. Bir kullanıcı aynı zamanda birden fazla grubun üyesi olabilir [2]. Grup bazında erişim yöntemi Şekil 1'de bir örnek üzerinde gösterilmiştir.

Bu çalışmada dosya içindeki veri ve bilgilerin gizliliği ve doğruluk/bütünlüğü için hem simetrik hem de asimetrik şifreleme yöntemleri

kullanılmıştır. Dosyalar çok değişik büyüklüklerde (örneğin 1KB – 100 MB aralığında) bulunabileceği için dosyalar 3DES [3] ile simetrik, simetrik şifrelemede kullanılan anahtar da 1024 bit RSA [4] ile asimetrik olarak şifrelenmiştir. 1024 bit RSA şifreleme ayrıca oturum açarken kullanıcı parolası için de kullanılmıştır.



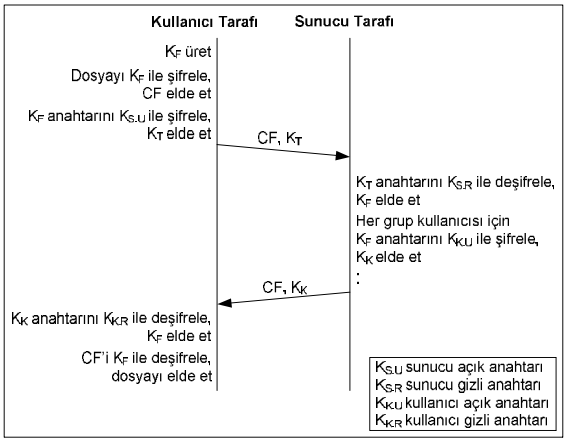
Şekil 1. Grup bazında erişim örneği

Önerilen merkezi dosya saklama ortamları için erişim denetimli kriptografik güvenlik mimarisinde, bir kullanıcının yetkisi dahilinde bir dosyayı sunucuya yükleyebileceği veya sunucudan indirebileceği kabul edilmiştir. Dosya şifreleme ve deşifreleme işlemleri sadece kullanıcı uygulamasında gerçekleştirilmekte ve bunun için 3DES algoritması kullanılmaktadır. Dosya şifreleme işleminden önce kullanıcı uygulaması şifreleme anahtarını (KF) rasgele üretmektedir. Bu anahtar kullanılarak 3DES ile şifrelenen dosya ve sunucu açık anahtarı ile şifrelenen KF anahtarı sunucuya gönderilmektedir (bknz Şekil 2). Böylece sunucuya dosya yükleme işlemi gerçekleştirilmiş olur.

Sunucu kendisine gelen dosyayı ilgili gruba ait dizine yerleştirirken aynı zamanda kendi gizli anahtarı ile KF anahtarını deşifreler ve grupta bulunan her kullanıcı için kullanıcı açık anahtarı ile KF anahtarını tekrar şifreler ve veritabanına yerleştirir. Böylece yüklenen dosyayı ilgili grubun her üyesi kendi gizli anahtarı ile açabilir. Sunucu veritabanına tüm grup üyeleri için anahtarı yerleştirdikten sonra KF anahtarını siler (bknz Şekil 2).

Gruba üye bir kullanıcı dizindeki bir dosyayı sunucudan indirmek istediğinde sunucu dosyayı grup dizininden ve talepte bulunan kullanıcının açık anahtarı ile şifrelenmiş KF anahtarını veritabanından alarak kullanıcıya yollar. Kullanıcı uygulaması önce kullanıcı gizli anahtarı ile KF anahtarını deşifreler, sonra da KF anahtarı ile dosyayı deşifreler (bknz Şekil 2). Artık dosya açık metin halinde kullanılabilir durumdadır.

Burada kullanılan kriptografik yöntemin zayıflığı sunucu tarafında KF anahtarının açık olarak sunucu yazılımı tarafından işlenmesidir. Sunucu hiçbir anda KF anahtarını disk üzerinde bir yere kaydetmese bile bellekte tuttuğu ve (işletim sistemi bellek güvenliği sayesinde) pratikte zor olmakla birlikte teorik olarak bellekte açık olarak duran KF anahtarı yetkisiz kişi veya programlar tarafından okunabileceği için bir zayıflık söz konusudur. Bu zayıflığı ortadan kaldırmak, sunucuda gerçekleştirilen grup üyeleri açık anahtarları ile şifreleme işleminin kullanıcı uygulamasında yapılması ile mümkündür [5]. Ancak bunun için kullanıcı uygulamasının grup üyelerini ve açık anahtarlarını biliyor olması ve 1024 bit RSA şifreleme işlemlerinden sonra <grup_üye, açık_anahtar_şifreli_KF anahtarı> ikililerini sunucuya şifreli dosya ile birlikte yüklemesi gereklidir. Bu bildirinin yazarları zayıflığın giderildiği durumu sergileyen uygulamayı gerçekleştirmeyi ve bu çalışmanın çıktısı olan uygulama ile karşılaştırmayı gelecekte ortaya koymayı planlamıştır.



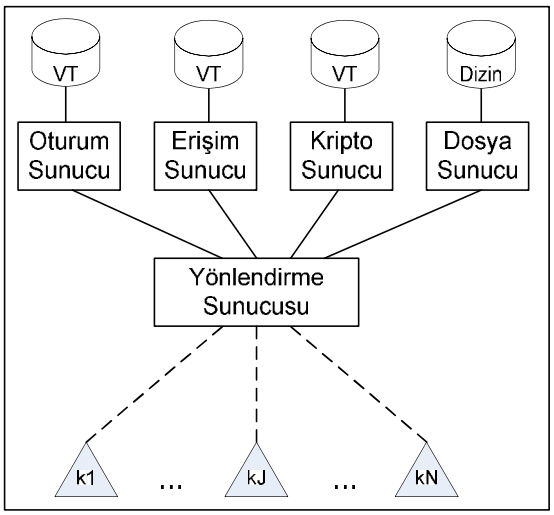
Şekil 2. Kullanıcı ve sunucu şifreleme işlemleri

## 3. MİMARİ

Merkezi dosya saklama ortamları için erişim denetimli kriptografik güvenlik mimarisi önceki bölümde açıklanan erişim denetimi ve şifreleme yöntemleri kullanılarak geliştirilmiştir. Anılan yöntemlerin kodlandığı yazılım bileşenleri tekrar kullanılabilirlik ve ölçeklenebilirlik hedefleri doğrultusunda Şekil 3'de gösterildiği biçimde tasarlanmıştır. Tasarlanan uygulama halihazırda var olan oturum ve dosya sunucuları kullanabilecek şekilde tasarlanmıştır. Sunucuların hepsi aynı bilgisayar üzerinde olabileceği gibi farklı bilgisayarlar üzerinde bulunabilir. Sunucular bileşenler şeklinde tasarlandığı ve kendi işlemleri dışında bir iş mantığına sahip olmadıkları için bu sunucuları sevk ve idare edecek orkestra şefi

mahiyetinde bir yönlendirme sunucusu tasarıma ve uygulamaya eklenmiştir.

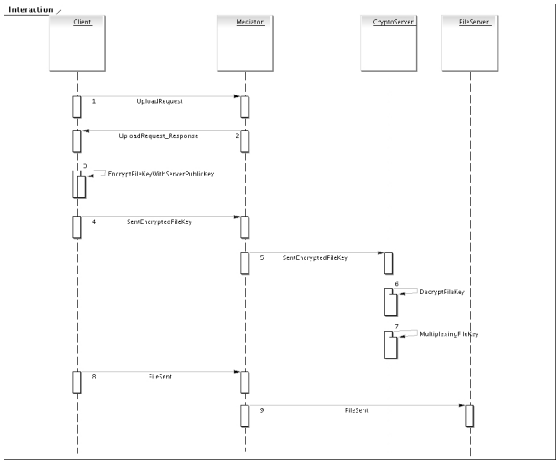
Önerilen mimariye ilişkin senaryo bir kullanıcının oturum açma isteği ile başlar. Kullanıcı; kimlik, parola ve çalışacağı grup bilgileri ile oturum açma isteğini yönlendirme sunucusuna, o da oturum sunucusuna gönderir. Oturum sunucusu özgünlük denetimini, erişim sunucusu erişim (istenilen grup üzerinden işlem yapıp yapamayacağı) denetimini gerçekleştirir ve yönlendirme sunucusu her ikisi tarafından bilgilendirilir, o da kullanıcıya sunucuya dosya yükleme veya sunucudan dosya indirme işlemleri için hazır olduğunu bildirir.



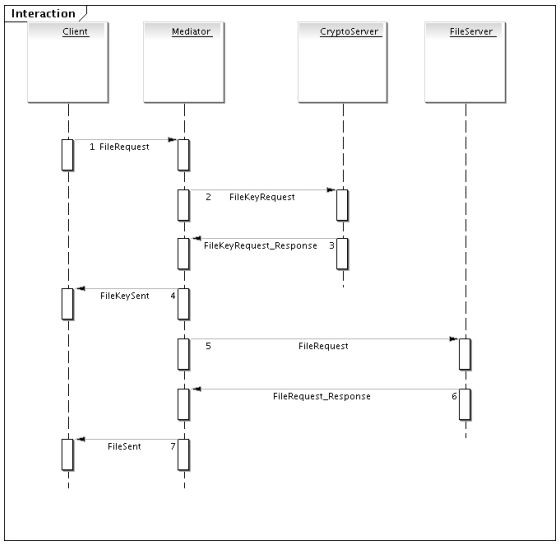

Şekil 3. Merkezi dosya saklama ortamları için erişim denetimli kriptografik uygulama mimarisi

Kullanıcı dosya yüklemek istiyorsa Şekil 4'de verilen etkileşim diagramı doğrultusunda gerekli adımları atar. Dosya yükleme isteği onaylandıktan sonra Şekil 2'de gösterilen işlemler kendi üzerinde gerçekleştirir ve önce sunucu açık anahtarı ile şifrelenmiş dosya anahtarını gönderir. Kripto sunucusu bu anahtar üzerindeki işlemleri bitirdiğinde yönlendirme sunucusu şifrelenmiş dosyayı yüklemesini ister. Yükleme sonucunda şifrelenmiş dosya dosya sunucusu tarafından ilgili dizine, grup üyelerine ait anahtarlar ise kripto sunucusu tarafından veritabanına yerleştirilmiş durumdadır.

Kullanıcı dosya indirmek istiyorsa Şekil 5'de verilen etkileşim diagramı doğrultusunda gerekli adımları atar. Dosya indirme isteği onaylandıktan sonra Şekil 2'de gösterilen işlemler gerçekleşir ve önce dosya anahtarının kullanıcı açık anahtarı ile şifrelenmiş hali kripto sunucusu tarafından hemen ardından da şifreli dosya dosya sunucusu tarafından kullanıcıya gönderilir. Kullanıcı kendi üzerinde gerekli deşifreleme işlemlerini yaparak dosyanın açık metin halini elde eder.




Şekil 4. Dosya yükleme etkileşim diagramı




Şekil 5. Dosya indirme etkileşim diagramı

## 4. UYGULAMA

Önerilen merkezi dosya saklama ortamları için erişim denetimli kriptografik güvenlik mimarisine ilişkin uygulama Java progamlama dili kullanılarak geliştirilmiştir. Bu uygulama içinde beş tanesi sunucu ve bir tanesi kullanıcı uygulaması olmak üzere altı adet yazılım bileşeninden oluşmaktadır. Önceki bölümde sunucu bileşenleri açıklanmıştı. Bu bölümde kullanıcı uygulaması tanıtılacaktır.

Kullanıcı uygulamasının aşağıda listelenen yetenekleri sahip olması gerektiği düşünülmüş ve bu doğrultuda yazılım bileşeni gerçekleştirilmiştir:

- Kullanıcı kimlik, parola ve grup bilgileri sunucu açık anahtarı ile şifrelenip gönderilmektedir. Parola bu şifreleme işlemine girmeden önce md5 algoritmasına sokulmakta çıkan öz değeri şifrelenip yollanmaktadır.
- Dosyalar 3DES algoritması ile şifrelenmektedir. Bu şifreleme için gerekli anahtar (Şekil 2'de KF olarak gösterilmişti) rasgele üretilmektedir. KF

anahtarı sunucu açık anahtarı ile şifrelenip dosya ile birlikte gönderilmektedir.

- Sunucuda bulunan yetki dahilindeki herhangi bir dosya ve anahtarı indirilmektedir. Anahtar kullanıcı gizli anahtarı ile deşifrelenip dosyayı deşifrelemek için kullanılmaktadır.

Kullanıcı oturum açma penceresi Şekil 6'da ve sunucuya dosya yükleme ve sunucudan dosya indirme işlemlerinin yapıldığı işlem penceresi de Şekil 7'de gösterilmiştir.

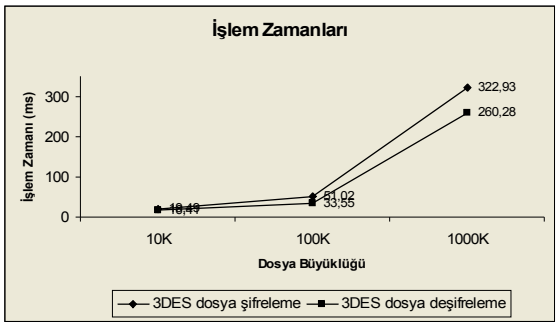

Şekil 6. Kullanıcı oturum açma penceresi


Şekil 7. Kullanıcı işlem penceresi

## 5. DENEYSEL BULGULAR

Önerilen merkezi dosya saklama ortamları için erişim denetimli kriptografik bir güvenlik mimarisi sunucularından her biri 3.4 GHz Pentium işlemci ve 2 GB ana belleğe sahip bir bilgisayara Linux işletim sistemi üzerinde çalışacak şekilde kurulmuştur. Deneyde yer alan bir diğer yazılım bileşini olan kullanıcı uygulaması ise laboratuvar ortamında 3GHz Pentium 4 işlemci ve 1 GB ana bellek özellikli Windows XP SP2 işletim sistemi yüklü 10 ayrı bilgisayara kurulmuştur. Bu deney düzeneği 10K, 100K ve 1000K dosya büyüklükleri için ayrı ayrı 10 defa çalıştırılmış ve aşağıda verilen sonuçlar elde edilmiştir.

Kullanıcı uygulamasının oturum açma isteğini oluşturup şifrelemesi ortalama 124,7 milisaniye (ms), bu isteği gönderip yanıt alması ortalama 562,83 ms sürmektedir. Yine kullanıcı uygulamasının dosya şifrelemek için 3DES anahtarını üretme süresi ortalama 0,68 ms almaktadır. Ortalama dosya şifreleme ve deşifreleme süreleri Şekil 8'de verilmiştir.




Şekil 8. Ortalama dosya şifreleme ve dosya deşifreleme süreleri

## 6. SONUÇ

Hassas, gizli ve mahrem veri ve bilgiler gitgide artan bir şekilde dosyalarda saklanmaktadır. Bu bildiri, merkezi dosya saklama ortamları için erişim denetimli kriptografik bir güvenlik mimarisi önerisini ortaya koymaktadır. Önerilen mimari, sunucu tarafında oturum açma, erişim denetimi, kripto, dosya ve yönlendirme sunucusu olmak üzere beş ve bir de kullanıcı uygulaması ile altı adet yazılım bileşeninden oluşmaktadır. Bileşenler çalışma yöntemleri ve birbirleri arasındaki etkileşimler dikkate alınarak açıklanmıştır. Ayrıca, gerçeklenen bileşenlerin kullanıldığı deneyler sonucunda elde edilen bulgular da sunulmuştur.

Önerilen mimari birçok açıdan geliştirilebilir. Güvenlik açısından bakıldığında sunucular arası SSL bağlantısı yapılması ve grubun kullanılacak şifreleme algoritma tipini belirlemesi geliştirme hedefidir. Operasyonel açıdan yaklaşıldığında kullanıcı, dosya ve sürüm yönetimi mimariye eklenmelidir. Önerilen mimaride kullanılan kriptografik yöntemin zayıflığını giderecek şekilde yöntemi iyileştirme ve bu iyileştirme sonucu ortaya çıkacak kayıp ve kazançların değerlendirilmesi öncelikli gelecek çalışma olarak belirlenmiştir.

## KAYNAKLAR

[1] Stanton, P. Securing Data in Storage: A Review of Current Research. Department of Computer Science, University of Illinois at Urbana-Champaign, 2004.

[2] Gollman, D. Computer Security. John Wiley & sons, 1999, p.38.

[3] Triple DES. http://en.wikipedia.org/wiki/Triple_DES, Retrieved on March 2, 2008.

[4] RSA. http://en.wikipedia.org/wiki/RSA, Retrieved on March 2, 2008.
[5] Perlman, R.J. and Hanna, S.R. Method and apparatus for using non-secure file servers for secure information storage, United States Patent 7178021, Issued on February 13, 2007.