ÜNİVERSİTE YÖNETİM SİSTEMLERİ İÇİN İŞ SÜREÇLERİNİN EVRAKSIZLAŞTIRILMASINA YÖNELİK KRİPTOLU DOKÜMAN YÖNETİM SİSTEMİNİN GELİŞTİRİLMESİ

2013
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

Burhan GÜVEN

ÜNİVERSİTE YÖNETİM SİSTEMLERİ İÇİN İŞ SÜREÇLERİNİN EVRAKSIZLAŞTIRILMASINA YÖNELİK KRİPTOLU DOKÜMAN YÖNETİM SİSTEMİNİN GELİŞTİRİLMESİ

Burhan GÜVEN

Karabük Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalında
Yüksek Lisans Tezi
Olarak Hazırlanmıştır

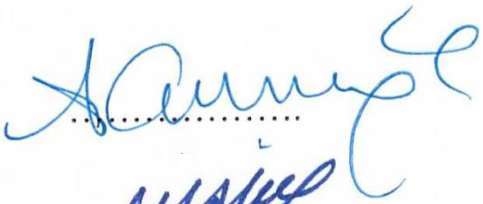
KARABÜK
Eylül 2013

Burhan GÜVEN tarafından hazırlanan "ÜNİVERSİTE YÖNETİM SİSTEMLERİ İÇİN İŞ SÜREÇLERİNİN EVRAKSIZLAŞTIRILMASINA YÖNELİK KRİPTOLU DOKÜMAN YÖNETİM SİSTEMİNİN GELİŞTİRİLMESİ" başlıklı bu tezin Yüksek Lisans Tezi olarak uygun olduğunu onaylarım.

Prof. Dr. Mehmet AKBABA

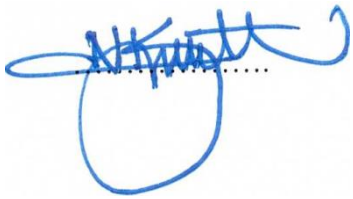
Tez Danışmanı, Bilgisayar Mühendisliği Anabilim Dalı

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir. 05/09/2013

Ünvanı, Adı SOYADI (Kurumu)	İmzası
Başkan : Prof. Dr. Abdullah ÇAVUŞOĞLU	
Üye : Prof. Dr. Mehmet AKBABA	
Üye : Yrd. Doç. Dr. Salih GÖRGÜNOĞLU	

…./…. /2013

KBÜ Fen Bilimleri Enstitüsü Yönetim Kurulu, bu tez ile, Yüksek Lisans derecesini onamıştır.



Prof. Dr. Nizamettin KAHRAMAN

Fen Bilimleri Enstitüsü Müdürü

"Bu tezdeki tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu; ayrıca bu kuralların ve ilkelerin gerektirdiği şekilde, bu çalışmadan kaynaklanmayan bütün atıfları yaptığımı beyan ederim."

Burhan GÜVEN

ÖZET

Yüksek Lisans Tezi

ÜNİVERSİTE YÖNETİM SİSTEMLERİ İÇİN İŞ SÜREÇLERİNİN EVRAKSIZLAŞTIRILMASINA YÖNELİK KRİPTOLU DOKÜMAN YÖNETİM SİSTEMİNİN GELİŞTİRİLMESİ

Burhan GÜVEN

Karabük Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı:
Prof. Dr. Mehmet AKBABA
Eylül 2013, 43 sayfa

Bu çalışmada, resmi kurumların özellikle de üniversitelerin kendi iç yazışma uygulamalarının bilgisayar ortamında güvenli bir şekilde yapılması amaçlanmıştır. DYS, kullanıcılar tarafından web tabanlı olarak bir web tarayıcısı aracılığı ile kullanılmaktadır. Tüm bilgiler MSSQL veri tabanında tutulmaktadır. Sistem isteğe bağlı olarak elektronik onay ya da dijital sertifikalı e-imza ile çalışabilmektedir. Sistem kurumlarda uygulandığı zaman kullanıcılara hem zaman, hem de kırtasiye giderlerini en az seviyeye düşürmüş olacaktır.

Anahtar Sözcükler **:** Resmi kurumlar, üniversiteler, iç yazışma, bilgisayar, DYS, MSSQL, elektronik onay, dijital sertifika, e-imza.

Bilim Kodu **:** 916.2.033

ABSTRACT

M. Sc. Thesis

DEVELOPMENT OF CRYPTOGRAPHIC DOCUMENT MANAGEMENT SYSTEM DEVOTED TO NON-DOCUMENTATION OF WORK PROCEDURES FOR UNIVERSITIES

Burhan GÜVEN

Karabük University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

Thesis Advisor:
Prof. Dr. Mehmet AKBABA
September 2013, 43 pages

This system purposes to form their internal correspondence of official institutions safely, especially universities on computer system. DYS is used web based through a browser by users. All data stored in the MSSQL database. The system can operate with electronic confirmation or digital signature optionally. When the system applies to the institutions or universities, time and stationary cost will be minimized.

Key Word **:** Official institutions, universities, internal correspondence, DYS, MSSQL, electronic confirmation, digital signature.

Science Code **:** 916.2.033

TEŞEKKÜR

Bu tez çalışmasında desteklerini esirgemeyen sayın hocam Prof. Dr. Abdullah ÇAVUŞOĞLU'na ve sayın danışmanım Prof. Dr. Mehmet AKBABA'ya ve de çalışmalarım esnasında değerli fikirleri ve destekleri için meslektaşım Recep GARİP'e teşekkürlerimi sunarım.

Hayatım boyunca her zaman maddi manevi desteklerini hiç esirgemeyen sevgili aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

KISALTMALAR

e-imza	: Elektronik imza.
MSSQL	: Microsoft Structured Query Language
KDV	: Katma Değer Vergisi
DYS	: Doküman Yönetim Sistemi
SDP	: Standart Dosya Planı
NARA	: National Archives and Records Administration
DoD	: Deparment of Defense
AB	: Avrupa Birliği
TSE	: Türk Standartları Enstitüsü
ISO	: International Organization for Standardization
Kr	: Kripto
OCR	: Optical Character Recognition
DBA	: Database Administration
PK	: Primary Key
ID	: Identity
Id	: Identity
D.B.	: Daire Başkanlığı
Bşk.	: Başkanlığı
SSL	: Secure Socket Layer
TSL	: Transport Layer Security
AES	: Advance Encryption Standard
pda	: Personal Digital Asistant

BÖLÜM 1

GİRİŞ

İçinde bulunduğumuz dünyada teknolojik gelişmeler sebebiyle ve internetin de çalışma hayatına girmesiyle hem kurumların hem de kurumlarla muhatap olan insanların klasik metotlarla evrak işlerinin takibi, pek çok sorunlarıyla beraber sistemi de yavaşlatmaktaydı. Örneğin, daha önceleri defterdarlıklara verilen KDV beyannamelerini muhasebeciler yazılı formlara doldurduktan sonra maliyeye elden teslim etmek durumundaydılar. Sadece teslim aşamasında bile saatlerce kuyruk beklenmekteydiler. Bu işlemler sonucunda alınan değerler ise yine bir başka görevli tarafından bilgisayarlara işlenmekte idi. Bu işlemler sırasında matematiksel rakam hatalarına sıkça rastlanmaktaydı. Bu durumdan da her iki taraf mağdur olabilmekteydi. Oysa Maliye Bakanlığı'nın bu sistemi internet vergi dairesi adı altında elektronik doküman yönetimi sistemine entegre etmesiyle; mükellefler bu bilgileri kendileri internet (web sitesi) aracılığı ile dijital ortama girip, hatalarını düzeltip, gönderebilmektedirler. Üstelik bu işlemi yedi gün yirmi dört saat kesintisiz yapabilmektedirler. Kurum ise tüm raporlama işlemlerini ve uyarılarını anlık olarak alabilmektedir.

Doküman Yönetim Sistemini kullanan kurumlarda daha önce birimler arasında elden ya da posta, ulak ile yapılan evrak sevkiyat işlemleri dijital olarak mili saniyeler içerisinde alıcıya ulaşmaktadır. Bu durum, DYS kullanıcısı kurumlara büyük ölçüde hız sağlamaktadır. Normalde bir evrak beş birime uğrayacaksa bu işlem birkaç gün sürerken DYS kullanan birimde birkaç dakika içerisinde sonuçlanmaktadır. Bu aynı zamanda kurumların karar alma ve uygulama süreçlerini de çok hızlandırmaktadır. Böylece önceleri hantal yapıda bulunan bürokratik kurumlar dinamik bir yapıya kavuşmaktadırlar.

Bu durum etkin personel kullanımında fayda sağlamaktadır. Daha çok sayıda fakat nitelik olarak daha düşük personel yerine daha az sayıda nitelikli personel ihtiyacı doğmaktadır. Böylece maddi olarak büyük miktarda personel giderleri düşürülmüştür. Aynı zamanda evrakların fiziksel dolaşımı yerine dijital dolaşım yapıldığında kırtasiye giderleri (kâğıt israfı, toner, kartuş, mürekkep vb.) azalıp neredeyse sıfıra inmekle beraber her birim için ihtiyaç olan donanım (lazer yazıcı vb.) gerekmemektedir.

DYS kullanıldığında belgelerin arşivlenmesi de dijital ortamda yapılmaktadır. Üzerinde çalışılmış geçmiş tarihli bir evrakın aranması ya da bir işlemle ilgili olarak geçmişteki yazışmaların raporlanması çok kısa süre içerisinde olduğu gibi eski sistemlerdeki tozlu arşiv odalarında evrak aramak gibi bir durum söz konusu olmamaktadır. Böylece arşivlerin kaybolması, yangın, deprem, sel gibi doğal afetlerden etkilenmesi gibi durumlara karşı avantajları da bulunmaktadır.

DYS sistemi kullanan kurumlarda çalışan kişiler, sistem web tabanlı ve internet ortamında kullanıldığı için zaman ve mekân sınırları kalkmış olmaktadır. Yani yetkili kişi mesai saatleri dışında bile işlemlerini yürütebilmektedir. Şimdilik çok lokasyonlu kurumlarda kullanıcılar nerde olursa olsun sistemi sanki odalarındaymış gibi kullanabilmektedirler. İlerde yapılacak hukuki bir düzenlemeyle hastalık, tatil, izin, seyahat gibi durumlarda kullanıcıların yerine vekil bırakmaya gerek kalmadan işlemler yürütülebilecektir. Sistemin web tabanlı olması sisteme akıllı cep telefonu, pda, tablet gibi cihazlardan da erişimi kolaylığı sağlamaktadır.

DYS kullanan kurumlarda yapılan işlemlerin hangi aşamada olduğu evrak üzerinde izleme hakkı bulunan kişilerce takip edilebilmektedir. Bu durum kurum içinde çalışma performansını arttırdığı gibi kurum dışında da sistem izlenebilir olduğu için şeffaflık ve güven sağlamaktadır.

DYS kullanıcısı personellerin belirli periyotlarda yaptıkları işlemlerin toplam sayıları takip edilip aynı işi yapan personeller arasında otomatik olarak dengeli iş dağılımı sağlanabilmektedir. Ayrıca personellerin bu zaman dilimlerindeki performansları (birim zamanda yapılan iş sayıları, standart bir işlem yapma süreleri vs.) takip

edilebilmektedir. Aynı zamanda bekleyen evrakların kimde ne kadar süre beklediği izlenip, gerekirse yöneticilere uyarılar gönderilebilmektedir. Personellerin birim zamanda iş tamamlama performansları kayıt altına alınıp raporlanabilmektedir. Buda personel performans izleme açısından önemli bir veri kaynağı oluşturmaktadır.

DYS kullanan kurumlarda konu başlıkları standartlara bağlanıp (SDP) arşiv aramalarında tüm kurumlar içerisinde geçerli olacak olan standartlar üzerinden aramalar yapılabildiği gibi, kurumlar arasındaki elektronik haberleşmelerde de konu adlarının standart olması iletişimi kolaylaştırmaktadır.

Evrakların dijital platformlarda tutulması, klasik olarak arşivlenmesine göre hem daha ucuz (daha az yer kaplaması bakımından) hem de daha güvenli (yangın, sel, deprem gibi doğal afetlere karşı) olmaktadır.

Günümüzde kurum ve kuruluşlarda kullanılan birçok uygulamada olduğu gibi doküman yönetim sistemlerinde de güvenlik oldukça yüksek önem taşımaktadır. Yapılan araştırmalar göstermiştir ki, şimdiye kadar geliştirilmiş sistemlerde sistem üzerindeki evrakların ve dosyaların güvenliği konusunda herhangi bir önlem alınmamış ve sadece sunucuların ve veri tabanı uygulamalarının güvenliğine bırakılmıştır. Geliştirilen bu uygulamada, standart güvenlik unsurlarının yanı sıra belge ve bilgi güvenliğini üst seviyelere çıkarmak için bir kripto algoritması geliştirilerek sistemin daha güvenli bir yapıya kavuşması sağlanmıştır.

Bu çalışmanın amacı, doküman yönetim sistemlerindeki eksik yanların giderildiği, kullanıcı dostu bir ara yüze sahip, kolay öğrenilebilir ve özellikle sistem üzerindeki bilgi ve belgelerin güvenli bir şekilde saklanmasını sağlayan yeni bir uygulama geliştirmektir.

Bu çalışmada ikinci bölümde diğer çalışma ve standartlardan, üçüncü bölümde yazılım alt yapısı ve sistem güvenliğinden, dördüncü bölümde sistem çalışma algoritmasından ve kurum organizasyon yapılarından, beşinci bölümde ise kullanıcı ara yüzlerinden bahsedilmiş ve altıncı bölümde de değerlendirme ve sonuç sunulmuştur.

BÖLÜM 2

DİĞER ÇALIŞMA VE STANDARTLAR

Belge yönetim sistemleri üzerine bir yazılım hazırlamadan önce konu ile ilgili literatür taraması yapılmıştır. Böyle bir durumda karşımıza çıkan mevzuat, standart ve yapılan diğer çalışmalar aşağıdaki gibidir.

2.1. YÖNETMELİK VE STANDARTLAR

Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'te genellikle evrak üzerinde fiziksel ve nitelik olarak yapılan çalışmalar yer almaktadır. Fiziksel çalışmalarda; kâğıt ölçüleri ve diğer unsurların (başlık, kurumadı, dipnot, ana metin, imzalar vs.) kâğıt üzerinde alması gerektiği yerler tanımlanmıştır. Nitelik çalışmalarında ise kurum kodlarının analizi, konu kodlama sistemleri, ilgili yazılar gibi yazı içeriği hakkında düzenlemeler yapılmıştır. Ayrıca belgelerin güvenliği, saklanması ve imha edilmesi hakkında da bilgi verilmiştir [1].

DYS sistemleri ile ilgili olarak dünyada ilk standardı uygulayan ülke Avustralya olup, AS4390 kod numaralı Avustralya Belge Yönetim Satandardı (Australian National Standard for Records Management) baz alınarak 2001 yılında Uluslararası Standartlar Örgütü (International Organisation for Standardization - lSO) tarafından uluslararası nitelikteki ilk belge yönetimi standardı olan ISO 15489 Enformasyon ve Dokümantasyon - Belge Yönetimi (Information and Documentation - Records Management) ortaya çıkarılmıştır [2].

Amerikada, Amerikan Ulusal Arşivi (National Archives and Records Administration - NARA) katkılarıyla 1997 senesinde yayımlanan DoD 5015.2 Elektronik Belge Yönetim Yazılım Uygulamaları için Standart ve bu standartı temel alarak da 2001 yılında İngiliz Ulusal Arşivi (British Public Records Office) ve Avrupa Birliği (AB)

tarafından Elektronik Belge Yönetimi Model Gereksinimi (Model Requirements for Electronic Records Management- MoReq) oluşturulmuştur [2].

Ülkemizde ise Başbakanlık tarafından hazırlanan bir genelgede elektronik doküman yönetiminin gerekliliği hakkında bilgi verilerek ve bu sistemin standartlarının Türk standartları tarafından belirlenip sistem yönetiminin de Devlet Arşivleri Genel Müdürlüğü tarafından yapılacağı belirtilerek şöyle denmektedir [3].

"Kamu adına görev yapan kurum ve kuruluşların faaliyetleri sonucu oluşan belgelerin kayıt altına alınması ve bu belgelerin istenildiği anda erişilebilir şekilde yönetilmesi, kurumsal faaliyetlerin ayrılmaz bir parçası ve bir kamu görevidir. Herkesin, her zaman, her yerden kolaylıkla ulaşabileceği şeffaf, verimli ve sade bir kurum yapısı günümüzde modern ve demokratik kurumların temel hedefi haline gelmiştir. Elektronik ortamda sunulan hizmetlerin ve e-kurum yapısının temelini elektronik bilgi sistemleri oluşturmaktadır".

"Kamu kurum ve kuruluşları oluşturacakları elektronik belge yönetim sistemlerinde TSE 13298 nolu standarda göre işlem yapacak, ayrıca üretmiş oldukları elektronik belgenin kurumlar arası paylaşımını www.devletarsivleri.gov.tr internet adresinde belirlenen kurumlar arası elektronik belge paylaşım hizmeti kriterlerine göre gerçekleştirecektir. Genelgenin yayımı tarihinden önce kurulan sistemler ise ilgili kamu kurum ve kuruluşlarınca gözden geçirilerek iki yıl içinde standarda uyumlu hale getirilecektir".

Doküman yönetimi sahasında asgari uygulama ölçütlerini belirlemek adına standartlaşma çalışmalarının doksanlı yıllarla beraber yoğunlaştığı görülmektedir. Bu alanda iki dernek ön plana çıkmıştır. İlki Uluslararası Arşiv Konseyi diğeri ise yeni adıyla Enformasyon Yönetimi Derneğidir [2].

Bu bağlamda TSE'ye bağlı Bilgi Teknolojileri ve İletişim İhtisas Grubu tarafından ISO 15489 Uluslararası Belge Yönetimi Standardı ve teknik raporu Türkçe 'ye çevrilmiş ve Bilgi ve Dokümantasyon – Belge Yönetimi adı ile Temmuz 2007'de standart olarak kabul görmüştür [2].

2.2. ÖNCEKİ YAPILAN ÇALIŞMALAR VE FARKLARI

Kurum yazılıma başlamadan önce, başka kurumların yapmış olduğu yazılımlar hakkında bir ön çalışma yapıldı. Üç farklı yazılım incelenip hazırlanan yeni yazılımla ilgili değerlendirme kriterlerinin bulunduğu karşılaştırma tablosu Çizelge 2.1'de verilmiştir.

Çizelge 2.1. Karşılaştırma tablosu.

	A Firması	B Firması	C Firması	DYS
Ortam	Web	Web	Web	Web
Veri kayıt ve Raporlama Hızı (Saniye)	3-4	3-4	2-3	1-2
Kullanıcı Ara yüzü (Sayfa Sayısı)	22	16	14	6
Eğitim Süreleri (Gün)	30	2	15	2
Sayfalar Arası Geçiş Süresi (Saniye)	3-4	3-4	2-3	1-2
Raporlama Erişim Kolaylığı (İşlem adımı)	3-4	2-3	4-5	1-2
Veri Tabanı	Oracle	Oracle	MS-SQL	MS-SQL
Veri Tabanı Güvenliği	Oracle	Oracle	MS-SQL	MS-SQL+Kr.
Ekli dosya güvenliği	Oracle	Güvenlik Yok	Güvenlik Yok	MSSQL+Kr.
Basılı belge güvenliği	Hologram	Yok	Yok	Sayfa İşaretleme

Üç farklı firma ve Yeni yazılım web ortamında hazırlanmıştır. A ve B firmaları Oracle veri tabanı kullanmış olup C firması ve Yeni Yazılım MS-SQL veri tabanı kullanmaktadır. A ve B firmasının standart veriler üzerinden evrak kayıt ve raporları getirme süreleri 3-4 saniye aralığındayken C firmasında 2-3 saniye ve Yeni Uygulamada ise bu süre 1-2 saniye aralığındadır. A ve B firmaları bu sürelerin fazla

oluşunun Oracle veri tabanının web üzerinden erişim performansı ile ilgili bir problemden kaynaklandığını söylemektedirler.

Yeni programın diğerlerinden çok hızlı olmasının sebebi ise sistemde kayıt için çok az tablo kullanılmasıdır (iki tablo kullanılmıştır). Kayıtların ve sorgulamaların sadece bahsedilen iki ana tablodan yapılması verilerin oldukça hızlı bir şekilde toplanmasını ve işlenmesini sağlamaktadır. Bu da raporlama sürelerini ve kayıt aşamalarını oldukça hızlandırmaktadır.

Sistem web tabanlı bir yapıya sahip olduğu için uygulama üzerinde sayfalar arası geçiş hızı oldukça önem taşımaktadır. Sayfalar arası geçiş hızı bilgisayarın ağ iletişimine bağlı olmakla beraber, sayfalar üzerinde yapılan işlemlerin (veri tabanı bağlantı işlemleri vb.) miktarına da bağlı olarak değişebilmektedir. İncelenen uygulamalarda A ve B firmasının sayfalar arası geçiş hızları ortalama 3-4 saniye aralığındadır. Bu süre diğer yazılımda 2-3 saniye civarındadır. Yeni yazılımda ise bu süre 1-2 saniye aralığına çekilerek kullanıcının bekleme süresi oldukça azaltılmıştır. Bu sürenin Yeni yazılımda oldukça kısa olmasının en önemli sebebi de çok az sayıda tablo kullanılmış olması ve yapılan aramalarda veri tabanına minimum sayıda sorgu çekilmesidir.

Yeni yazılımda sayfalarında mümkün olduğu kadar az nesne kullanılmış olup gerek ana menü (üç düğme) gerekse de ara yüzdeki ekranlar çok sade tasarlanmıştır. Buda diğer firmalara göre çok daha kullanıcı dostu bir tasarım sunmaktadır. C firmasında yaklaşık 14 ayrı sayfa kullanılmıştır. Bu sayı B firmasında 16 ve A firmasında ise 22 sayfaya kadar çıkmaktadır. DYS'de ise sadece 6 sayfa kullanılarak gerekli tüm işlemler gerçekleştirilmektedir. Nadiren ihtiyaç olacak olan düğmeler kullanıcıdan gizlenmiş olup kullanıcının yetki ve kişisel becerisine göre bu düğmeler aktif hale gelmektedir. Bu durum ise eğitim sürecini kısaltmaktadır. Kurum içerisinde yapılan uygulamalar bunu göstermiştir. Elli personelin sistem kullanımı eğitimi firmalara sorulduğunda A firması 30 iş günü birebir eğitimle, B firması 2 iş günü toplu eğitimle, C firması birebir eğitimle 15 günde tamamlarken Yeni yazılımda birebir eğitim olmak kaydıyla 2 iş günüdür.

Yeni yazılımda sistem gelen ve giden evrak defteri mantığı ile tasarlandığı için hem kişilerin öğrenme süreci azalmakta olup, hem de eski belgelerin raporlanması ve raporlara erişim kolaylığı sağlanmaktadır. Şöyle ki; sistem açıldığında gelen evrak defteri otomatik olarak gelip kişinin onaylaması gereken işlemler süzülmüş halde beklemektedir. Yani kişinin gereken işlemi yapmak için ayrıca bir işlem tuşuna basmasına gerek kalmamaktadır. Ama gönderdiği evrakları görmek isterse hiçbir işlem yapmadan sadece süzme kriterini tek tuşla değiştirerek görebilmektedir.

Güvenlik yönünden bakıldığında A, B ve C firmaları güvenlik işlemini tamamen veri tabanına bırakmışlardır. Yani veri tabanı yetkilisi (DBA) sistem üzerindeki tüm tablolara erişim hakkı olduğu için içerisinde kişiye özel verilerde bulunan tüm bilgileri görebilmektedir. Yani sistemin Başbakanlıkta kullanıldığı varsayılırsa başbakanlığın yapmış olduğu tüm evrak işlemleri bir bilgisayar uzmanı tarafından gözlemlenebilir. Yeni yazılımda ise veriler veri tabanına kriptolanarak kaydedildiği için tablolara bakan bir kişi gerçek veriler yerine bir takım alfa numerik değerler görecektir. Sisteme ilave eklenen veya taranmış olan belgeleri içeren dosyalar, A firmasında veri tabanının içerisinde tutulmaktadır. B ve C firmalarında ise veri tabanında fazla yer tutmaması için sunucu üzerinde bir klasörde tutulmaktadır. Sunucu üzerinde erişim hakkı olan ya da sunucuya izinsiz erişen herkes veri tabanındaki verilere erişemese bile bu ekli dosyaları görebilmektedir. Bu durum da güvenlik yönünden büyük bir risk taşımaktadır. Yeni yazılımda ise bu tür dosyalar da sistem tarafından belirli bir kripto algoritmasından geçirilip şifrelenerek saklanmaktadır. Bu dosyalara erişim hakkı olmayanlar eriştiğinde bile kullanamamaktadırlar. Sisteme ilişkin bu şifreleme algoritmasından sonraki bölümlerde bahsedilmiştir.

2.3. FARKINDALIKLAR

Bu durum gözlendiğinde Yeni yazılım diğer firmalarda bulunmayan gelişmiş güvenlik önlemleriyle ön plana çıkmaktadır. Karşılaştırma tablosunda bulunmayan başka firmalarda da bu tür güvenlik önlemlerine rastlanılmamış olup bu yönden Yeni yazılım tamamen yeni bir yapı oluşturmaktadır.

Diğer uygulamalarda olmayan güvenlik önlemlerinin yanı sıra kolay kullanım ve sadelik yönünden de diğer yazılımlara göre çok büyük farklılıklar taşımaktadır. Çizelge 2.1'de olan ve olmayan diğer firmaların ortalama sayfa sayıları 30-35 civarında iken Yeni yazılımda üç temel sayfa (Gelen/Giden Evrak, Yeni Evrak, Detaylı Arama Rapor Ekranı) ve yardımcı sayfalar (Onay Bekleyenler sayfası, Taslaklar sayfası) bulunmaktadır.

BÖLÜM 3

YAZILIM ALTYAPISI

Sistemle ilgili yazılımlar .Net 4.0 platformunda MS Visual Studio 2010 (MSVS10) uygulama geliştirme aracı kullanılarak yazılmıştır. Sistemde yardımcı araçlar olarak AjaxControlToolKit 4.x, Anti XSS 4.2.1 araçları da kullanılmıştır. Sistem verilerinin saklanması için veri tabanı olarak MS_SQL 2008R2 kullanılmıştır. Veriler 12 adet tabloda tutulmaktadır [4,5].

3.1. TABLO YAPILARI

Tablolar 2 farklı grupta yer almaktadırlar. Bunlardan birisi evrak takip işlemlerinin sürdürüldüğü grup olup diğeri de kullanıcı işlemlerinin takip edildiği gruptur.

Evrak takip işlemlerinde;

Tbl_evrak
Tbl_hareket
Tbl_durum
Tbl_birimler
Tbl_not tabloları kullanılmıştır.

Kullanıcı takip işleminde ise;

Tbl_kullanıcı
Aspnet_membership
Aspnet_users
Aspnet_roles
Aspnet_usersinroles tabloları kullanılmıştır.

Sırasıyla bu tabloların içeriği hakkında bilgi vermek gerekirse;

Tbl_evrak:

Ana evrak tablosu olup tüm evrak bilgileri bu tabloda tutulmaktadır. Her bir evrak bu tabloya bir satır olarak ilave edilmektedir. Tablonun birincil anahtar kaydı (PK) evrak id numaralarının tutulduğu "id" sütunudur. Tablonun diğer üyeleri ise;

Evrakno : Evrak üzerindeki resmi evrak numarasıdır. Yeni oluşturulan evraklarda herbir birim için belirli bir sayaçtan unique olarak oluşturulmaktadır son evrak no birimler tablosunda ayrıca tutulmaktadır. Gelen evraklarda ise, eğer evrak kurum içerisinde oluşmuş ise ilk oluşan numara esas alınmaktadır. Kurum dışından gelen evraklarda ise evrak üzerindeki numara sisteme girilmektedir.

Tarih : evrağın ilk oluşturulduğu tarihtir. Dışardan gelen evraklarda evrağın sisteme giriliş tarihidir.

Nereden : Evrağı oluşturan birimin ID sidir.

Nereye : evrağın gideceği birimin ID sidir.

Konu kodu :STP ye göre evrak konu başlığının kodudur.

Ozet : Evrak içeriği ile ilgili kısa bir metindir.

Dosyano :Evrağın fiziksel arşivdeki dosyalama numarasıdır. (isteğe bağlı)

islem : Evrağın dış birimlere gönderme biçimini belirtir. (elden, aps, posta vb.)

durum :Evrağın sistem üzerindeki hareketlerini bildirir

evraktip :Evrağın iç ya da dış evrak (kurum içi yada kurum dışı) olduğunun belirtir.

Bulundugubirim: Evrağın şu anda işlem yapılmakta olduğu birimin ID sidir

Evraktarihi : evrak üzerindeki tarihtir.

Disbirim : kurum dışına giden evraklar için metin olarak giden birimin adı

Anaevrakid : İlgi olarak yazılan evraklarda ilgili evrak ID si

Kayittip : Dışarıdan gelen evrakların birimlerinin ayırt edildiği değer

Gonderimturu : Bilgi, gereği yada koordine olup olmadığı

Evraknotu : Evrakla alakalı not (evrak üzerinde işlem yapan herkesin görebileceği not)

Filepath : Evraka ekli dosyanın yolu

filepath2 : Evraka ekli ikinci dosyanın yolu

filepath3 : Evraka ekli üçüncü dosyanın yolu

filepath4 : Evraka ekli dördüncü dosyanın yolu

filepath5 : Evraka ekli beşinci dosyanın yolu

içerik : Evrak ana metni

ilgi : İlgili evrak no

anabirimbaslik : Evrağın gönderildiği birimin adı

gonderimtipi : evrağın dış birimemi yoksa iç birimemi gittiğini göstren değer

ownerid : evrak üzerinde işlem yapan personel id si

Tbl_hareket:

Evrakların sistem üzerinde yaptığı tüm hareket bilgilerinin tutulduğu tablodur. Evrakın sisteme ilk girişinden başlamak üzere, gezdiği tüm birimler ve kişilerin bilgileri ayrı ayrı bu tabloda tutulmaktadır. Bu tablodan evrakın hangi birime yada kişiye ne zaman verildiği ve ondan ne zaman çıktığı tarih ve saatleri de alınıp performans raporları oluşturulmaktadır. Tablonun birincil anahtar kaydı (PK) hareket id numaralarının tutulduğu "id" sütunudur. Tablonun diğer üyeleri ise;

Evrakid : İlgili evrakın ID' sidir.

Bulundugubirim : Evrağın şu anda işlem yapılmakta olduğu birimin ID' sidir.

Gelenevrakno : Evrakın ilgili birime giriş yaptığı kayıt sıra numarasını gösterir.

Gidenevrakno : Evrakın ilgili birimden çıkış yaptığı kayıt sıra numarasını gösterir.

Gelistarihi : Evrakın ilgili birime giriş yaptığı tarihi gösterir.

Cikistarihi : Evrakın ilgili birimden çıkış yaptığı tarihi gösterir.

Birimid : İlgili hareket kaydının hangi birime ait olduğunu gösterir.

Onaytarihi : Evrakın alındığı birim tarafından onaylandığı tarihi gösterir.

Gonderen : Evrakın birim içindeki kişiden kişiye yapılan havale kayıtlarında, evrakı gönderen kişinin ID sidir.

Alan : Evrakın birim içindeki kişiden kişiye yapılan havale kayıtlarında, evrakın gönderildiği kişinin ID sidir.
Havaletarihi : Evrakın birim içindeki kişiden kişiye yapılan havale kayıtlarında, havalenin tarihini gösteren alandır.

Tbl_not:

Evrakların birim içinde kişiler arasındaki mesajların tutulduğu tablodur. Bu tabloda, mesajı gönderen ve gönderilen kişilerin ID leri, kişilerin birbirlerine yazdıkları mesajların içerikleri ve bu işlemin hangi tarihte yapıldığını gösteren bilgiler bu tabloda saklanmaktadır. Tablonun birincil anahtar kaydı (PK) mesaj id numaralarının tutulduğu "id" sütunudur. Tablonun diğer üyeleri ise;

Evrakid : İlgili evrakın ID' sidir.
Tarih : Mesajın gönderildiği tarihi gösterir.
Mesaj : Gönderilen mesajın içeriğidir.
Gonderen : Mesajı gönderen kişinin ID sini gösterir.
Alici : Mesajın gönderildiği kişinin ID sini gösterir.

Tbl_birimrole:

Tablodaki verilerin tutulmasının amacı kullanıcıların bir başka kullanıcıya vekalet etme durumlarında bu vekilin adının, rolünün ve vekalet süresinin de tutulmasıdır.
Tablonun birincil anahtar kaydı (PK) mesaj id numaralarının tutulduğu "id" sütunudur. Tablonun diğer üyeleri ise;

Userid : Kendisine vekâlet edilecek kişinin ID sini gösterir.
Vuserid : Vekil tayin edilen kişinin ID sini gösterir.
Birimid : Kendisine vekâlet edilecek kişinin çalıştığı birimin kodudur.
Roleid : Kendisine vekâlet edilecek kişinin bulunduğu birimdeki rolünü gösterir.

Baslangictarihi : Vekâlet süresinin ne zaman başladığını gösterir.
Bitistarihi : Vekâlet süresinin ne zaman sonlanacağını gösterir.

Tbl_konular:

Standart dosya planına (STP) ait olan konu başlıklarının tutulduğu tablodur.
Tablonun birincil anahtar kaydı (PK) konu id numaralarının tutulduğu "id" sütunudur. Tablonun diğer üyeleri ise;

Baslik : Konu ana başlığının tutulduğu alandır.
Anadosya : Konu başlığının ana dosya adının tutulduğu alandır.
Altkonu1 : Birinci alt konu başlığının tutulduğu alandır.
Altkonu2 : İkinci alt konu başlığının tutulduğu alandır.
Altkonu3 : Üçüncü alt konu başlığının tutulduğu alandır.

Tbl_Kullanici:

Tablonun birincil anahtar kaydı (PK) kullanıcı id numaralarının tutulduğu "id" sütunudur. Tablonun diğer üyeleri ise;

Ad : Kullanıcının adı.
Soyad : Kullanıcının soyadı.
Birim : Kullanıcının görev aldığı birimin kodu.
Birimrole : Kullanıcının görev aldığı birimdeki rolünü gösteren alandır.

BÖLÜM 4

GÜVENLİK ALTYAPISI

Sistem üzerinde saklanan dosya, bilgi ve verilerin güvenliği doküman yönetim sistemleri için oldukça büyük bir önem taşımaktadır. Dolayısıyla bu gibi yapılarda, güvenlik önlemleri vazgeçilmez unsurlardır. Böyle bir durumda bilgilerin güvenliğinin sağlanması, bilgilere erişim engellenemese bile, bir şekilde bu bilgilerin gizlenmesi gerekmektedir. Bu noktada da kriptojik yöntemler ön plana çıkmaktadır.

Bir metnin anlaşılabilirliğini engellemek maksadı ile farklı iki metot kullanılanabilir. Bunlardan ilki metnin belirli bir yöntem yardımıyla kısaltılması, diğeri ise belirli bir metotla metnin anlaşılamaz bir şekilde dönüştürülmesidir. Bunlardan birincisine steganografi, ikincisine ise kriptografi denir [6,7].

Kriptografik algoritma şifreleme ve şifre çözme işlemini yapabilmek için kullanılan matematiksel bir fonksiyondur. Kripto algoritmasının çalışması için bir anahtar (key) ve şifrelenecek bir metin (text) gerekir. Farklı anahtarlar kullanıldığında aynı şifrelenmemiş metinden başka şifrelenmiş yapılar oluşturulabilir [8].

Roma imparatoru Julius Sezar 2000 yıl önce, basit bir öteleme yöntemi ile şifreleme mantığı geliştirmiştir ve bu şifreleme metodu Sezar şifresi olarak bilinir. On üçüncü yüzyılda Robert Bacon bir kaç farklı yöntem ortaya koymuştur. On beşinci yüzyılda ise Leon Alberti çevirme mantığına dayanan bir şifreleme metodu ortaya çıkarmıştır ve bu frekans analizini olarak bilinir.1585 yılında ise Blaise de Vigenere kriptoloji üzerine bir kitap yayınlayarak, öteleme yöntemindeki şifreleme mantığını geliştirmiştir. Bu metot özellikle savaş alanlarında kullanılmıştır. Fakat teknolojinin ilerlemesi ile yeni şifreleme metotları ortaya çıkmıştır. Artık bilgilerin daha ileri düzey şifreleme teknikleri ile şifrelenmesine ihtiyaç duyulmuştur [8].

Kriptoloji günümüzde askeri iletişim, komuta kontrol ve karmaşık silah sistemlerinin de vazgeçilmez bir unsuru haline gelmiştir. Savaş uçakları, düşmanı yüzlerce kilometre öteden kriptoloji yardımıyla ayırt ederken, pilotun silah kullanma yetkisi olup olmadığını kriptografik yöntemlerle kontrol edebilmektedir. Zamanla diğer askeri teknolojilerde olduğu gibi kriptoloji de sıradan bir kişinin günlük hayatına girmiş ve bu alanda öncü teknoloji internet olmuştur. İnternetin yaygınlaşması ile banka şubeleri bilgisayarlarımıza kadar girmiş ve bankalardaki paralarımızın sanal karşılığı olan sayıların koruma altına alınması gerekmiştir. Bu gayeyle kullanılan ilk kripto protokolü Netscape firması tarafından geliştirilen SSL olmuştur. Ancak o dönemlerde ABD'nin uyguladığı güçlü kriptonun yayılmasını sınırlayan kurallar gereği, SSL kripto protokolündeki şifreleme algoritması kısa anahtar boyu ile kullanılmıştır. Daha sonraları Andrew Twyman isimli bir öğrenci 1996 senesinde, bağlantı başına 584 dolar maliyetle bu sistemin kırılabileceğini açıklamıştır. Kriptologların çalışmaları ile bu protokol oldukça güvenilir bir yapıya bürünmüş ve TSL ismi ile bankacılık işlemlerinde ana güvenlik bileşenlerinden biri olmuştur [9].

Sistemler arası bağlantılarda ya da farklı iki nokta arasındaki haberleşmede bilginin güvenli bir şekilde gönderildiğinden emin olmak gerekir. Bunun sağlanması ise gönderilen verinin kriptolanması ile olur. Böylece açık haberleşme kanalları kullanılarak bilginin güvenli bir şekilde gönderilmesi sağlanır. Haberleşmede, açık bir iletişim kanalı kullanılıyorsa saklı tutulmak istenen verinin yetkisiz bir kişi tarafından dinlenebileceği ya da değiştirebileceği (yanlış verinin gönderilmesi) düşüncesi her zaman önemli bir sorun oluşturur [10,13].

Kerckhoffs'un ilkesine göre kriptoanalizde saldırganın saldırı yapılan sistemi bildiği kabul edilir. Sistemde kullanılan anahtar çok iyi bir şekilde saklanmalıdır. Çünkü anahtar sistemin çekirdeğidir [10,14].

Veri güvenliği konusunda geçmişten günümüze kullanılagelen birçok şifreleme tekniği mevcuttur. Basit şifreleme metotları genellikle kâğıt kalem kullanarak gerçekleştirilebilen, çok karmaşık matematik esaslarına dayanmayan sistemlerdir. En ileri örnekleri mekanik cihazlar olan bu şifreleme yöntemleri, elektronik aletlerin kullanılmaya başlanmasıyla birlikte ortadan kalkmıştır [15].

Basit şifreleme metotlarında bir tanesi mono alfabetik şifrelemedir. En ilkel ve basit şifreleme yöntemlerinden olan Sezar yöntemi mono alfabetik şifrelemenin tipik bir örneğidir. Sezar döneminde kullanılan bu yöntemde harflerin yeri değiştirilir. Şifrelenecek metindeki harfler alfabede üç harf kaydırılarak değiştirilir [15].

Bir başka şifreleme yöntemi private key encryption olarak da bilinen simetrik şifreleme yöntemidir. Bu yöntem her iki tarafın da bildiği tek bir ortak anahtar yardımıyla şifrelemeyi ve deşifrelemeyi gerçekleştiren şifreleme metodudur. Bu şifreleme metodunun en önemli eksiği her iki tarafın da tek bir anahtar üzerinde anlaşması ve sadece bu anahtarı kullanarak şifreleme ve çözme işlemini gerçekleştirmesidir. Bu teknikte hiç bir taraf, diğer tarafın gerçekten doğru taraf olup olmadığını bilememektedir. Hatta her iki taraf da olması gereken kişiler olmayabilir. Genellikle simetrik şifreleme diğer şifreleme metotlarında gönderilecek anahtarlar gibi her iki taraf içinde ortak ifadelerin şifrelenmesi gerektiğinde kullanılır [16,17].

Mono alfabetik şifrelemelerde Türkçe için "29!-1" farklı şifreleme söz konusudur. İlk bakışta çok güvenli gibi görünmesine rağmen mono alfabetik şifrelemeler de çözülebilmektedir. Bu metotla oluşturulan şifrelemenin için kullanılan dil rahatlıkla tespit edilebilmektedir. Şifrelemenin yapıldığı dil üzerine istatiksel bir çalışma yaparak kısa zamanda kırılması mümkündür. Her dilde belirli harflerin tekrarlanma sayıları bellidir. Elimizdeki şifrelenmiş metinde en çok tekrarlanan harfler ile şifrelemenin yapıldığı dildeki en yüksek tekrarlı harfleri eşleştirdiğinizde tahmin edilenden çok daha kısa bir zamanda çözülebilir [18].

Simetrik şifrelemede, şifreleme ve deşifreleme işlemleri gizli bir anahtar yardımıyla yapılır. Şifreleme işlemleri tamamlandıktan sonra şifreli metni alıcıya gönderirken ayrıca gizli anahtarın da güvenli bir şekilde gönderilmesi gerekir. Simetrik şifreleme algoritmaları oldukça hızlıdır [9].

Simetrik şifrelemede bilgisayarların işlem kabiliyetindeki artış sebebiyle, simetrik metodun temel versiyonları artık güvenilir olarak düşünülemez. Bu nedenle 2000 yılında AES (Advanced Encryption Standard) adınyla daha güçlü ve yeni bir şifre

standartlaştırılmıştır. En kapsamlı alanda kullanılan simetrik algoritmanın yerine geçecektir [11].

Şifreleme tekniklerine verilecek örneklerden bir diğeri de asimetrik şifrelemedir. Asimetrik şifrelemede ikili anahtar yardımıyla şifreleme ve deşifreleme işlemleri gerçekleştirilir. Bu şifreleme metodunda herkesin iki anahtarı bulunur. Bunlardan biri publictir, yani herkes tarafından bilinir. Diğeri ise privatetır ve sadece şifrelemeyi yapan tek bir taraf tarafından bilinir. Bu iki anahtar rasgele seçilmiş iki anahtar biçiminde değildir. Her ikisi de birbirini tamamlayan anahtarlar şeklindedir [12,16].

Asimetrik sistemde şifreleme işlemi herkesçe bilinen açık anahtarlarla yapılır. Şifreleme ve deşifreleme işlemi birbirinin simetriği olmayan algoritmalarla yapılması sebebiyle asimetrik şifreleme sistemi olarak bilinir [9,19].

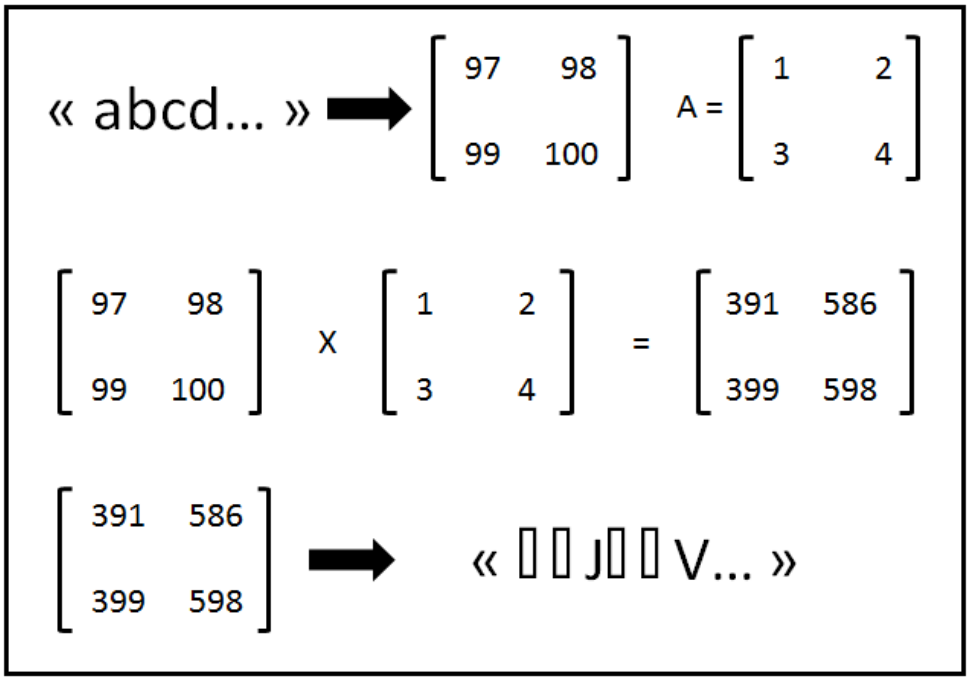
Şifreleme algoritmasının birinci parçası açık metindir. Açık metin metin veya mesaj olarak şifrelemeye alınır. İkinci parça ise şifreleme algoritmasıdır. Bu şekilde açık metin şifrelenir. Açık metinle yerine koyma ve dönüşüm işlemleri yapılır. Üçüncü parça gizli anahtardır. Anahtar, açık metin ve algoritmadan ayrıdır. Anahtara göre şifreleme algoritması farklı sonuçlar üretir. Bir diğer parça şifreli metindir. Şifreli metin gizli anahtara bağlı olarak oluşan, anlaşılması güç veri dizisidir. Son parça deşifreleme algoritmasıdır. Bu algoritma, şifreli metin ve gizli anahtar verilerini şifrelemenin aksi işlemler yaparak açık metin çıktısı oluşturur [9,20].

Burada anlatılan şifreleme teknikleri her ne kadar güvenli gibi görünse de gerçek anlamda güvenlik gerektiren sistemler üzerinde çok da sağlıklı yöntemler değildir. Bu nedenle DYS'de bir başka şifreleme tekniği olan ve klasik şifreleme yöntemlerine nazaran çok daha güvenli olan matris şifreleme yöntemi kullanılmıştır. Sistemimizde kullandığımız matris yönteminde, veriler belirli parçalara ayrılarak matrislerde tutulmaktadır. Önceden belirlenmiş bir matris anahtar yardımıyla şifreleme işlemi gerçekleştirilip veri tabanına şifrelenmiş veriler kaydedilmektedir. Klasik matris şifreleme yönteminden farklı olarak yeni yazılımdaki algoritmada anahtar belirli periotlarla değişmektedir. Bu sayede sisteme yapılan saldırılarda anahtarın belirlenmesi oldukça zor bir hal almıştır. Ayrıca algoritmanın anahtar güvenliği ise

çok güçlü bir hale gelmiştir. Eğer klasik yöntemlerdeki gibi tek bir anahtar kullanılmış olsaydı, anahtara erişimle tüm sistem çözülebilir bir hale gelebilirdi.

4.1. İÇERİK ŞİFRELEME ALGORİTMASI (ENCRYPTION)

Sistem üzerinde saklanan evrakların içerikleri veri tabanına kaydedilmeden önce bahsedilen şifreleme algoritmasından geçirildikten sonra veri tabanına kaydedilmektedir. Şekil 4.1'de işlem detayı verilen bu algoritmada 2x2'lik bir kare matris kullanılarak string formatında alınan evrak içeriği dörderli gruplar halinde ayrılarak bu karakterlerin ascii karşılıkları matrislere yazılır. Elde edilen bu kare matris yine 2x2 boyutlarında olan önceden belirlenmiş anahtar matris ile çarpılarak şifreli sonuç elde edilmiş olur.

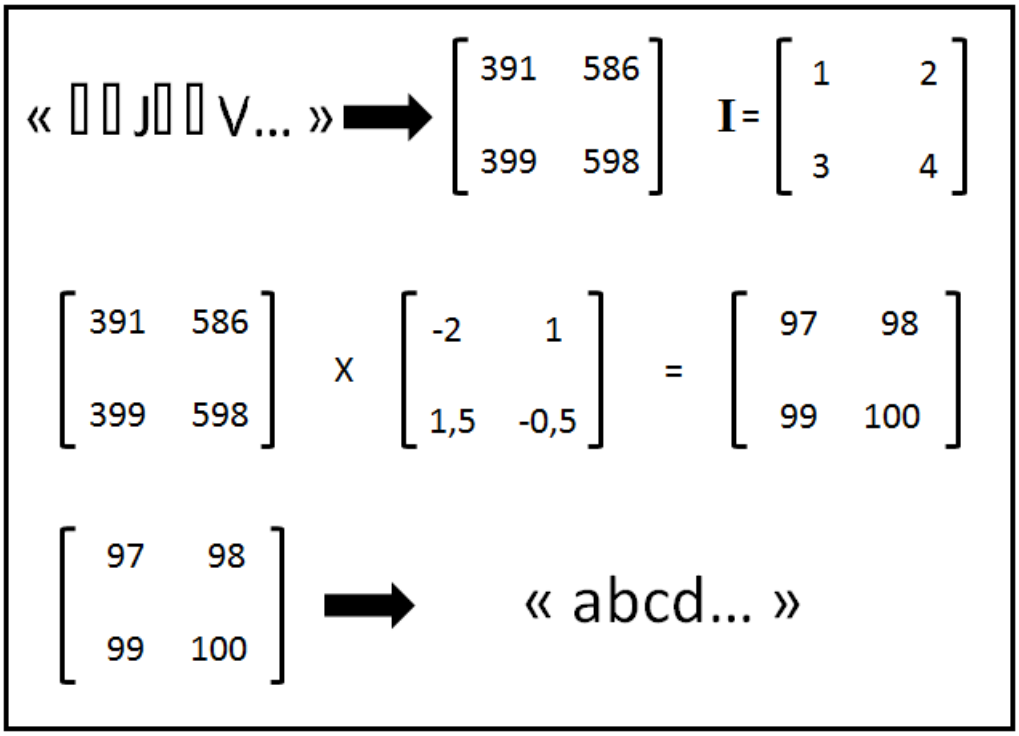


Şekil 4.1. İçerik şifreleme.

Şekil 4.1'de verilen "abcd…" örnek metnindeki ilk dört karakter alınarak bu karakterlerin ascii karşılıklarıyla elde edilen kare matris, önceden belirlenmiş olan bir anahtar matris (A) ile çarpılarak şifrelenmiş sonuç matrisi elde edilmektedir. Elde edilen bu matrisin metin karşılığı (##J##V…) da veri tabanına bu şekilde kaydedilmektedir.

4.2. İÇERİK DEŞİFRELEME ALGORİTMASI (DECRYPTION)

Veri tabanında şifrelenmiş olarak saklanan evrak içerikleri, veri tabanında kaydedilen alandan string formatında okunduktan sonra ilgili deşifreleme algoritmasından geçirilerek orijinal metne ulaşılır. Şekil 4.2 üzerinde anlatıldığı üzere veri tabanından çekilen metin yine şifreleme algoritmasında olduğu gibi dörtlü karakter setleri şeklinde ayrı ayrı işleme tabii tutulurlar. Şifrelenmiş her dört karakterin ascii karşılıkları yine 2x2 boyutlarında bir kare matrise yazılır ve daha önceden belirlenen anahtar matrisin tersi (I) ile çarpılarak orijinal metnin ascii karşılıklarına ulaşılır. Bu işlem şifrelenecek olan metin üzerinde her dört karakter için tekrarlanır ve elde edilen sonuçların birleşimiyle şifreli metin oluşturulmuş olur.



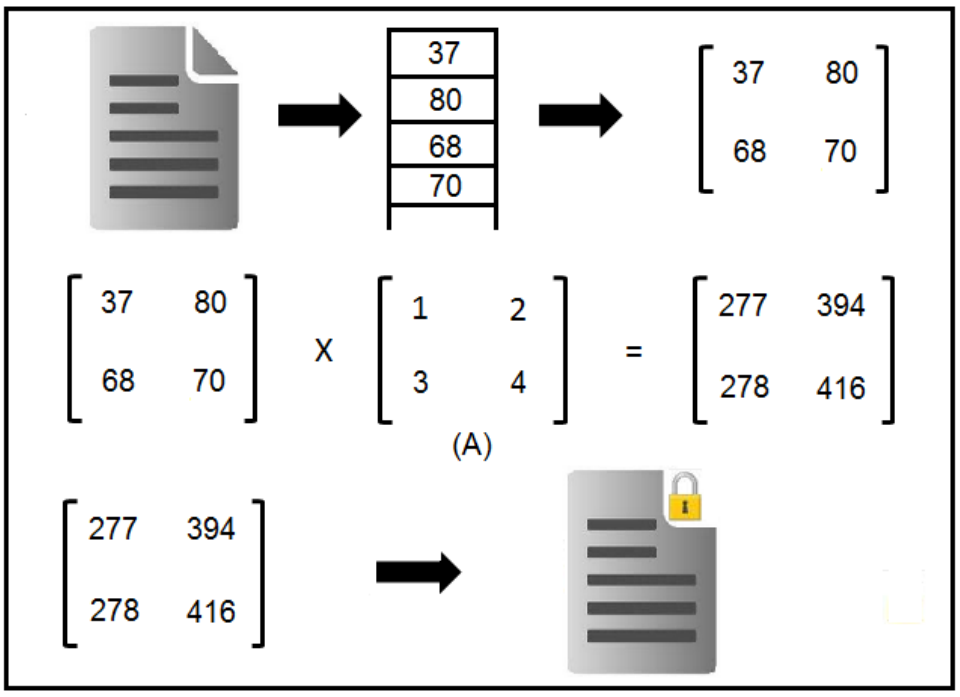
Şekil 4.2. İçerik deşifreleme.

Şekil 4.2'de de görüldüğü gibi veri tabanında saklanan şifreli örnek metnin (##J##V…) ascii karşılıkları, şifreyi çözmek için kullandığımız anahtar matrisin ters matrisi (I) ile çarpılarak orijinal metnin karakter kodlarına ulaşıldıktan sonra ekranda gösterilmek üzere karakter karşılıkları oluşturulur.

4.3. DOSYA ŞİFRELEME ALGORİTMASI (FILE ENCRYPTION)

Doküman yönetim sistemlerinde oluşturulan evrak ve belgelerin yanı sıra sistem üzerinde saklanan taranmış evraklar da mevcuttur. Bu evraklar birimlere başka bir dış birimden gelebileceği gibi kurum içerisinde oluşturulan evraklara ek olarak da hazırlanmış gönderime taranarak eklenebilir. Bu tip dosyalar DYS'nin bulunduğu sunucular üzerinde saklanmaktadır. Evrak içeriklerindeki metinlerin güvenliği kadar sunucular üzerinde kaydedilmiş bu dosyaların güvenliği de bir o kadar önem taşımaktadır. Bu noktada önemli olan evrakların yetkisiz kişilerce ele geçirilmesinden çok, ele geçirildiği takdirde saldırganların bu evrakları kullanılamaz bir halde bulmalarıdır. Bazı kurumların sunucularına yapılan saldırılar sonucu ortaya çıkan birçok gizli statüdeki evrak internet üzerinde yetkisiz kişilerce görüntülenebilmektedir. Bu ve bunun gibi güvenlik açıklarını kapatmak adına taranmış dosya ve belgelerin de bir kripto algoritmasından geçirilerek saklanması gerekmektedir.

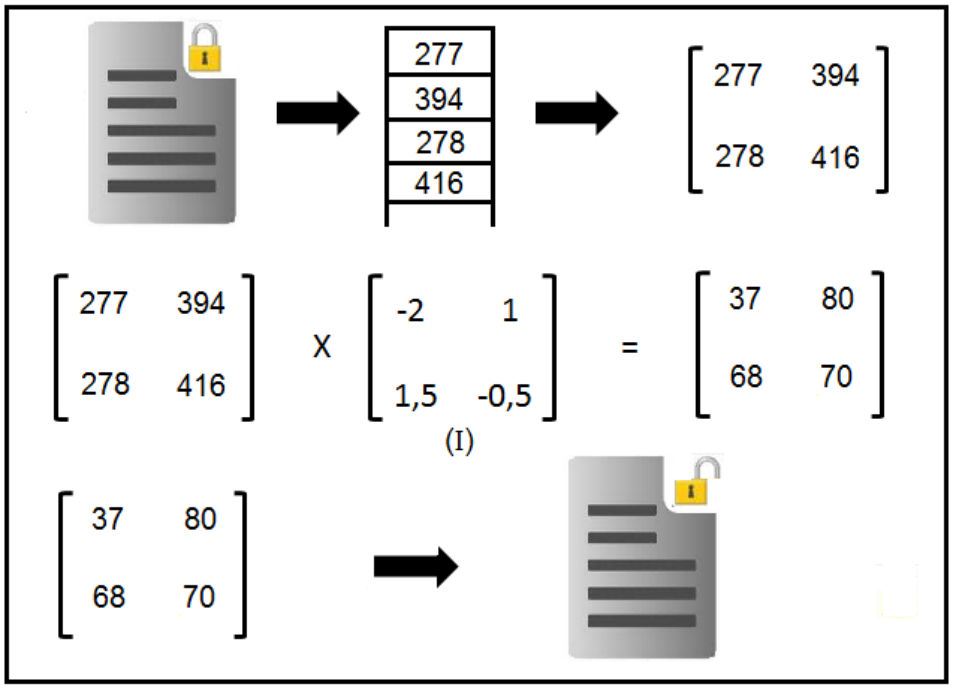
Kullanıcıların sistem üzerine yükleyecekleri dosyalar sunuculara kaydedilmeden önce içerik şifrelemede olduğu gibi yine aynı algoritma kullanılıp şifrelendikten sonra saklanmaktadır. Şekil 4.3'de anlatıldığı gibi yüklenecek dosyalar byte formatında bir diziye aktarıldıktan sonra metin şifrelemede olduğu gibi yine gruplar halinde matris işlemlerine tabii tutularak şifrelenmektedir.



Şekil 4.3. Dosya şifreleme.

4.4. DOSYA DEŞİFRELEME ALGORİTMASI (FILE DECRYPTION)

Evraklarla ilişkilendirilmiş dosyaların sunucu üzerinde ya da kişisel bilgisayarlarda dosya okuma programları kullanılarak görüntülenmesi imkânsızdır. Kullanıcı evraka ait taranmış belgeyi görüntüleyebilmek için sistem üzerinden işlem yapmalıdır. Bu noktada şifrelemiş olan dosyanın tekrar uygun anahtar aracılığıyla deşifreleme algoritmasından geçirilerek kullanıcının görüntülenmesi sağlanmalıdır. Şekil 4.4'de olduğu gibi şifrelenmiş dosyanın yeniden byte formatında bir diziye aktarılarak matris çarpımından geçirildikten sonra orijinal dosyaya erişim sağlanır. Burdaki çarpımda yine anahtar matrisin (A) ters matrisi (I) işleme konulur. İşlem sonucunda dosyanın byte kodlarına ulaşılır.



Şekil 4.4. Dosya deşifreleme.

Bu şekilde yapılan şifrelemelerle dosya ve içerik güvenliği oldukça güçlü bir yapıya sahip olur. Özellikle içerik ve dosya şifrelemelerinde kullanılan anahtarın da sürekli değişken olduğu düşünülürse, sistemin kırılması bir hayli zor bir duruma gelecektir.

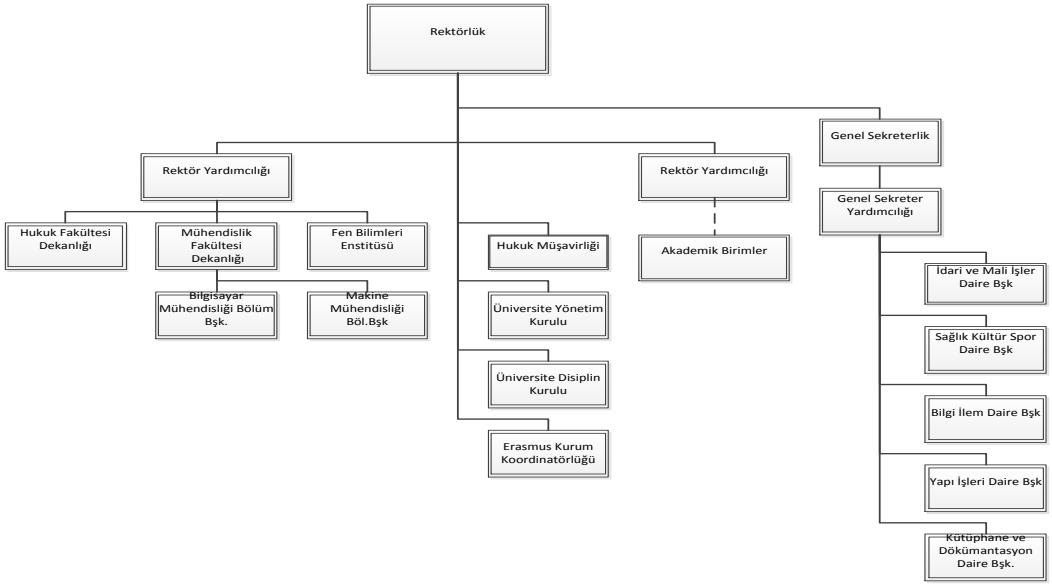
BÖLÜM 5

SİSTEM ÇALIŞMA ALGORİTMASI

5.1. ORGANİZASYON ŞEMASI

Sistemde kurumların organizasyon şemalarına uygun olarak yerleştirilen bir ast-üst ilişkisinin de bulunduğu yapı söz konusudur. Şekil 5.1'de duruma ilişkin bir şema gösterilmiştir.

Örnek Üniversite için;
Rektör, Rektör Yardımcıları (Akademik birimler)
Mühendislik Fakültesi
Bilgisayar Bölüm Başkanlığı
Genel Sekreter (İdari Birimler)
Bilgi İşlem Daire Başkanlığı
İdari ve Mali İşler D.B.



Şekil 5.1. Kurum organizasyon şeması.

5.2. SİSTEMİN İŞLEYİŞİ

Sistem her uç birim içerisinde;

Birimin imza yetkilisi,

Birimin evrak sorumlusu,

Birimde çalışan memurlar

Bulunup imza yetkilisi olan kişi birim adına imza atma yetkisi olan (dekan, daire başkanı, vekilleri vb.) kişidir. Bu imza ıslak ya da elektronik (eimza) olabilmektedir. Evrak sorumlusu ise birime gelen tüm evrakları alan birim içinde ilgili kişiye havale yapabilen, birim içindeki evrak akışını yöneten kişidir. Bu role sahip kişi yetkili tarafından onaylanmış evrakları da diğer birimlere sevk edebilmektedir. Bu rol gelen ve giden evrak sorumlusu olarak ayrı ayrı kişilerde verilebilmektedir. Birimde çalışan memurlar evrakı hazırlarlar, cevaplanacak bir evrak var ise cevabı hazırlarlar ve işleri bittikten sonra evrak sorumlusuna ya da birim yetkilisine havale ederler. Hazırlık aşamasında dilerlerse birim içindeki bir başka memura da havale edebilirler. Örnek senaryolar;

Kurum içindeki bir idari Birim ile idari birim arasındaki evrak akışı

Kurum içindeki bir idari Birim ile Akademik birim arasındaki evrak akışı

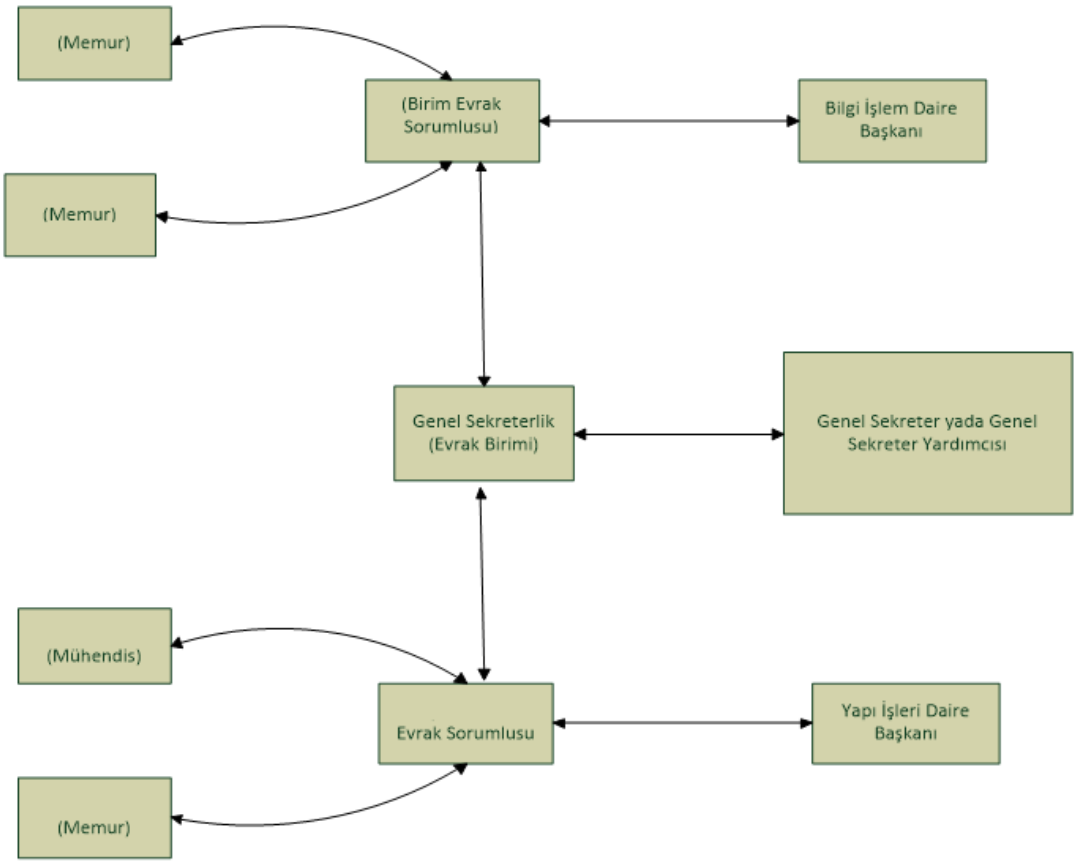
Kurum içindeki bir Akademik birim ile Akademik birim arasındaki evrak akışı

Rektörlükten tüm birimlere toplu gönderim

Kurum dışından idari bir birime evrak akışı senaryolarının işleyiş biçimi aşağıda anlatılmaktadır.

5.3. İDARİ BİRİMLER ARASINDAKİ EVRAK AKIŞI

Örnek: Bilgi işlem daire başkanlığı, Yapı işleri daire başkanlığına yeni binanın veri kablolama işleri hakkında bir evrak gönderdiğini varsayalım evrakta yeni binaya döşenecek olan fiber kablonun yaklaşık olarak metrajı istenmektedir. Şekil 5.2'de örneğe ilişkin şema gösterilmiştir.



Şekil 5.2. İki idari birim arasındaki evrak akış şeması.

Resmi Yazı Örneği:

Sayı : 75153282 / 61 Tarih: 07.05.2013

Konu : Kablolama

GENEL SEKRETERLİĞE

(Yapı İşleri Daire Başkanlığı)

Üniversitemizin Ovacık yerleşkesindeki yeni binasına döşenmesi için uygun görülen fiber kablo miktarının tarafımıza bildirilmesi gerekmektedir.

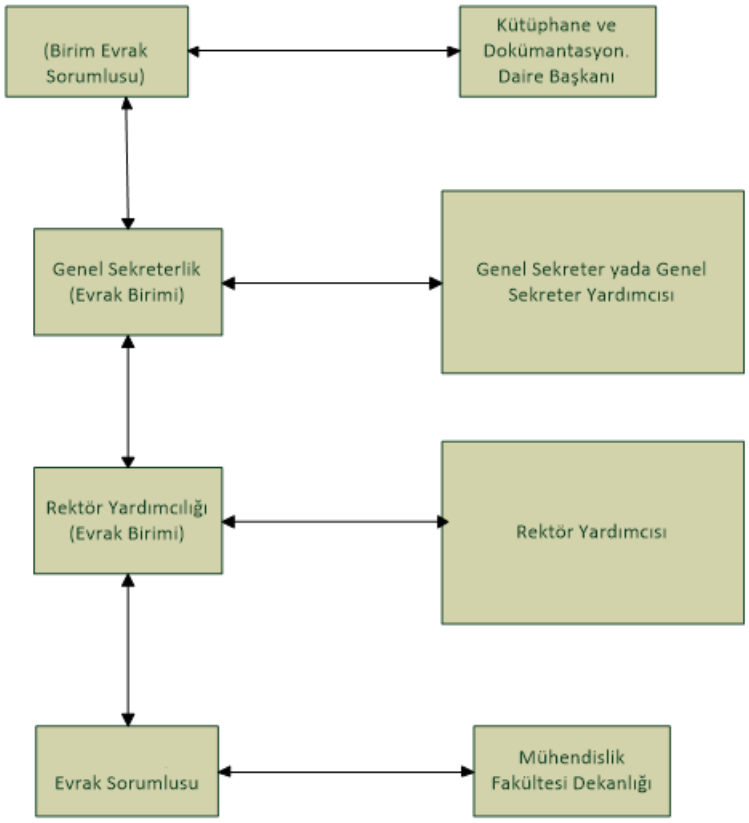
Bilgilerinizi ve gereğini arz ederim.

İMZA

Bilgi işlem dairesinde çalışan birinci memura daire başkanlığı bu konuda yazı yazması talimatını verdikten sonra, memur evrakı hazırlar ve taslak olarak kaydedip evrak sorumlusuna havale eder. Memur işe yeni başladığı için evrak sorumlusu olan diğer memura evrakta bir takım yazım usul hataları tespit edip, düzeltmesi için birim içindeki tecrübeli ikinci memura havale eder. Bu memur evrakı kontrol eder ve düzelttikten sonra gönderir. Evrak sorumlusu evrakı daire başkanına gönderir. Daire başkanı da evrakı onayladıktan sonra dilerse göndermesi için evrak sorumlusuna havale eder, dilerse de kendisi direk olarak alıcı birime (Yapı İşleri Daire Bşk.) gönderir. Evrak birimden çıktığı anda birim evrak defterine kaydolup tarih ve sayı alır. Aynı zamanda da karşı birimin gelen evrak defterinden tarih ve sayı almış olur. Yani bir birimin giden evrakı diğer birimin gelen evrakıdır. Her iki idari birimler haberleşmelerini Genel Sekreterlik Üzerinden yapacakları için Bilgi İşlem Daire Bşk. den çıkan evrak Yapı işlerine değil de genel sekreterliğe gelir. Genel sekreterlikten gerekli onay alındıktan sonra, evrak yapı işlerine ulaşır. Yapı işlerinde evrak sorumlusu (gelen evrak memuru) tarafından kontrol edilmesi için Daire başkanına havale edilir. Daire başkanı da bu konuda gerekli cevabın hazırlanması için Elektrik mühendisi olan memura havale eder.

5.4 İDARİ BİRİM VE AKADEMİK BİRİM ARASINDAKİ EVRAK AKIŞI

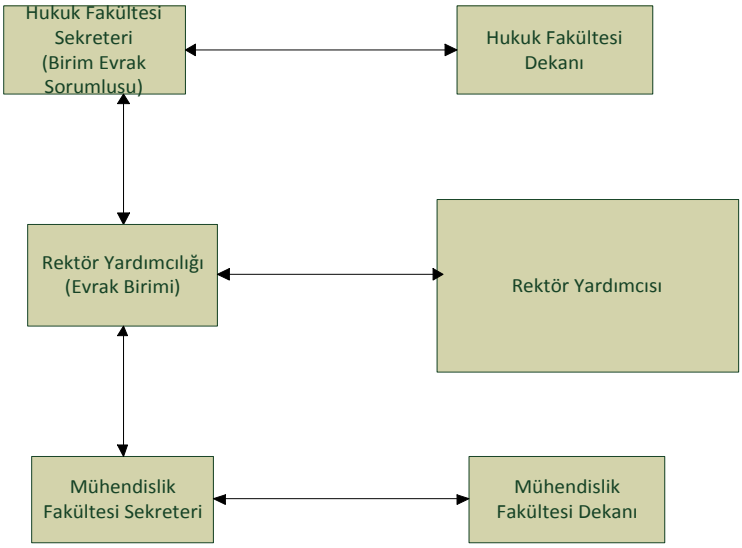
Örnek: Kütüphane ve Dokümantasyon Daire Başkanlığında görevli memur, kütüphane arşivine eklenecek olan yeni mühendislik ders kitapları bilgilerinin kendilerine ulaştırılması için Mühendislik ve Doğa Bilimleri Fakültesine bir talep yazısı hazırlamış ve göndermiştir. Yazı, Kütüphane ve Dokümantasyon Daire Başkanlığının giden defterinden sayı alarak çıkış yapmış ve ilgili fakültenin üst birimi olan Rektör Yardımcılığının gelen evrakları arasına kaydedilmiştir. Rektör yardımcılığı daire başkanlığından gelen bu evrakı onaylayana kadar evrak fakülteye ulaşmayacaktır. Daire başkanlığından gelen evraka rektör yardımcılığı tarafından onay verildikten sonra evrak, rektör yardımcılığının giden defterinden sayı alarak fakültenin gelen defterine işlenir. Fakülte evrak sorumlusu, daire başkanlığından gelen bu evrakı inceledikten sonra onay vererek evrakı kabul etmiş olur. Şekil 5.3'de örneğe ilişkin şekil gösterilmiştir.



Şekil 5.3. İdari birim ile akademik birim arasındaki evrak akış şeması.

5.5. AKADEMİK BİRİMLER ARASINDAKİ EVRAK AKIŞI

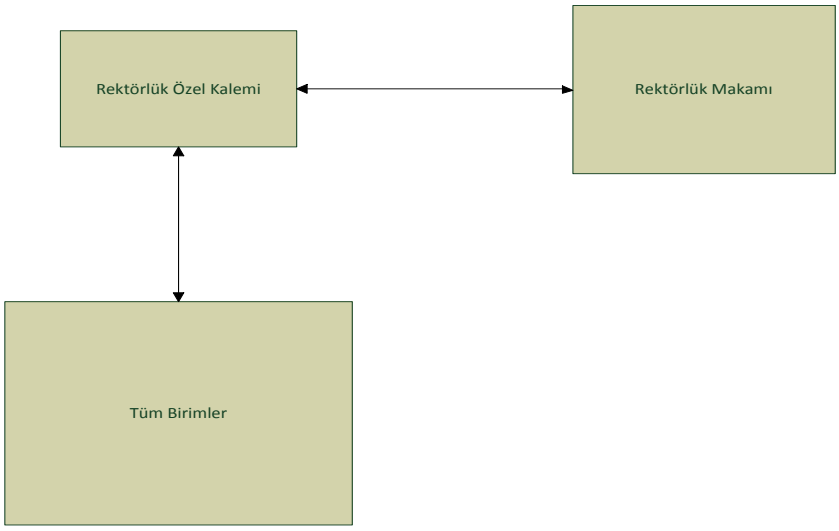
Örnek: Hukuk Fakültesi sekreteri olan memur, dekanlığın talebiyle Mühendislik ve Doğa Bilimleri Fakültesine Hukuk Fakültesi öğrencileri için yeni dönemde açılacak olan Comp101 dersi için hazırlanan ders programı hakkında bilgi talebinde bulunduğu bir yazı hazırlar. Evrakı gönderme esnasında, istenilen belgenin hangi formatta olacağına dair bir örnek teşkil eden ek belgeyi de gönderilecek evraka iliştirerek yazıyı gönderir. Gönderilen evrak Hukuk Fakültesi Dekanlığının giden evrak defterinden uygun sayıyı alarak fakülteden çıkış yapar ve Hukuk Fakültesi üst birimi olan ilgili rektörlük makamının gelen evrak defterinden sayı alarak giriş yapar. Rektörlük makamı bu yazıyı inceledikten sonra onay vererek evrakın birimden çıkış sayısını alarak varış birimine (Mühendislik ve Doğa Bilimleri Fakültesi) ulaşmasını sağlar. Mühendislik ve Doğa Bilimleri Fakültesinin evrak sorumlusu kişi, kendilerine gelen bu evrakı onayladıktan sonra ilgili memura havalesini yapar. Örneğe ilişkin şema Şekil 5.4'te gösterilmiştir.



Şekil 5.4. İki akademik birim arasındaki evrak akış şeması.

5.6. REKTÖRLÜKTEN TÜM BİRİMLERE TOPLU GÖNDERİM

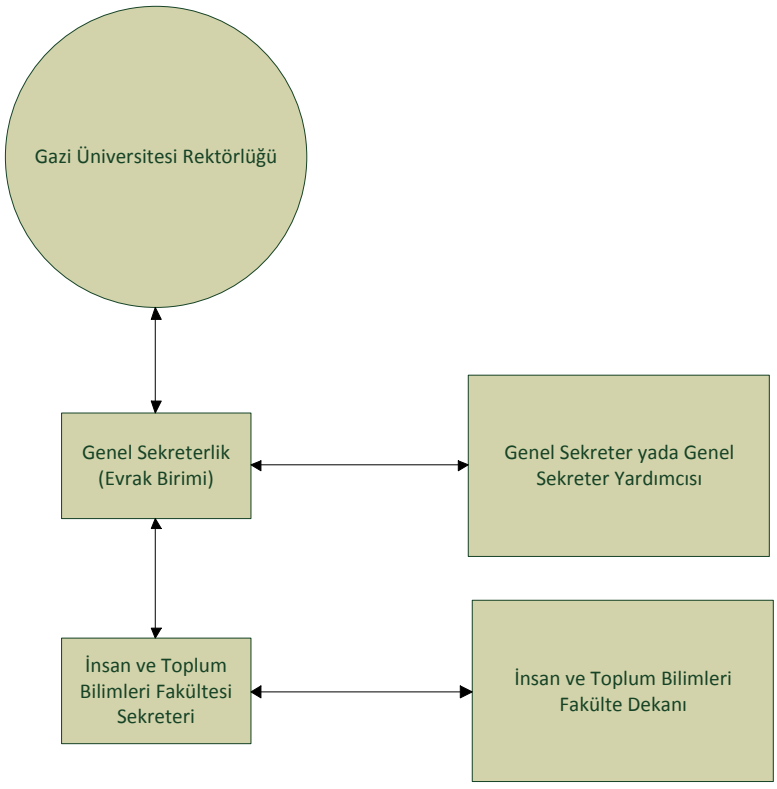
Örnek: Rektörlük makamının talimatıyla yaz dönemi için çalışanların ceket ve kravat kullanma zorunluluğunun olmadığını bildiren yazı, rektörlük özel kalem memurları tarafından tüm birimlere dağıtılmak üzere hazırlanır. Üniversite bünyesindeki tüm birimler seçilerek evrak gönderilir. Gönderilen bu evrak Rektörlük Makamının giden defterinden yeni bir sıra alınarak kaydedilir ve tüm birimlere aynı sayı ile gönderilmiş olur. Örneğe ilişkin şema sekil 5.5'te gösterilmiştir.



Şekil 5.5. Rektörlükten tüm birimlere evrak akış şeması.

5.7. KURUM DIŞINDAN İDARİ BİR BİRİME EVRAK AKIŞI

Örmek: Gazi Üniversitesi Rektörlüğü, kurumun İnsan ve Toplum Bilimleri Fakültesinin Doğu Dilleri ve Edebiyatları Bölümünde görev yapan bir öğretim üyesinin, belirtilen dersleri 2012-2013 bahar yarıyılında üniversitelerinde vermesi için bir görevlendirme talebinde bulunduğu yazı kurumun Genel Sekreterlik gelen evrak birimine ulaşmıştır. Birimde görevli memur, Gazi Üniversitesinden gelen bu yazıyı tarayıcı vasıtası ile taratarak sistem üzerine gerekli bilgileri de girdikten sonra yeniden düzenlenebilir bir şekilde kaydeder. Daha sonra genel sekreterlik makamının evrak sorumlusu olan kişi, Gazi Üniversitesinden gelen bu yazıyı inceleyip gerekli işlemleri yaptıktan sonra ilgili fakülte olan İnsan ve Toplum Bilimleri Fakültesine yönlendirir. Bu işlemlerin yapılması aşamasında, dış birimden gelen bu evrak üniversitenin genel sekreterlik biriminin hem gelen hem de giden defterinden sayı alınarak yönlendirilmiş olur. Son olarak da evrak, İnsan ve Toplum Bilimleri Fakültesinin gelen defterinden sayı alarak fakülteye giriş yapmış olur. Örneğe ilişkin şema Şekil 5.6'da gösterilmiştir.



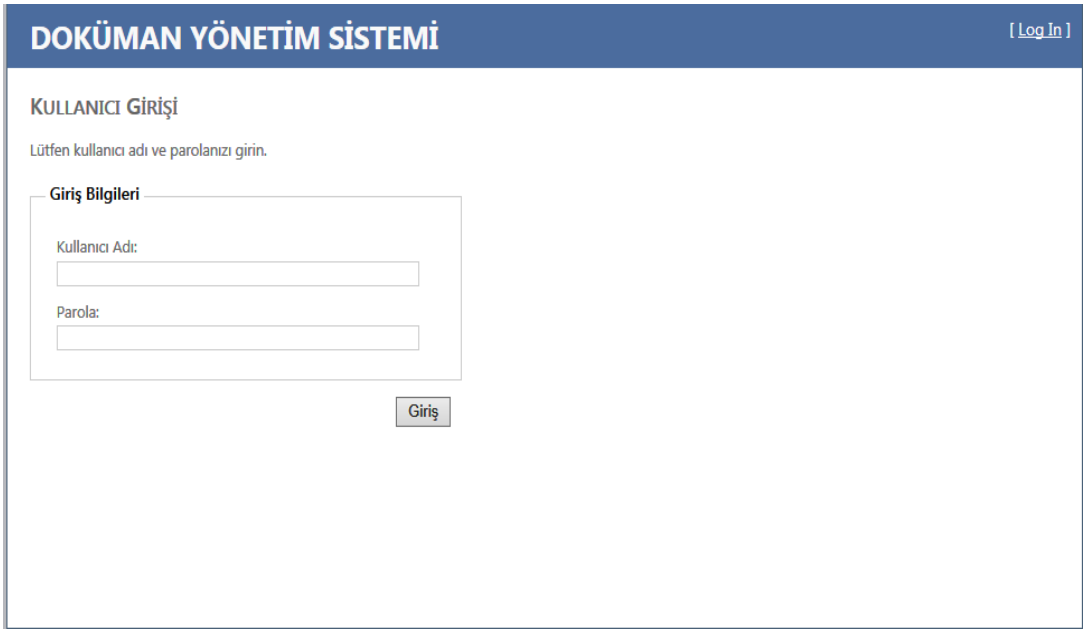
Şekil 5.6. Dış birimden bir idari birime evrak akış şeması.

BÖLÜM 6

KULLANICI ARAYÜZLERİ

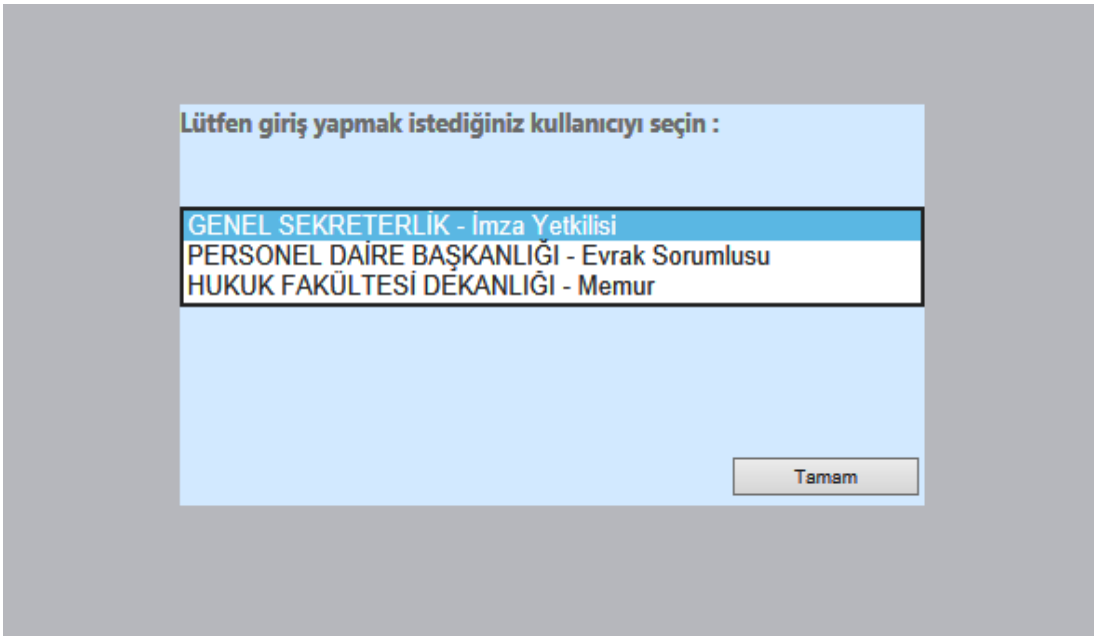
6.1. SİSTEME GİRİŞ VE ROL SEÇİMİ

Sistem web tarayıcıdan (tercihen internet explorer) çalıştırıldığında ilgili kullanıcının oturum açma ekranı gelir. Şekil 6.1' de oturum açma ekran görüntüsü verilmiştir.



Şekil 6.1. Oturum açma ekran görüntüsü.

Sisteme giriş yapıldıktan sonra özellikle farklı görevlerde olan personeller için sisteme hangi görevle gireceğini soran sayfa gelir. Bu sayfada kullanıcının vekâlet ettiği diğer kullanıcıların birimleri ve yetkileri listelenmektedir. Kullanıcı bu sayfadan hangi kullanıcı ile giriş yapmak istiyor ise onu seçerek devam eder. Şekil 6.2' de bu sayfanın ekran görüntüsü verilmiştir.

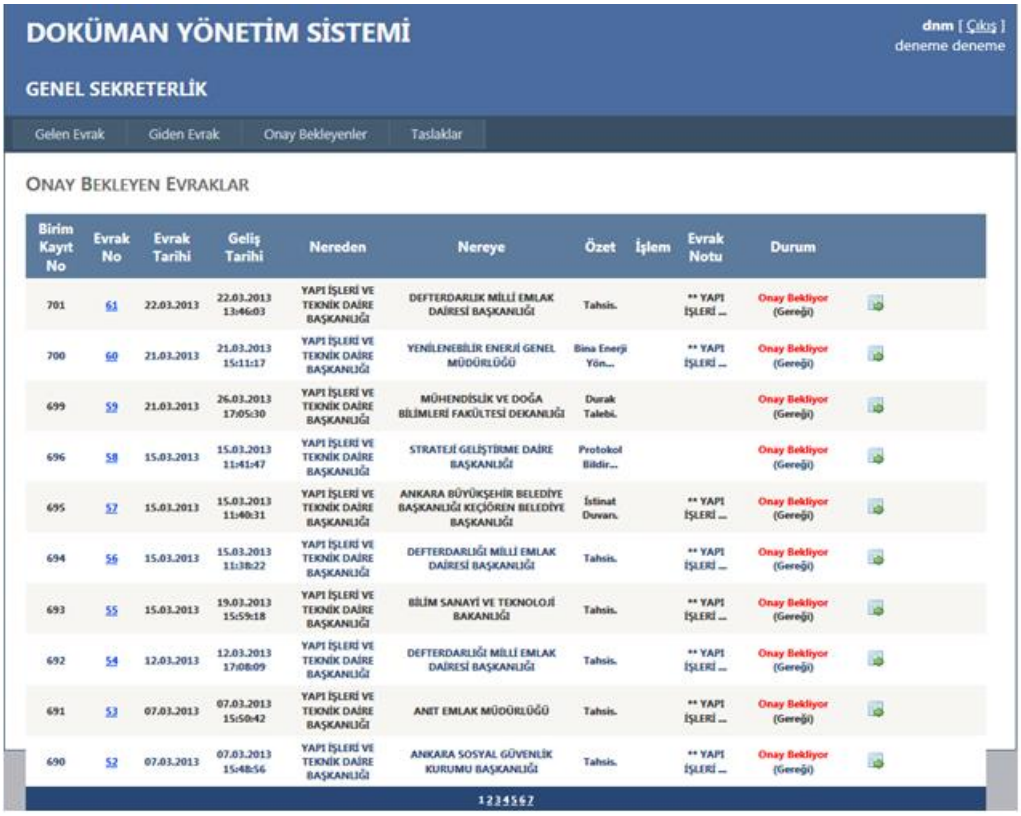


Şekil 6.2. Kullanıcının giriş yetkilerinin listelendiği ekran.

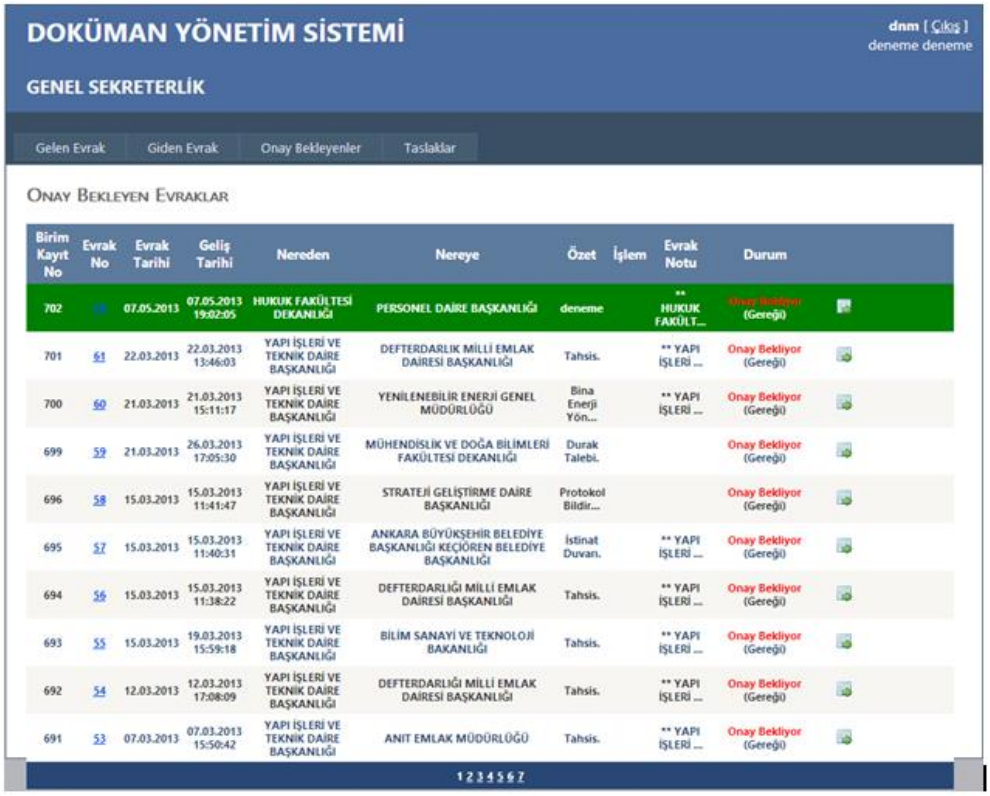
Bu ekran personelin hem bölüm başkanı hem de dekan ya da vekili gibi farklı birkaç görevi varsa hangi rolle giriş yapmak istediğinin sorulduğu ekrandır.

6.2. ONAY BEKLEYENLER

Gerekli olan kullanıcı rolü seçildikten sonra kullanıcıya ait gelen evrakların listelendiği Şekil 6.3' te gösterilmiş olan ekran alıntısındaki sayfa görüntülenir. Bu ekran bir çeşit bekleme (stand by) ekranıdır. Tarayıcı üzerinde bu sayfa açık olduğu sürece sistem her beş dakikada bir sunucudan istemde bulunur. Yani birime gelen yeni bir evrak olup olmadığı sorgulanır. Bu sorgulama süresi isteğe bağlı olarak uzatılıp kısaltılabilir. Eğer birime yeni bir evrak gelmiş ise aynı ekran üzerindeki tablo (gridview) güncellenir ve yeni evrak ilk sırada görüntülenir. Ekrana yeni bir evrak düştüğü bilgisini kullanıcıya vermek için yeni satır arka plan rengi değiştirilir ve aynı zamanda bir uyarı sesi ile kullanıcı uyarılır. Böylece kullanıcı o sırada başka bir ekranı kullanıyor dahi olsa sistem üzerinden yeni bir evrak geldiği bilgisini almış olur. Bu da kullanıcıyı sürekli ilgili ekranı takip etme zahmetinden kurtarmış olur. Bu durum Şekil 6.4' teki ekran alıntısında gösterilmiştir.



Şekil 6.3. Onay bekleyenler sayfası ekran görüntüsü.

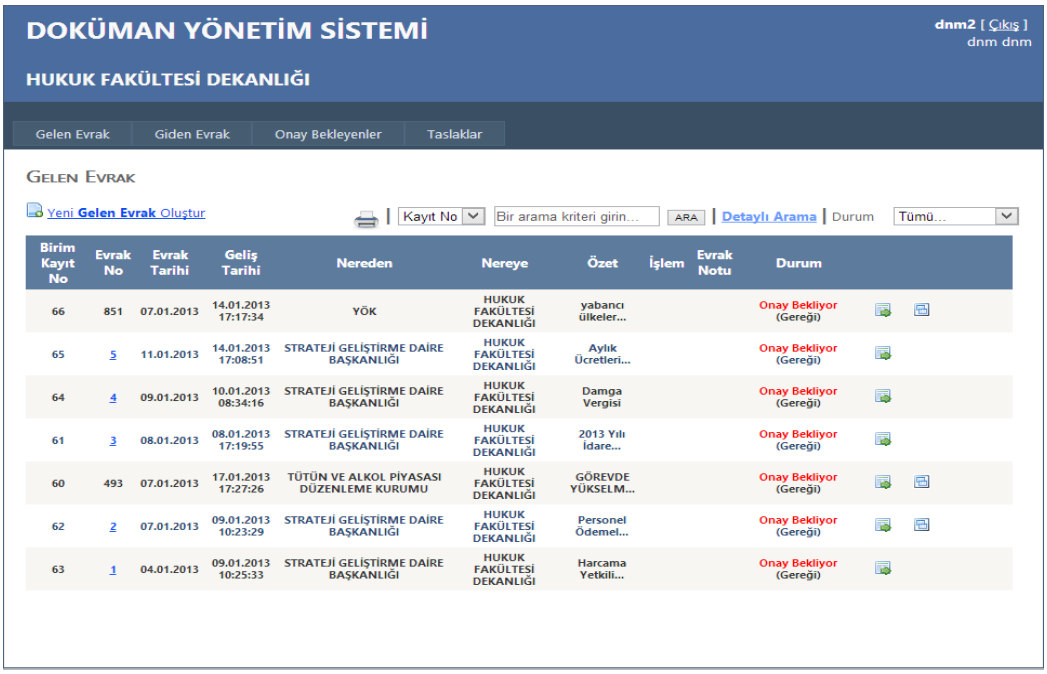


Şekil 6.4. Onay bekleyenler yeni evrak bilgisi görünümü.

“Onay Bekleyen Evraklar” adını verdiğimiz bu sayfada sadece birime yeni gelmiş ve onay beklemekte olan evraklar listelenir. Birimin evrak sorumlusu ya da yetkili kişisi bu ekranda, birime gelip onay bekleyen tüm evrakları görebilir. Bu ve diğer açıklaması yapılacak olan sayfalarda aynı datagrid kullanılmış olup, bu datagrid üzerinde bulunan tüm sütunlar ayrıntılı bir şekilde açıklanacaktır.

6.3. GELEN EVRAK

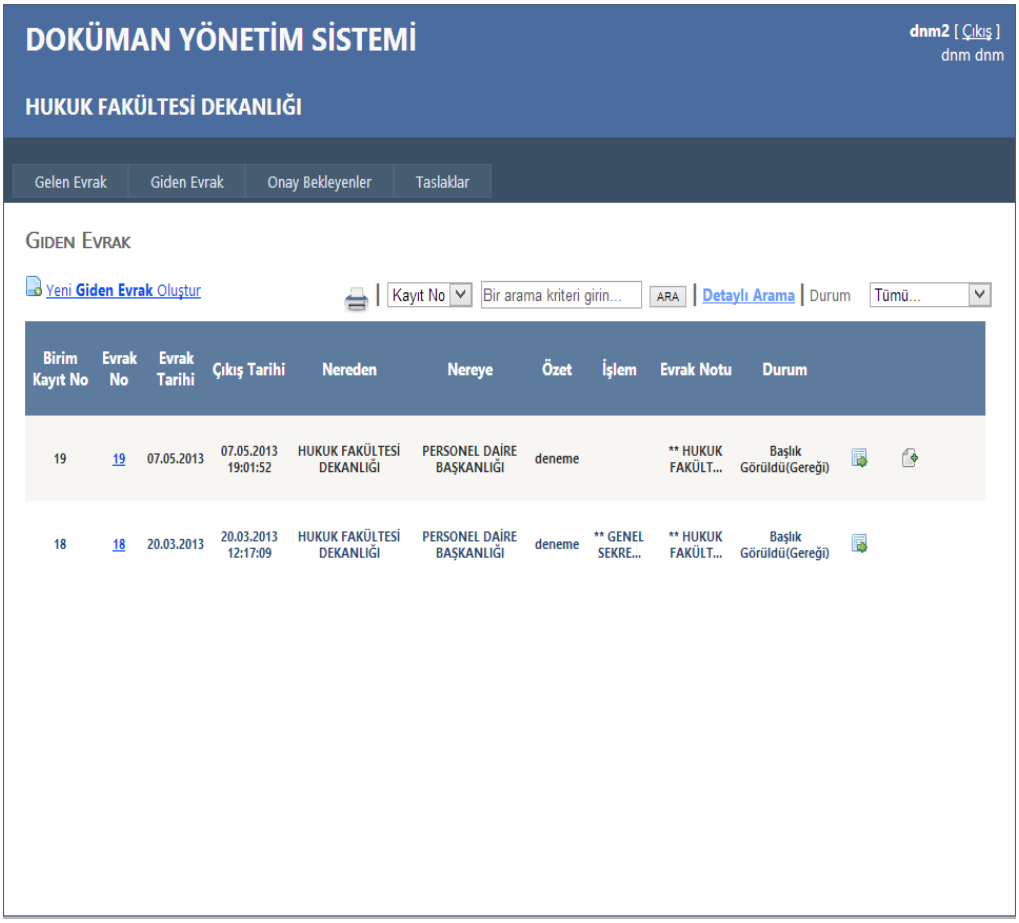
Ana şablonumuzda bulunan “Gelen Evrak” bağlantısı üzerinden erişilebilen sayfa, birime içeriden ya da dışarıdan gelen her türlü evrakın listelendiği sayfadır. Diğer sayfalarda da olduğu gibi bu sayfada da kullanıcı yetkisi dahilinde olan evrakları görecektir. Bu sayfada da bir önceki anlatılan sayfadaki gibi aynı datagrid kullanılmıştır. “Gelen Evrak” sayfasında sadece onay bekleyen evraklar değil, diğer farklı durumlara sahip evraklar da görüntülenir. Farklı durumlardan kasıt, datagrid üzerindeki “Durum” sütununda evrakın durumunun gösterildiği alanın alabileceği değişik değerlerdir. Bu konu da ilerleyen bölümlerde datagrid üzerindeki alanların anlatılacağı kısımda detaylarıyla açıklanacaktır. Şekil 6.5’te “Gelen Evrak” sayfasına ait ekran görüntüsü verilmiştir.



Şekil 6.5. Gelen evrak ekran görüntüsü.

6.4. GİDEN EVRAK

Bu bölüme girildiğinde standart olarak giden evrak listesi ekrana gelir. Bu liste de diğer sayfalardaki listeler gibi kişiye özeldir. Yani kişinin göndermiş olduğu evrakların listesidir. Ancak kişi imza yetkilisi ya da evrak sorumlusu ise birime ait giden tüm evrakları görebilir. "Giden Evrak" sayfasına ilişkin ekran alıntısı Şekil 6.6'te verilmiştir.

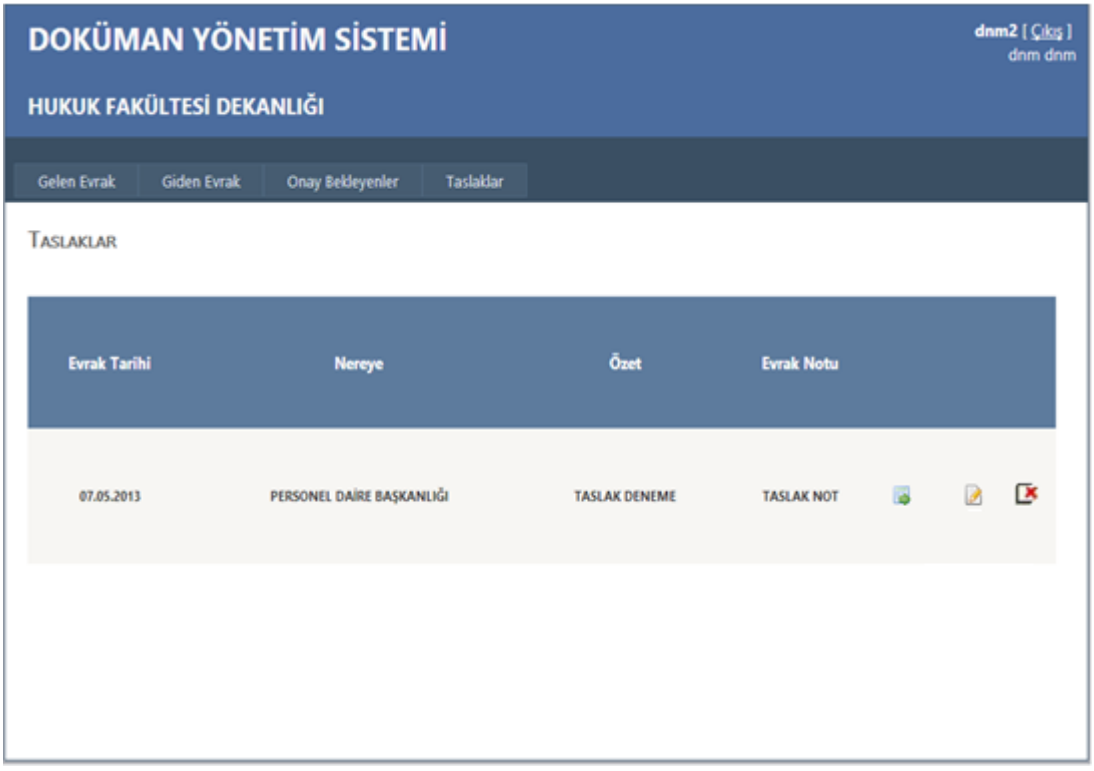


Şekil 6.6. Giden evrak ekran görüntüsü.

Eğer kişi yeni bir evrak hazırlayıp göndermek isterse aynı ekranda bulunan "Yeni Giden Evrak Oluştur" linkine tıkladığı anda yeni bir giden evrak oluşturması için giden evrak hazırlama ekranı gelir.

6.5. TASLAKLAR

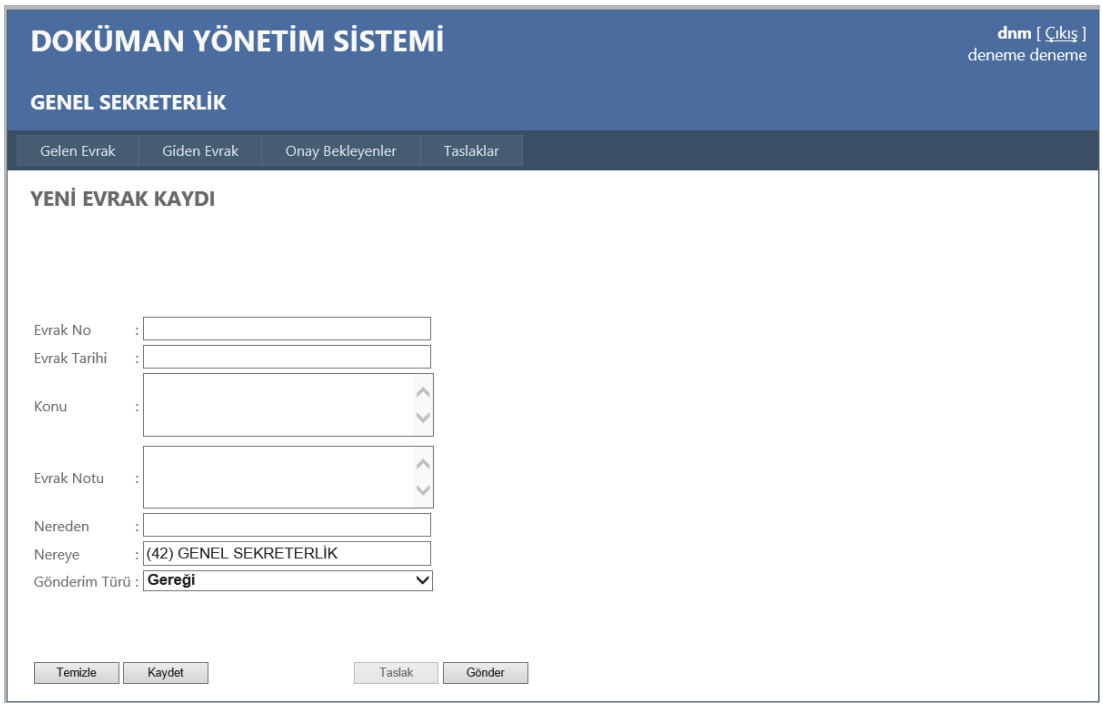
Bu bölümde taslak olarak kaydedilen evraklar bulunmaktadır. Taslaklar linki üzerinden erişilebilen bu sayfada evraka ait minimum sayıda veri girilerek sisteme kaydedilir. Bir evrakın taslak olarak kaydedilmesi demek, evrakın gelen ya da giden defterinden herhangi bir sayı almadan sadece bir şablon olarak saklanmasıdır. Yani evrak yeniden düzenlenebilir halde sistem veri tabanında tutulur. Bu sayede kullanıcı ileri bir tarihte oluşturması muhtemel olan bir takım evrakları önceden taslak olarak kaydederek, daha sonra üzerinde çalışabileceği bir şablon oluşturmuş olur. Taslaklar sayfasında sadece evrakın tarihi, hangi birimden çıkış yaptığı, özeti ve eğer yazılmışsa evraka ait not bilgileri bulunmaktadır. Şekil 6.7'da gösterilmiş olan taslaklar sayfası üzerinde bulunan düzenleme linki sayesinde evrak bilgileri düzenleme ekranına taşınarak üzerinde gerekli işlemler yapılabilir.



Şekil 6.7. Taslaklar sayfası ekran görüntüsü.

6.6. YENİ EVRAK

Kullanıcıların yeni evrak oluşturmak için kullandığı bu sayfaya, hem gelen evrak hem de giden evrak sayfalarında bulunan yeni (gelen, giden) evrak oluştur linkleriyle erişilebilmektedir. Şekil 6.8'de ekran görüntüsü verilen bu sayfa yardımıyla gelen ve giden yeni evrak oluşturulabilmektedir. Bu sayfada oluşturulacak olan evrakın, kullanıcı tarafından girilen evrak bilgilerinin analizi sonucu evrakın türü giden evrak ya da gelen evrak olarak değer kazanır. Kullanıcı ayrıca evrak türüyle ilgili bir bilgi girişi yapmaz.



Şekil 6.8 Yeni evrak sayfası ekran görüntüsü.

Sayfanın alt kısmında bulunan butonlar kullanıcının yetkisine göre aktif ya da pasif duruma geçmektedir. Bu fonksiyon butonlarının ilki olan "Temizle" butonu adından da anlaşılacağı üzere formdaki tüm verileri temizlemektedir. Bir sonraki "Kaydet" butonunun görevi ise, evrak bilgilerini aldıktan sonra evrakın birimden çıkış yapmadan tekrar düzenlenebilir halde saklanmasıdır. Yani evrak bilgileri veri tabanına kaydedilir ve yeniden düzenlenebilir bir halde tutulur. "Taslak" adlı butona tıklandığındaysa evrak herhangi bir sayı almadan yine "Kaydet" butonundaki gibi yeniden düzenlenebilir bir şekilde ve de silinebilir bir yapıda veri tabanına

kaydedilir. Birimin gelen ya da giden defterlerine herhangi bir kayıt yapılmaz. “Kaydet” butonunda saklanan evrak bilgileri birimin gelen ya da giden defterlerine işlendiğinden mevzuat gereği silinmeleri mümkün değildir. Ancak “Taslak” butonunda yapılan kayıt herhangi bir deftere işlenmediğinden üzerinde istenildiği kadar değişiklik yapılabilir hatta silinebilir. Son olarak sayfada bulunan “Gönder” butonunda ise evrak bilgileri yine alındıktan sonra birim defterlerinden sıra numaraları alınarak ve karşı birimin de gelen defterinden sıra alınarak evrak bilgileri kayıt altına alınmaktadır. “Gönder” butonu ile evrak kaydedildiğinde evrak düzenlemeye kapatılır. Sistem bu evraklar üzerinde herhangi bir değişiklik yapılmasına izin vermez.

BÖLÜM 7

SONUÇLAR

DYS'nin kurum içerisinde uygulanması ile birlikte kurumların karar alma ve uygulama süreçleri çok hızlanmış, kurumlar daha dinamik bir yapıya kavuşmuşlardır. Evrak akışının dijital platformda gerçekleşmesi zorunlu tutulacağı zaman, DYS kullanıcıları için güvenli e-imza, kurum içinde güvenli e-imza kütüphanesinin hayata geçirilmesi ile dijital ortama taşınacak evrak işlem ve onay süreçlerinin daha süratli gerçekleşmesi ile kurumsal verimlilikte önemli bir artış meydana gelecektir. Bu durum aynı zamanda benzer işi yapan personeller arasındaki çalışma verimliliğinin takibi imkânını da sunduğu için ileriki aşamalarda performansa dayalı bir ücretlendirme sisteminin de alt yapısını oluşturmaktadır.

Tüm kurum ve kuruluşlarda bilgi ve belgelerin elektronik ortama taşınması beraberinde bu bilgi ve belgelerin güvenliği konusunu da ön plana çıkarmaktadır. Evrak ve belgelerin dijital ortamda tutulması, kurumlara büyük avantajlar sağlaması yanında önemli ölçüde bir güvenlik riskini de meydana getirmektedir.

Doküman yönetim sistemlerinin sahip olması gereken en önemli özelliklerden birisi de bünyesinde barındırdığı bilgi ve belgelerin güvenliğinin en iyi derece de sağlanması ve gizliliklerinin en üst seviyede korunmasıdır. İncelenen uygulamalarda ya hiçbir güvenlik önleminin alınmadığı ya da güvenliğin veri tabanı güvenliğine bırakıldığı görülmüştür. Özellikle taranarak sistem üzerinde saklanan evrakların, belgelerin güvenliği konusunda hiçbir önlem alınmamaktadır. Bu dosyaların saklandığı sunuculara yapılması ihtimal saldırılar sonucunda belge ve bilgiler tamamen korunmasız kalmakta ve ilgili kurumun belgeleri üçüncü şahısların ellerine geçebilmektedir. Bu noktada yapılması gereken, bu bilgi ve belgeler yetkisiz ellere geçse bile bu belgelerin içeriklerine ulaşılamaz ve kullanılamaz halde olmasını

sağlamaktır. DYS' de ortaya konulan bu yeni güvenlik yapısıyla sistem üzerinde oluşturulan yeni evrakların içerikleri ve taranarak sisteme aktarılan belgeler, oluşturulan yeni kripto algoritmasından geçirilerek güvenli bir hale getirildikten sonra ilgili alanlarda saklanmaktadır. Algoritmada tek bir anahtar yerine birden fazla ve değişken bir anahtarın kullanılması da güvenliğin üst seviyelere taşınmasını sağlamıştır. Ayrıca web tabanlı olan yeni uygulamada verilerin ağ üzerindeki hareketleri sırasında oluşabilecek güvenlik açıklarının, belirli ücretler karşılığında elde edilebilecek SSL sertifikalarının sisteme entegre edilmesiyle kapatılması, sistem güvenliğinin en üst düzeye erişmesini sağlayabilir.

Sonuç olarak oluşturulan bu yeni uygulamayla, kullanıcıların kolayla öğrenebileceği, kolay uygulanabilir, anlaşılır ve kolay kullanılabilen sade ara yüzlere sahip ve de bilgi ve belgelerin üst düzey bir güvenlik önlemiyle korunduğu bir yapı ortaya çıkarılmıştır.

KAYNAKLAR

1. İnternet: Resmi Gazete, "2004 Resmi Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelik", **http://www.resmigazete.gov.tr/eskiler/2004/12/20041202.htm#3** (2004).

2. İnternet: Sayıştay Dergisi, "2012 Elektronik Belge Yönetim Sistemi (EBYS) 'nin Faydaları ve Kurum Bünyesinde EBYS Yapılandırmaya Yönelik Bir Yol Haritası", **http://dergi.sayistay.gov.tr/icerik/der85m1.pdf** (2012).

3. İnternet: Resmi Gazete, "Elektronik Belge Standartları ile İlgili 2008_16 Sayılı Başbakanlık Genelgesi", **http://www.resmigazete.gov.tr/eskiler/2008/07/20080716-7.htm** (2008).

4. Kauffman, J. ve Millington, B., "ASP.NET ile Veritabanı Uygulamaları, 2. Basım", Üçüncüoğlu, C. B. (Ed.), Çömlekçi, K. (Çev.), ***Bilge Adam,*** İstanbul, 61-87 (2008).

5. Nagel, C., Evjen, B., Glynn, J., Watson, K. ve Skinner, M., ".NET Framework ile İleri C# Uygulamaları, 1", Kilyusufoğlu, H. (Ed.), Çelebi, A., Işık, H., Al, K., Çolak, S., Tezcan, Ü. (Çev.), ***Bilge Adam***, İstanbul, 163-378 (2008).

6. Yerlikaya, T., "Yeni şifreleme algoritmalarının analizi", Doktora Tezi, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü***, Edirne, 6-7 (2006).

7. Yerlikaya, T., Buluş, E. ve Buluş, H. N., "Eliptik eğri aritmetiği ve şifrelemede kullanılması", ***Sinyal İşleme ve İletişim Uygulamaları Kurultayı***, Antalya, 35-46 (2006).

8. Yıldırım, K., "Veri şifrelemesinde simetrik ve asimetrik anahtarlama algoritmalarının uygulanması (Hybrit şifreleme)", Yüksek Lisans Tezi, ***Kocaeli Üniversitesi Fen Bilimleri Enstitüsü***, Kocaeli, 1-7 (2006).

9. Bayar, E., "Modern kriptosistemlerle şifrelemenin modellenmesi ile veri güvenliğinin sağlanması", Yüksek Lisans Tezi, ***Marmara Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 3-19 (2012).

10. Apohan, A. M., "Gündelik hayatta kriptoloji", ***Bilim ve Teknik,*** 1: 48-49 (2009).

11. Buluş, H. N., "Temel şifreleme algoritmaları ve kritpanalizlerinin incelenmesi", Yüksek Lisans Tezi, ***Trakya Üniversitesi Fen Bilimleri Enstitüsü***, Edirne, 20-21 (2006).

12. İnternet: Tübitak, "Açık İletişim Ağlarında Bilgi Güvenliği", **http://www.tuena.tubitak.gov.tr/rapor/pdf/2103-M-T-A-02.pdf** (2002).

13. Koltuksuz, A., "Elektronik ticarette güvenlik, özgürlük denetimi, doğruluk – bütünlük ve sayısal imza", ***4. Türkiye İnternet Konferansı***, İstanbul, 47-49 (1998).

14. Denton, B., "Evaluation of cryptographic constructions properties and security requirements of secure hashing algorithms", M. Sc. Thesis, ***Alabama University Department of Electricity and Computer Engineering***, Alabama, US, 17-55 (2011).

15. İnternet: Kamu Sertifikasyon Merkezi, "Basit Şifreleme Teknikleri", **http://www.kamusm.gov.tr/dosyalar/rehberler/guvenli_belge_rehberi.pdf** (2011).

16. İnternet: Yunus, A., "İnternette Veri Güvenliği", **http://yunus.hacettepe.edu.tr/~umutal/publications/datasecurity.pdf** (2012).

17. İnternet: İstanbul Teknik Üniversitesi, "İnternet Güvenliğine Bir Bakış", **http://www.itu.edu.tr/bid/bilgi/guvenlik2.htm** (2002).

18. İnternet: Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, "Şifreleme Bilimi", **http://ceng.gazi.edu.tr/~guvenlik/BBG4.pdf** (2009).

19. Yerlikaya, T., Buluş, E., ve Arda, D., "Asimetrik kripto sistemler ve uygulamaları", ***II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi***, İstanbul, 26-33 (2005).

20. Başkök, M. D., "AES şifreleme algoritmasının modellenmesi", Yüksek Lisans Tezi, ***Gazi Üniversitesi Fen Bilimleri Enstitüsü***, Ankara, 19-22 (2007).

ÖZGEÇMİŞ

Burhan GÜVEN 1983'te Konya'da doğdu. İlk, orta ve lise öğrenimlerini Konya'da tamamladı (1999). Doğu Akdeniz Üniversitesi'nde başladığı lisans eğitimini Ankara'da Atılım Üniversitesi'nde tamamladı (2004). 2009 yılında başladığı lisansüstü eğitimini Karabük Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda tamamladı. Kısa bir süre Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı Yazılım Geliştirme Departmanında görev aldıktan sonra özel bir şirketin yazılım geliştirme bölümünde çalıştı (2010). Yıldırım Beyazıt Üniversitesi Bilgi İşlem Daire Başkanlığı Yazılım Geliştirme Departmanı'nda 2012 yılında göreve başladı ve halen aynı yerde görevine devam etmektedir.

ADRES BİLGİLERİ

Adres : Yıldırım Beyazıt Üniversitesi
Bilgi İşlem Daire Başkanlığı
Ulus - Altındağ / ANKARA

Tel : (544) 746 7098

E-posta : burhan.guven@hotmail.com