BOZOK ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

MULTI FACTOR AUTHENTICATION

&

CENTRALIZED IDENDITY MANAGEMENT

PROJE ÖDEVİ RAPORU

YAVUZ ÇELİKER

2019-2020 BAHAR DÖNEMİ

İÇİNDEKİLER

1. MULTI FACTOR AUTHENTICATION

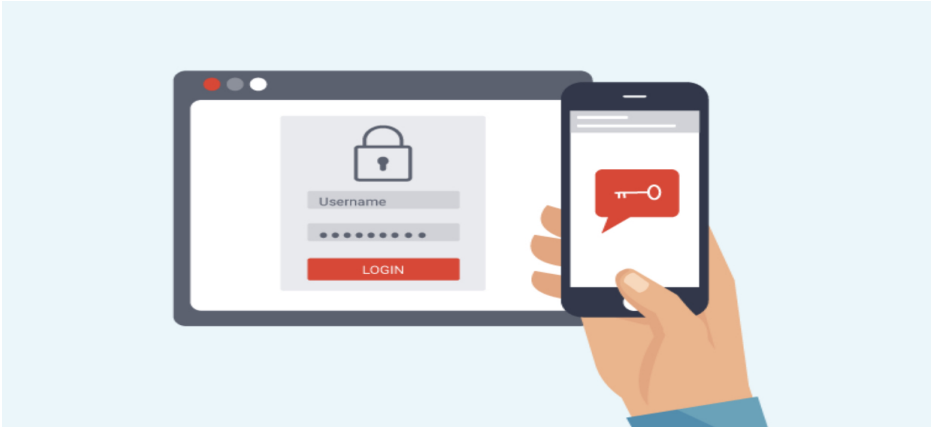
1.1. MULTI FACTOR AUTHENTICATION NEDİR?

Türkçeye "Çok Faktörlü Kimlik Doğrulama" olarak çevrilmiş olan Multi Factor Authentication, bir kimlik doğrulama sistemine iki veya daha fazla sayıda sadece kullanıcının bildiği bir kanıt sunularak, ilgili sisteme erişim izni verilen bir kimlik doğrulama sistemidir.

Şekil 1. MFA Örnek Gösterimi

1.2. TWO FACTOR AUTHENTICATION(2FA) NEDİR?

Türkçeye "İki Faktörlü Kimlik Doğrulama" olarak çevrilen 2FA, MFA'nın altında bulunan bir doğrulama sistemidir. 2FA genellikle sosyal medya hesapları, online oyunlar gibi birçok alandan aşina olduğumuz bir doğrulama sistemidir. Bu sistemde kullanıcı kimlik doğrulama sistemine genellikle bildiği bir şey ve sahip olduğu bir şey sunarak erişim izni kazanır.



Şekil 2. 2FA Örnek Gösterimi

1.3. KİMLİK DOĞRULAMA FAKTÖRLERİ

Birinin kimliğini doğrulamak için çoklu kimlik doğrulama faktörlerinin kullanımı yetkisiz bir kişinin erişim için gerekli faktörleri sağlayamaması ihtimali üzerine kuruludur. Bir erişim girişiminde parçalardan en az birinin eksik olması ya da hatalı sağlanması durumunda, kullanıcının kimliği kurulmayacak ve erişimi istenen ve çok faktörlü kimlik doğrulama sistemi ile korunan mülke (yapı ya da veri) bloke durumda kalacak.

Şekil 3. Parmak İzi ve Yüz Tanıma Örnek Gösterimi.

- Kullanıcının sahip olduğu bazı fiziksel nesneler, örneğin gizli token kullanan USB bellek, bir banka kartı, bir anahtar vb.
- Kullanıcı tarafından bilinen bazı sırlar, örneğin şifre, PIN, TAN, vb.
- Kullanıcının bazı fiziksel özellikleri (biyometri), örneğin parmak izi, iris, ses yazma hızı, tuşa basma aralıklarında desen vb.
- Lokasyonu tanımlamak için spesifik bir ağa bağlandığın ya da bir GPS sinyalini kullandığın bir yer.

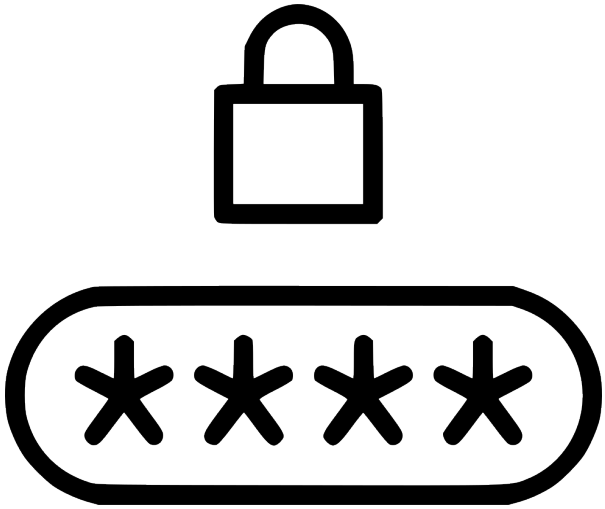
1.3.1. Bilgi Faktörleri

Bilgi faktörleri en yaygın kullanılan kimlik doğrulama şeklidir. Bu formda, kullanıcının kimliğini doğrulamak için bir sadece kendisine ait olan bir bilgiyi kanıtlaması gerekmektedir.

Parola, kullanıcı kimlik doğrulaması için kullanılan gizli bir kelime veya karakter dizisidir. Bu, en yaygın kullanılan kimlik doğrulama mekanizmasıdır. Birçok çok faktörlü kimlik doğrulama tekniği şifreye kimlik doğrulamanın tek faktörü olarak güvenir. Varyasyonlar, hem birden fazla kelimeden (parola ya da geçiş ifadesi) oluşan daha uzun şifreleri hem de ATM erişimi için

yaygın olarak kullanılan daha kısa, tamamı sayılardan oluşan, kişisel kimlik numaraları (PIN) içerir. Geleneksel olarak, şifrelerin ezberlenmesi beklenir.

"Doğum yeriniz neresidir?" gibi birçok gizli soru bilgi faktörünün zayıf örnekleridir, çünkü birçok kişi tarafından tanınabilirler veya araştırılabilirler.



Şekil 4. Örnek PIN Doğrulaması

1.3.2. Sahiplik Faktörleri

Sahiplik faktörleri ("sadece ve sadece kullanıcının sahip olduğu bir şey"), yüzyıllardır anahtar-kilit formunda kimlik doğrulaması için kullanılmıştır. Temel ilke, anahtarın, anahtar ve kilit arasında paylaşılan bir sırrı somutlaştırmasıdır ve aynı ilke, bilgisayar sistemlerinde sahiplik faktörü kimlik doğrulamasının temelini oluşturur. Bir güvenlik tokeni sahiplik faktörünün bir örneğidir.

1.3.3. Bağlantısız Tokenlar

Bağlantısız tokenların istemci bilgisayar ile bir bağlantısı yoktur. Genellikle, manuel olarak kullanıcı tarafından girilen, üretilmiş kimlik doğrulama verisini görüntülemek için yerleşik ekran kullanırlar.

1.3.4. Bağlı Tokenkar

Bağlı tokenler, kullanılacak bilgisayara *fiziksel olarak* bağlı olan cihazlardır. Bu cihazlar verileri otomatik olarak iletir. Kart okuyucular, kablosuz etiketler ve USB tokenler de dahil olmak üzere birçok farklı türü vardır.

1.3.5.Yazılım Tokenları

Bir yazılım tokenı, bilgisayar hizmetlerinin kullanımına izin vermek için kullanılabilecek iki faktörlü bir kimlik doğrulama güvenlik aracı türüdür. Yazılım tokenları masaüstü bilgisayar, dizüstü bilgisayar, PDA veya cep telefonu gibi genel amaçlı bir elektronik cihazda saklanır ve çoğaltılabilir. (Giriş bilgilerinin bu iş için ayrılmış bir donanım cihazında saklandığı ve çoğaltılamayan donanım tokenlarının aksinedir.) Bir soft token kullanıcının etkileşimde bulunduğu bir cihaz olmayabilir. Cihaza yüklenen ve güvenli bir şekilde saklanan bir sertifika da bu amaca hizmet edebilir.

1.3.6. Doğal Faktörler

Bunlar kullanıcı ile ilişkilendirilmiş faktörlerdir ve genellikle parmak izi, yüz, ses ya da iris tanıma gibi biyometrik metotlardır. Tuş dinamiği gibi davranışsal biyometrikler de kullanılabilir.

1.3.7. Lokasyon Bazlı Faktörler

Giderek artan şekilde, kullanıcının fiziksel konumunu içeren dördüncü bir faktör devreye giriyor. Kurumsal ağa kablo bağlantısı zor olsa da, kullanıcının ağ üzerinden kapalı bir yazılım tokeninden kod girerken yalnızca bir pin kodu kullanarak giriş yapmasına izin verilebilir. Bu, ofise erişimin kontrol altında tutulduğu kabul edilebilir bir standart olarak görülebilir.

Ağ giriş kontrolü sistemleri, kablosuz erişim ve kablolu bağlantı gibi, ağa erişim seviyenizin cihazınızın bağlı olduğu belirli bir ağa bağlı olabileceği benzer şekillerde çalışır. Bu aynı zamanda kullanıcının ofisler arasında hareket etmesine ve her birinde aynı düzeyde ağ erişimini dinamik olarak almasına izin verir.

1.3.8. Cep Telefonu Kullanımı

Birçok çok faktörlü kimlik doğrulama sağlayıcısı, cep telefonu tabanlı kimlik doğrulaması sunar. Bazı yöntemler, push tabanlı kimlik doğrulama, QR kod tabanlı kimlik doğrulama, tek kullanımlık şifre ile kimlik doğrulaması (olay ve zaman tabanlı) ve SMS tabanlı doğrulama içerir. SMS tabanlı doğrulama, bazı güvenlik endişelerinden muzdariptir. Telefonlar klonlanabilir, uygulamalar birkaç telefonda çalışabilir ve cep telefonu bakım çalışanı SMS metinlerini okuyabilir. En azından, cep telefonları genel olarak tehlikeye girebilir, yani telefon artık sadece kullanıcının sahip olduğu bir şey değildir.

Kullanıcının sahip olduğu bir şeyi içeren kimlik doğrulamasının en büyük sakıncası, kullanıcının hemen hemen her zaman fiziksel tokenı (USB bellek, banka kartı, anahtar veya benzeri) yanında taşımak zorunda olmasıdır. Kayıp ve hırsızlık birer risktir. Birçok

kuruluş kötü amaçlı yazılım ve veri hırsızlığı riskleri nedeniyle tesis içinde veya dışında USB ve elektronik cihazların taşınmasını yasaklar ve çoğu önemli makinede aynı sebepten dolayı USB portları yoktur. Fiziksel tokenlar genellikle ölçeklenmez, tipik olarak her yeni hesap ve sistem için yeni bir token gerektirir. Bu tür belirteçlerin tedarik edilmesi ve sonradan değiştirilmesinin bir maliyeti vardır. Ek olarak, kullanılabilirlik ve güvenlik arasında doğal çatışmalar ve kaçınılmaz değişimler vardır.

Cep telefonlarını ve akıllı telefonları içeren iki adımlı kimlik doğrulaması özel fiziksel cihazlara bir alternatif sağlar. Kimlik doğrulamasını gerçekleştirmek için, insanlar cihaza kişisel erişim kodlarını (yani, yalnızca bireysel kullanıcının bildiği bir şey) ve genellikle 4 ila 6 basamaktan oluşan tek kullanım için geçerli, dinamik şifresini, kullanabilir. Şifre, mobil cihazlarına SMS aracılığı ile gönderilebilir veya tek kullanımlık şifre oluşturma uygulaması tarafından oluşturulabilir. Her iki durumda da, bir cep telefonu kullanmanın avantajı, kullanıcılar mobil cihazlarını her zaman yanlarında taşıma eğiliminde olduklarından, özel bir tokena gerek kalmamasıdır.

2018 itibarıyla, SMS, tüketiciye yönelik hesaplar için en yaygın olarak kabul edilen çok faktörlü kimlik doğrulama yöntemidir. SMS doğrulamasının popülaritesine rağmen, ABD NIST bunu bir kimlik doğrulama biçimi olarak reddetti ve güvenlik savunucuları bunu alenen eleştirdi.

Sırasıyla 2016 ve 2017 yıllarında, hem Google hem de Apple, alternatif bir yöntem olarak push bildirimi ile kullanıcıya iki adımlı kimlik doğrulaması uygulamaya başladı.

Mobil olarak sunulan güvenlik tokenlerının güvenliği tamamen mobil operatörün operasyonel güvenliğine bağlıdır ve ulusal güvenlik kurumları tarafından telefon dinleme veya SIM klonlama yoluyla kolayca ihlal edilebilir.

1.4. BAZI KİMLİK DOĞRULAMA YÖNTEMLERİ

1.4.1. Şifre ile Kimlik Doğrulama

En yaygın olarak kullanılan doğrulama yöntemi sadece kullanıcı tarafından bilinen, bir paroladır. Bu parolalar erişilecek sisteme göre değişiklik göstermekle beraber numerik karakterler veya hibrit olarak alfanumerik karakterler, özel semboller ve numerik karakterlerin birleşimi şeklinde farklı şekillerde kullanıcılardan talep edilebilmektedir. Bu şifreleme yöntemi ile ne kadar hibrit ve uzunluğu fazla şifreler tercih edilirse güvenlik o düzeyde artırılmış olacaktır. Şifrelemenin karmaşıklığı ile tahmin aralığını belirtmek gerekirse şu şekilde gösterebiliriz:

Numerik 8 karakter uzunluğunda bir şifre: $10.10.10.10.10.10.10.10 = 10^8$ farklı şifre.

Alfanumerik 8 karakter bir şifre yaklaşık olarak: $32.32.32.32.32.32.32.32 = 32^8$ farklı şifre.

Numerik ve alfanumerik 8 karakter şifre: $42.42.42.42.42.42.42.42 = 42^8$ farklı şifre.

Yukarıda da görüldüğü üzere karakter çeşitliliği arttıkça olası şifre çeşidi de gözle görülür oranda artmaktadır. Bu sebepten ötürü şifre ile doğrulama yöntemi neredeyse tüm sistemlerde birincil doğrulama yöntemi olarak tercih edilmektedir.

1.4.2. Pin İle Kimlik Doğrulama

Pin ile doğrulama yöntemi de şifre ile doğrulama yöntemi ile benzerlik göstermekle 0000-9999 dahil toplamda 10000 faklı pin oluşmaktadır. Genellikle ikincil doğrulama yöntemi olarak tercih edilen pin kelimesini açtığımız zaman "Personel Identity Number" yani "Kişisel Kimlik Numarası" açılabilmektedir. Bu doğrulama yönteminin kullanıldığı en yaygın alan ATM cihazlarıdır. ATM cihazları için birincil doğrulama yöntemi banka kartıdır. Eğer banka kartına sahipseniz ikincil doğrulama olan pin kodunu doğru bir şekilde girerek sisteme erişim hakkı kazanılmış olmaktadır.

1.4.3. Parmak İzi İle Kimlik Doğrulama

Vücudumuzda bulunan biyolojik ve benzeri olmayan doğrulama yöntemimiz parmak izleri yaradılıştan gelen bir biyolojik doğrulama yöntemi olarak bizlere verilmiş durumda. Parmak izi ile doğrulama yöntemi ilk defa 1880 yılında kanlı bir parmak izi veya kil üzerinde kalmış olan parmak izleri ile suçluların kimlik teşhisinin yapılabileceği iddiası ile bir rapor hazırlanarak ilk defa kabul edilmiş olundu. Günümüzde ise adli olaylarda kullanılmasından ziyade kişisel olarak genellikle mobil cihazlar üzerinde kimlik doğrulama yöntemi olarak tercih edilmektedir. Mobil cihazlarda ikincil doğrulama yöntemi olarak tercih edilen parmak izi ile kimlik doğrulaması, birincil olarak belirlenmiş olan bir şifreden sonra tercih edilmektedir. Mobil cihazların yanı sıra günümüzde birçok yerde kullanılmaktadır. Bunlara örnek olarak üniversitelerde bulunan giriş çıkış sistemlerinde, yeni nesil akıllı araçlarda, Ar-Ge olarak test aşamasında olan parmak izi ile doğrulama işleminden sonra aktif hale gelen kilitler ve USB bellekler bunlara örnek olarak verilebilir.

1.4.4. Yüz Tanıma İle Kimlik Doğrulama

Bir diğer biyolojik doğrulama yöntemi olan yüz tanıma ile kimlik doğrulama günümüzdeki mobil cihazların birçoğunda aktif olarak kullanılmaktadır. Birçok farklı algoritma ile yüzün tanınması ile sisteme erişime izin veren bu yöntem genel olarak gözler arasındaki mesafe, burun genişliği, göz çukurlarının derinliği, elmacık kemiklerinin şekli, çene hattının uzunlukları vs. ölçülerek kayıtlarla eşleştirerek sisteme erişime izin vermektedir. Genel manada güvenlikli bir sistem olmasına karşın tek yumurta ikizi olan iki kardeş, tam anlamıyla kontrolü sağlanmamış algoritmalar üzerinde yüz tanıma ile kimlik doğrulama sistemini aldatabilir.

1.4.5. İris Tanıma İle Kimlik Doğrulama

Yüz tanıma ile kimlik doğrulama yöntemine göre daha güvenilir olan iris tanıma ile kimlik doğrulaması kullanıcının gözünün dijital görüntüsünün alınıp işlenerek, sisteme kayıtlı diğer verilerle kıyaslanır. Daha sonra eşleşen kayıt olduğu takdirde sisteme erişime izin verilir. İris tanıma ile kimlik doğrulama yöntemi yüz tanıma ile kimlik doğrulama yöntemine kıyasla çok daha iyi sonuç vermektedir. Bunun sebebi olarak her insanın farklı bir iris yapısına sahip olması gösterilebilir. Tek yumurta ikizlerinde ise DNA yapısına sahip olmalarına rağmen iris yapıları farklıdır. Dünya üzerindeki insanlarda aynı iris yapısına sahip olma oranı $1/10^{78}$ olarak belirtilmiştir. Bu sebepten ötürü güvenilir bir kimlik doğrulama yöntemidir.

1.4.6. SMS İle Kimlik Doğrulama

2FA kullanan neredeyse tüm sistemlerde ikincil doğrulama yöntemi olarak kullanılan sms ile kimlik doğrulama yöntemi kullanıcının yanında bulunan bir cihaza gelen kod ile doğrulama yapmasını sağlıyor. Buradaki maksat kullanıcının gerçekten sisteme erişmeye çalışan kişi olup olmadığını doğrulamak. Doğrulama smsinin gittiği cihaz kullanıcının yanında bulunan bir cihaz olduğu için belirli bir süre içerisinde doğrulanması gereken kodu sisteme girerek erişim kazanacaktır.

1.4.7. E-Mail İle Kimlik Doğrulama

E-Mail ile kimlik doğrulama yönteminde amaç, kullanıcının bildiği bir e-mail adresine sistem tarafından gönderilecek tek kullanımlık, genelde 6 numerik karakterden oluşan bir şifre ile kullanıcının kimliğini belirlemesini sağlamaktır. Genellikle ikincil doğrulama yöntemi olarak tercih edilen e-mail ile kimlik doğrulama yöntemi günümüz şartlarında online sistemlere erişimi ulan tüm kullanıcıların bir e-mail adresi olması göz önünde bulundurulduğu zaman mevcut sistemlerde en yaygın kullanılan ikincil doğrulama yöntemlerinden biridir.

1.4.8. Kart İle Kimlik Doğrulama

Kart ile kimlik doğrulama yöntemi genellikle bankacılık işlemleri için ATM'lerde tercih edilen birincil doğrulama yöntemidir. Bunun haricinde kullanılan kart çeşitlerine göre değişiklik göstermekle beraber banka kartları haricinde RFID kartlar ile kişiye özel ulaşım kartları ile turnike geçiş işlemleri, şehir içi otobüs, feribot, banliyö seferleri gibi birçok alanda bu ulaşım kartları kullanılmaktadır. RFID teknolojisi ile kartların içerisinde bulunan kimlik numarası ile benzersiz kartlar oluşturulmaktadır.

1.5. AVANTAJLARI

- İlave tokenler gerekli değildir, çünkü neredeyse her zaman taşınan mobil cihazları kullanır.
- Sürekli değiştikleri için, dinamik olarak oluşturulan parolaların kullanımı, sabit (statik) oturum açma bilgilerini kullanmaktan daha güvenlidir.
- Çözüme bağlı olarak, geçerli bir kodun her zaman kullanılabilir olmasını sağlamak için kullanılan şifreler otomatik olarak değiştirilir, bu yüzden iletim / alım sorunları girişleri engellemez.

1.6. DEZAVANTAJLARI

- Kullanıcılar, kimlik doğrulaması gerekli olduğunda, bir cep telefonu taşımalı ve cep telefonunu hücresel ağın kapsama alanında tutmalıdır. Cihaz, hasar görme, bir güncelleme için kapanma ya da aşırı sıcaklık maruziyetinden dolayı mesajları gösteremez durumdaysa, erişim genellikle imkansızdır.
- Mobil operatörler, kullanıcıya mesajlaşma ücreti yansıtabilirler.
- SMS kullanan cep telefonlarına yapılan metin mesajları güvensizdir ve ele geçirilebilir. Böylece üçüncü şahıslar tokenı çalabilir ve kullanabilir.
- Kısa mesajlar anında gönderilemeyebilir ve kimlik doğrulama işlemine ek gecikmeler eklenir.
- Hesap kurtarma tipik olarak cep telefonunun iki faktörlü kimlik doğrulamasını atlar.
- Modern akıllı telefonlar hem e-postaya görüntülemek hem de SMS almak için kullanılır. E-posta genellikle her zaman giriş yapılmış haldedir. Böylece telefon kaybolur veya çalınırsa, telefon ikinci faktörü alabildiği için e-postanın anahtar olduğu tüm hesaplar saldırıya uğrayabilir. Yani, akıllı telefonlar iki faktörü bir faktörde birleştiriyor.
- SIM klonlama , bilgisayar korsanlarının cep telefonu bağlantılarına erişmesini sağlar. Mobil operatör şirketlerine yapılan sosyal mühendislik saldırıları, çift SIM kartların suçlulara iadesi ile sonuçlandı.

1.7. MOBİL İKİ FAKTÖRLÜ KİMLİK DOĞRULAMASINDA GELİŞMELER

Mobil cihazlar için iki faktörlü kimlik doğrulama araştırmasındaki ilerlemeler, kullanıcıya bir engel oluşturmazken, ikinci bir faktörün uygulanabileceği farklı yöntemleri göz önünde bulundurmaktadır. GPS, mikrofon, ve jiroskop / hızlandırıcı gibi mobil donanımların doğruluğundaki sürekli kullanım ve iyileştirmelerle, ikinci bir kimlik doğrulama faktörü olarak kullanma kabiliyeti daha güvenilir hale geliyor. Örneğin, kullanıcının bulunduğu yerin ortam gürültüsünü bir mobil cihazdan kaydederek ve kullanıcının kimliğini doğrulamaya çalıştığı odadaki bilgisayardan elde edilen ortam gürültüsünün kaydıyla karşılaştırarak kimlik doğrulama faktörü. Bu aynı zamanda süreci tamamlamak için gereken zaman ve çabayı azaltır.

1.8. ÖRNEKLER

Birçok popüler web servisi, genellikle varsayılan olarak devre dışı bırakılmış opsiyonel bir özellik olarak çok faktörlü kimlik doğrulaması kullanır.[8] Pek çok İnternet servisi (aralarında Google ve Amazon AWS'ninde bulunduğu), iki aşamalı kimlik doğrulamasını desteklemek için açık kaynaklı Zaman Tabanlı Tek Kullanımlık Şifre Algoritmasını (TOTP) kullanır.

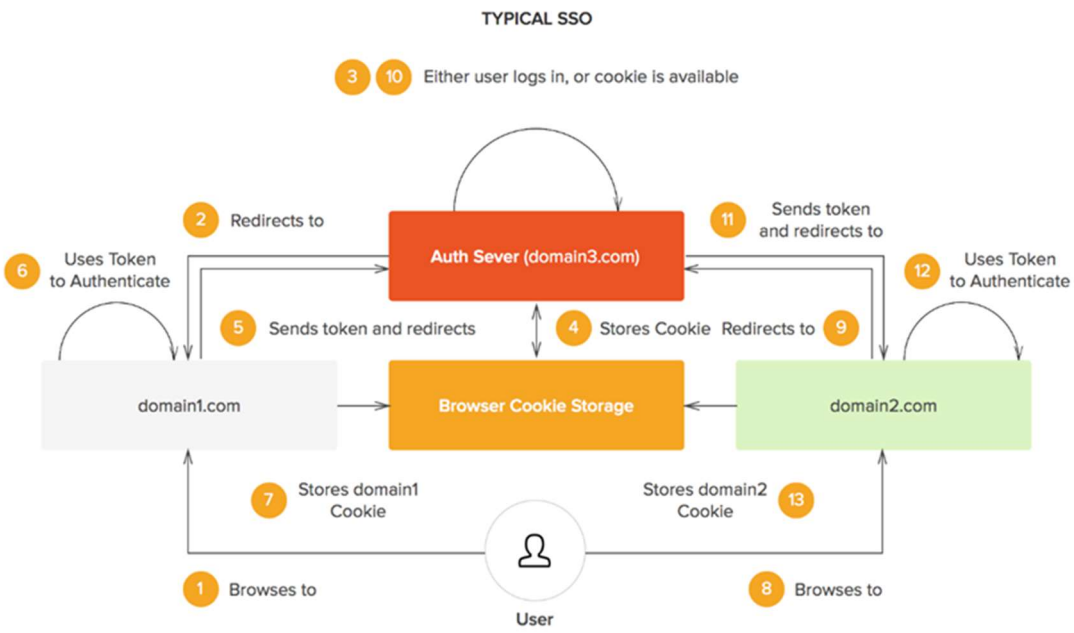
2. CENTRALIZED IDENTITY MANAGEMENT (SINGLE SIGN-ON)

2.1. Single-Sign-On

Single-Sign-On, kullanıcıların bir kurumun web sitesinde bulunan her bir uygulama için ayrı ayrı kullanıcı adı/parola ikilisi tanımlama zorunluluğunu ortadan kaldırır; bunun yerine birçok uygulamaya sadece bir kullanıcı adı/parola ikilisi ile erişebilmeyi sağlar.

Şekil1. SSO Genel Gösterimi

Single-Sign-On, hem lokal hem de bulut bilişim tabanlı servislerde uygulanabilmektedir; aynı zamanda kullanıcının statüsü göz önünde bulundurularak erişim hakkına sahip olduğu kaynak ve uygulamaların dışında diğer bilgilere ulaşamayacağı şekilde bir erişim kontrolü sağlanmaktadır. Bu sistemde güvenlik ve kullanışlılık gibi ikisinin aynı anda işletilmesi zor olan servisler bir arada uygulanabilmektedir. Hem kullanıcının birden fazla kimlik bilgisi tutmasına gerek kalmamakta hem de sistemin güvenliği arttırılmış olmaktadır. Bu süreç işletilirken kullanıcı hangi uygulamadan giriş yapmak isterse istesin sistem kimlik doğrulama için kullanıcıyı merkezi kimlik doğrulama sunucusuna yönlendirmektedir. Böylelikle kullanıcının kimliği tanımlanmakta ve eğer doğrulandığı takdirde bu veriye ihtiyaç duyan diğer tüm alt sistemlerle paylaşılmaktadır.



Şekil2. SSO çalışma mekanizması

2.2. Web Tabanlı SSO

Web tabanlı SSO sistemi, bir domaine ait birçok uygulamaya kullanıcıların sadece bir kimlik bilgisi ile bir oturumda yanlızca bir login işlemi yaparak erişmelerini sağlar. Kullanıcının yanlızca bir uygulama için doğrulama işlemi yaptırması yeterli olmaktadır. İlk doğrulamayı gerçekleştiren web tabanlı SSO, oturum bilgisini kullanıcıyı tanıması gereken diğer uygulamalara dağıtmaktadır.

Tarayıcılar güvenlik hizmetlerinin bir gereği olarak cookie veya lokalde saklanması gereken diğer verilere sadece bu veriyi üreten domainin ulaşmasını şart koşan Same Origin Policy servisini uygulamaktadır. Bu da domainler arası oturum bilgisini paylaşmayı zorlaştırmaktadır. Bunun çözümü için de farklı domainlere oturum bilgisi tokenlarını paylaşmayı sağlayan web tabanlı SSO kullanılmaktadır. Bu sistemde oturum bilgisini içeren token imzalanarak paylaşılmaktadır, bu da oturum verilerinin kullanıcı tarafından değiştirilmesini zorlaştırmaktadır.

SAML(Security Assertion Markup Language) protokolü web tabanlı SSO için kullanılan OneLogin tarafından geliştirilmiş açık kaynak kodlu önemli protokollerden biridir. Bu protokol kullanıcı bilgilerini dijital imza ile imzalanmış XML dosyaları halinde göndermektedir.

2.3. SAML'in Çalışma Mekanizması

- Kullanıcı login olmak istediği sitenin linkine tıkladığında, uygulama IP adresi gibi bilgileri kullanarak istemcinin kaynak bilgisini tespit eder ve kullanıcıyı kimlik doğrulamasının yapılabilmesi kimlik sağlayıcıya(identitiy provider) yönlendirir.
- Kullanıcının zaten kimlik sağlayıcısı ile aktif olan bir oturumu mevcut olabilir, yada eğer mevcut oturumu yoksa kimlik sağlayıcıya giriş yaparak yeni oturum alır.
- Kimlik sağlayıcı, XML formatında düzenlenmiş olan ve kullanıcının isim ve email adresini barındıran kimlik doğrulama bilgisini X.509 sertifikası ile imzalayarak servis sağlayıcıya gönderir.
- Kimlik sağlayıcısını zaten tanıyan ve sertifika özetini(certificate fingerprint) tutan servis sağlayıcı sertifika parmak izini kullanarak kimlik doğrulama bilgisinin geçerliliğini denetler.
- Kimlik doğrulamadan sonra kullanıcı kimliği tanımlanmış olur ve kullanıcının uygulamaya erişimine izin verilir.

2.4. Aktif Dizinin SSO İle Entegrasyonu

Aktif dizinin(Active Directory) SSO ile entegrasyonu iki-faktörlü ve çok faktörlü kimlik doğrulama yöntemlerinin uygulanarak kullanıcıların güvenli bir şekilde kimlik doğrulamasından geçirilmesini sağlamaktadır. Aktif dizin entegrasyonu aynı zamanda BT yöneticisinin uygulamalara ve veritabanlarına kimlerin, ne zaman ve nerden hangi bilgilere ulaştığı gibi erişim denetlemelerini gerçekleştirmesine imkân vermektedir.

Sanal makineler, yazıcılar, BYOD, personel giriş çıkış kartı, biyometrik kimlik doğrulama veya personel bilgisayar başından ayrıldığında iş istasyonunun otomatik olarak kilitlenip personel döndüğünde ise tekrar kimlik bilgilerini istemesi gibi servisler SSO ile entegrasyonu faydalı olacak sistemler arasında sayılmaktadır.

2.5. LDAP'ın SSO İle Entegrasyonu

LDAP'ın SSO'yla entegrasyonu; kullanıcılar oluşturulduğunda, güncellendiğinde veya engellendiğinde değişikliklerin otomatik olarak SSO'ya bildirilmesini sağlar. Bu yöntemin avantajları:

- Kullanıcıların sisteme giriş ve kimlik doğrulama işlemlerinin hızlı ve güvenli bir şekilde yapılabilmesi
- Çalışan işten çıktığında yetkisiz erişimlerin ve veri kayıplarının önlenmesi için kullanıcının sistemden ve aktif dizin servislerinden engellenmesi
- Mail adreslerinin, kullanıcı ismi ve grup üyeliklerinin güncellenmesi.

2.6. CAS(Central Authentication Service) Çalışma Mekanizması

Kullanıcı kimlik doğrulaması isteyen bir uygulamayı ziyaret ettiğinde uygulama kullanıcıyı Merkezi kimlik doğrulama servisine yani CAS'e yönlendirir. Genellikle CAS kullanıcı adı ve parolasını Kerberos, LDAP veya Active Directory gibi bir veri tabanında kontrol edip eşleştirme yoluyla kullanıcıyı doğrulamaya çalışır. Kimlik doğrulaması başarıyla gerçekleştirilirse CAS bir servis token(service ticket) oluşturarak kullanıcıyı uygulamaya geri döndürür. Tokenın geçerliliğini kontrol etmek için uygulama CAS'e güvenli bir bağlantı üzerinden kendi servis tanımlayıcı(service identifier) ve bilet(ticket) bilgilerini gönderir. Bunun üzerine CAS kullanıcının başarılı bir şekilde doğrulandığına dair veriyi uygulamaya gönderir.

2.7. OAuth Çalışma Mekanizması

Kimlik doğrulamadan(Authentication) farklı olarak yetkilendirme(Authorization) işlemi istemcinin hangi kaynaklara erişim hakkı olduğunu denetleyen ve belirlenen kısıtlamalara göre erişim kontrolü sağlayan bir yetkilendirme sistemidir. Erişim kontrolü ve yetkilendirme işlemi yapan OAuth sistemi ile kimlik doğrulama işlemi yapan CAS Authentication sistemi birbirinden farklı işlevleri yerine getirir, ancak yetkilendirme süreci kendi içinde ayrı bir kimlik doğrulama mekanizması barındırmaktadır. OAuth sisteminde yetkilendirme sürecinden önce veri kaynaklarının sahibi yetkilendirme(authorization) sunucusu tarafından kimlik doğrulama işlemine tabi tutulmaktadır, aynı şekilde istemci de kimlik doğrulama işleminden geçirilmektedir. Kimlik doğrulamayı yetkilendirme üzerine uygulamanın yararı domainler arası kimlik bağımsızlığını koruması ve son kullanıcı izninin alınmasını kolaylaştırmasıdır. Bir diğer kolaylık ise kullanıcının doğrulanmış kimlik bilgileri ile başka diğer korunmuş API'lere erişim izni de isteyebilmesidir. Bu hem geliştiricilerin hem de kullanıcıların süreci yönetmesini kolaylaştırmaktadır.

3. MFA VE SSO YÖNTEMLERİYLE HAZIRLANAN PROJE

3.1 PROJE HAKKINDA GENEL BİLGİLENDİRME

Proje üç ana bölümden oluşmaktadır. Öncelikle bu üç bölüm şu şekilde tanımlanabilir.

1- **Görev Yönetim Sistemi:** Görev yönetim sistemi bir işletme için personel görevlendirmesi, iş takibi ve proje yönetimi gibi işlemlerin gerçekleştirildiği hayal edilerek tercih edilmiş olan, personellerin sıklıkla kullandığı bir sistemdir.
   Proje Linki: https://gorev.yavuzceliker.com.tr

2- **Muhasebe Yönetim Sistemi:** Muhasebe yönetim sistemi de görev yönetim sisteminde olduğu gibi bir işletmenin olmazsa olmazı olan bir sistemdir. Bu sebeple ikinci hayali sistem olarak tercih edilmiştir. Muhasebe yönetim sistemi muhasebe personellerinden ziyade diğer personeller de avans talepleri, harcırah bilgileri, maaş ve diğer maddi işlemler için kullanılmaktadır.
   Proje Linki: https://muhasebe.yavuzceliker.com.tr

3- **Kullanıcı Yönetim Sistemi:** Kullanıcı yönetim sistemi hazırlanan projenin konu ile alakalı kısmını oluşturmaktadır. Bu sistem üzerinde çok faktörlü doğrulama yöntemi kullanılarak ek güvenlik yöntemleri ile daha güvenli bir ortamda sisteme kayıt işlemleri, oturum kontrol işlemleri, şifre yenileme işlemleri ve hesap doğrulama işlemleri yapılmaktadır.
   Proje Linki: https://odev.yavuzceliker.com.tr

Muhasebe ve görev yönetim sistemlerini tam anlamıyla çalışıp görevlendirme işlemleri, cari ve muhasebe işlemleri yapmamaktadır. Konu ile alakası olmadığı için çalışır hale getirilmemiştir. Sadece ana sayfa kısmı ve oturum kapatma kısmı aktif hale getirilerek kullanıcının sistemlere giriş yaptığının veya yapmadığının kontrol edilmesi hedeflenmiştir.

3.2. PROJENİN HAZIRLANDIĞI ORTAM, DİL VE VERİ TABANI

- Proje Visual Studio 2019 üzerinde hazırlanmıştır.
- Proje ASP.NET – MVC ile EntityFramework kullanılarak hazırlanmıştır.
- Proje için MSSQL veri tabanı tercih edilmiştir.

3.3 PROJENİN HAZIRLANMA AŞAMALARI

3.3.1 Planlama Aşaması

Proje hazırlanmaya başlanmadan önce, öncelikle neler yapılacağına karar verildi. Nasıl bi sistem olması gerektiği, konuya uygun ne gibi bir sistem olması gerektiği düşünüldü. İş akışı şu şekilde gerçekleşti.

1- Konu çok faktörlü kimlik doğrulama ve merkezi kimlik yönetimi olduğu için öncelikle birden çok bağımsız fakat ilişkili sistem olması gerektiği düşünüldü.

2- Bu bağımsız fakat ilişkili sistemler ayrı ayrı oturum bilgisi tutmayacağı, tek bir merkez üzerinden kullanıcı doğrulaması ve oturum kontrolü yapılması gerektiği düşünüldü.
3- Düşünülen sistem için minimum iki adet kullanıcıların aktif olarak kullanacağı sistem, bir tane de bu sistemlerin kullanıcı işlemlerini ve oturum kontrol işlemlerini sağlayacak kullanıcı yönetim sistemi yapılması gerektiği düşünüldü.
4- Projenin tasarlanması için hangi ortamda yapılacağı, hangi dil ve veri tabanı tercih edileceğine karar verilmesi gerektiği için ilgili konular belirlenmeye başlandı.
5- Hazırlanacak proje için günümüz şartlarında bir çözüm sunması gerektiği düşünüldü. Masaüstü sistemler günümüzde değerini kaybetmiş durumda ve her platformdan erişilebilir değil. Mobil uygulamalar ise günümüz şartlarına uygun sistemler olmasına rağmen, web tabanlı sistemler kadar aktif olarak tercih edilmemektedir. Bu sebeple web tabanlı sistemler yapılması gerektiği düşünüldü.
6- Web tabanlı yapılacak olan bu sistemler, tercihen ASP.NET üzerinde MVC mimarisi kullanılarak yapılmasına karar verildi.
7- Hazırlanacak sistemler için veri tabanı olarak MSSQL kullanılmasına karar verildi.
8- Projenin tasarlanması için gereken bilgilere karar verildi ve sonraki aşama olarak projenin tasarlanmasına başlanıldı.

3.3.2. Tasarlama Aşaması

Projenin tasarlanma aşaması için, öncelikle projenin kağıt üzerinde planlaması yapılmalıdır. Projenin tasarlanmasında sırayla yapılacak olanlar şu şekilde belirlenmiştir.

1- Kullanılacak kimlik doğrulama yöntemlerinin belirlenmesi.
2- Kullanılacak modellerin tasarlanması.
3- Tasarlanan modellere göre sistemin yapması gereken işlevlerin tasarlanması.
4- Yapması gereken işlevler için gerekli olan sayfaların tasarlanması.
5- Tasarlanan işlevler ve sayfalar için uygun sınıf ve fonksiyonların belirlenmesi.
6- Son olarak ise kağıt üzerinde hazırlanan sistemin gerçekleştirilmesi.

Tasarlama aşamaları, ihtiyaçlar ve gereksinimler belirlendi ve projenin tasarlanmasına başlanıldı.

3.2.2.1. Kullanılacak kimlik doğrulama yöntemlerinin belirlenmesi.

Hazırlanacak sistemler için kullanılacak kimlik doğrulama yöntemleri projenin şekil almasında önemli bir rol oynamaktadır. Oturum kontrolünün sağlanacağı yöntem, oturum açma ve şifre değiştirme sırasında kullanılacak güvenlik yöntemleri proje üzerinde kritik ve önemli bir rol oynamaktadır. Bu denli önemli olan bir sistem için yapılan bir araştırma sonrasında tercih edilecek yöntemler şu şekildedir.

1- Oturum verilerinin kontrolü ve saklanması için kullanılacak yöntem

   System.Web.Security altında bulunan FormsAuthentication sınıfıdır. Bu yöntem oturum verilerini istemci üzerinde çerezler olarak saklayarak sadece ilgili cihaz üzerinden erişime izin vermektedir. Bir oturum başlatmak için GetAuthCookie fonksiyonu ile yeni bir çerez oluşturuluyor. Daha sonra bir adet FormsAuthenticationTicket oluşturarak çerezin geçerlilik süresi ve taşınacak veri ekleniyor. Oluşturulan bu bilet Encrypt fonksiyonu aracılığı ile şifrelenerek bir string haline getiriliyor. Bu string hale gelen bilet oluşturulan çereze eklenerek ilgili http response'a iliştirilerek gitmesi gereken alt sisteme yönlendirilecektir.

2- Sisteme giriş yapmak için kullanılacak doğrulama yöntemleri

   Kullanıcının sisteme giriş yaparken kullanacağı iki adet kimlik belirleme yöntemi kullanılacaktır. Bu yöntemlerden birincisi kullanıcı şifresi olacaktır. Kullanıcı sisteme giriş yapmak istediği takdirde kullanıcı adı ve şifresini girecektir. Eğer ki doğru verileri girmiş ise, o zaman sisteme kayıtlı e-mail adresine bir doğrulama kodu gönderilecek ve gelen kodu girmesi istenecektir. Bu sayede 2FA(çift faktörlü kimlik doğrulama) kimlik doğrulama işlemi gerçekleştirilmiş olacaktır.

3- Şifre yenileme işlemi için kullanılacak doğrulama yöntemleri

   Kullanıcının sisteme erişimi kaybettiği zaman mevcut şifresini değiştirmek istemesi durumunda şifre yenileme talebinde bulunması gerekmektedir. Bu durumda öncelikle kayıtlı kullanıcı adı veya e-mail adresini girerek doğrulama amacıyla kayıtlı e-mail adresine gönderilen şifre yenileme bağlantısını açması gerekmektedir. Daha sonra ikinci aşama olarak eğer ki geçerli bir link ile gelmiş ise, sisteme kaydolurken oluşturmuş olduğu güvenlik sorusunun cevabını doğru olarak vermesi gerekecektir. Doğru cevap vermesi halinde yeni bir şifre oluşturabilecektir.

4- Sisteme kayıt olurken kullanılacak doğrulama yöntemleri

   Sisteme kayıt aşamasında kullanılacak bir adet doğrulama yöntemi bulunmaktadır. Bu doğrulama yöntemi kullanıcı gerekli tüm verilerini girip onaylandıktan sonra e-mail adresine gönderilecek olan bir hesap onaylama linki olacaktır. Bu link aracılığı ile kullanıcı hesabını doğrulayabilecektir. Bu şekilde rastgele e-mail adresi ile sisteme kayıt yaptırmanın önüne geçilmiş olunacaktır.

3.3.2.2. Kullanılacak Modellerin Tasarlanması

Proje üzerinde kullanılacak model projenin en önemli kısmını oluşturmaktadır. Çünkü sistemler bu model üzerinde dönecektir. Bu sebeple hazırlanacak model bir hayli önem arz etmektedir.

Hazırlanacak model için sorulacak sorular ve gereksinimler şu şekilde oluşturulacaktır.

1- Sistemler üzerinde bir kayıt işlemi gerçekleşecek mi?
   Bu soru üzerinden yola çıkarak sistem üzerinde gerçekleşecek kayıt işlemleri göz önüne getirildiğinde bariz olarak oturum açan kullanıcıların kaydının tutulması gerektiği görülmektedir. Bunun haricinde bir log kaydı tutularak hangi kullanıcıların işlem yaptığı kayıt altına alınabilir.
2- Herhangi bir yetkilendirme işlemi gerçekleştirilecek mi?
   Şu an üzerinde çalışılan konuya bakıldığı zaman görülebiliyor ki kullanıcı yönetim sistemi haricindeki sistemler faal olarak hizmet vermeyeceğinden ve sadece oturum kontrolü sağlanacağından ötürü herhangi bir yetkilendirme işlemine gerek duyulmayacaktır.
3- Hazırlanan modeller üzerinde herhangi bir ilişkilendirme yapılacak mı?
   Hazırlanacak olan log kaydı tutacak model ile kullanıcı bilgilerinin tutulduğu model arasında bir ilişkilendirme olacak. Bu ilişkilendirme ile log kaydına oturum açan kullanıcının kaydı iliştirilecek.
4- Hazırlanacak üç ayrı sistem için birden çok veri tabanı mı olacak, yoksa tek bir veri tabanı üzerinde mi çalışacak?
   Hazırlanacak sistemler şu an büyük bir proje olmadığından ötürü tek bir veri tabanı üzerinde çalışacak. Eğer daha büyük bir sistem yazılıyor olsa idi bir web servis aracılığı ile sadece gerekli olan verilerin talep edileceği, daha genişletilmiş bir sistem kullanılabilirdi.

Sorulacak ve cevaplanacak temel konular düşünülüp cevaplar verildikten sonra modeller şu ana kadar planlanan ve düşünülen akışa göre oluşturulmaya başlanabilir.

İlk olarak sistemlerin bel kemiği olacak olan kullanıcı modelini oluşturmamız gerekmektedir. Bu model için kullanılacak değişkenler şu şekilde olacaktır.

1- kullaniciId (PK,AI,int) : Her kullanıcı için otomatik artan sayı olarak oluşturulacak olan benzersiz kullanıcı kimlik numarası.
2- adSoyad (string) : Kullanıcının ad soyad bilgilerini tutacak olan değişken.
3- sifre (string) : Kullanıcının şifre bilgilerini tutacak olan değişken.
4- kullaniciAdi (string) : Kullanıcının sisteme giriş yaparken kullanabileceği kullanıcı adını tutacak olan değişken.

5- email (string) : Kullanıcının oturum açarken kullanabileceği, şifre yenileme işlemi ve doğrulama kodlarının gönderileceği e-mail adresini tutacak olan değişken.
6- soru (string) : Kullanıcının şifresini unuttuğu takdirde yeni bir şifre oluşturması için kullanılacak olan güvenlik sorusunu tutacak olan değişken.
7- cevap (string) : Oluşturulacak olan güvenlik sorusunun cevabını tutacak olan değişken. Kullanıcı eğer bu değişkende yazılı olan doğru cevabı girerse, şifre doğrulama işlemi sonraki adıma ilerleyecektir.
8- dogrulamaKodu (string) : MFA için gönderilecek doğrulama kodlarının kaydını tutacak olan değişken.
9- hesapDurumu (bool) : Sisteme kaydolan kullanıcının e-mail hesabını doğrulamadan önce pasif olan hesabını aktifleştirip aktifleştirmediğinin kontrolünün yapılacağı değişken.

Kullanıcı modeli tanımlandıktan sonra kullanılacak diğer model olan log modeli şu şekilde tanımlanacak.

1- ipLoginId (PK,AI,int) : Log kayıtlarının her biri için oluşturulacak benzersiz, otomatik artan sayı tipinde numaraları tutacak değişken.
2- zaman (DateTime) : Sisteme giriş zamanının tutulduğu değişken.
3- ipAdresi (string) : Kullanıcının oturum açarken kullandığı cihaza ait ip adresinin kaydının tutulduğu değişken.
4- dogrulama (string) : Kullanıcının oturum kontrolü yapılırken diğer sistemlere gizli olarak gönderilecek oturum kontrol doğrulama kodunu tutacak değişken.
5- kullanici (kullanici) : Kullanıcı modelinden türetilmiş olan kullanici tipinde, oturum açan kullanıcının bilgilerini tutacak olan değişken.

Toplamda iki adet olması planlanan modeller yukarıda tanımlandığı şekilde oluşturulmuştur. Oluşturulan bu modeller ile birlikte sonraki aşama olan sistemin yerine getirmesi gereken işlevlerin belirlenmesine geçilecektir.

3.3.2.3. Tasarlanan Modellere Göre Sistemin Yapması Gereken İşlevlerin Tasarlanması

Sistemler için gerekli olan modeller tanımlandıktan sonra artık çalışacak sistemlerin tasarlanması gerekmektedir. Bu sistemler için öncelikle ne işlevleri yerine getirmesi gerektiğine karar verilmelidir. Sistemlerin yerine getirmesi gereken işlevler aşağıda belirtildiği gibi olacaktır.

1- Kullanıcı yönetim sistemi

   Kullanıcı yönetim sistemi projenin en önemli sistemi olarak çalışacaktır. Bu sebeple en yoğun ve en işlevsel sistem bu olacaktır. Bu sistemin genel olarak yerine getireceği işlevler oturum kontrolüne yönelik işlevler olacaktır. Bunun haricinde şifre yenileme, kayıt ve hesap doğrulama

işlemlerini de yapacaktır. Bu işlemler için gerekli tanımlamalar ve kullanılacak yöntemler aşağıda tanımlanacaktır.

a. Yeni kullanıcı kaydı

Sistemin ilk adımı olarak her sistemde olduğu gibi yeni bir kullanıcı oluşturulması gerekmektedir. Yeni bir kullanıcı oluşturulurken de oluşturulan modele istinaden bir kayıt formu oluşturulmalı. Bu form üzerinde ad soyad, e-mail ve kullanıcı adı ilk adımda alınması gereken bilgiler olacaktır. Çünkü alınan kullanıcı adı ve e-mail adreslerinin sistem üzerinden kontrol edilerek mevcut herhangi bir kayıtla eşleşmediğinin doğrulanması gerekmektedir. Doğrulama işlemi tamamlandıktan sonra ikinci aşamaya geçerek güvenlik sorusu, soru cevabı ve kullanıcı şifresinin talep edilmesiyle beraber form gönderildikten sonra kayıt işleminin tamamlanması için kullanıcının girmiş olduğu e-mail adresine bir doğrulama linki gönderilmesi gerekmektedir. Gönderilen link vasıtası ile kullanıcı hesabını doğrulayarak kayıt işlemini tamamlamış olacaktır.

Bu senaryoya göre oluşturulması gereken fonksiyonlar şu şekilde sıralanabilir.

i. JsonResult girisBilgileriKontrol(string e-mail, string kullaniciAdi, string adSoyad)

Bu fonksiyon ile kayıt formundan ilk adımda girilen bilgilerin sistemde bir kullanıcıya işaret edip etmediğinin, boş olup olmadığının kontrolü yapılacaktır. Doğru olması halinde sonraki aşamaya, hatalı olması durumunda hata durumuna göre json paketi halinde bir hata kodu döndürmesi hedeflenmektedir.

ii. string MailGonder(string email, string konu, string mesaj)

Bu fonksiyon ile kullanıcı ile iletişime geçerek gerekli e-mail gönderme işlemleri gerçekleştirilecektir. Kullanıcı kaydı işlemleri için hesap doğrulama linkinin gönderilmesi işlemini gerçekleştirirken, giriş yapma ve şifre yenileme kısımlarında da kullanılacaktır.

iii. ActionResult dogrula(int kullaniciId, string dogrulamaKodu)

Bu fonksiyon vasıtası ile kayıt olan kullanıcıların hesap doğrulama işlemleri gerçekleştirilecektir. Kayıtlı e-mail adresine gönderilen link ile doğru verilere sahip olduğu takdirde hesabının doğrulama işlemi gerçekleştirilerek giriş sayfasına yönlendirilecektir. Aksi takdirde bir hata mesajı üreterek hatalı veya süresi geçmiş bir linke sahip olduğu belirtilecektir.

b. Sisteme giriş

Doğrulama gerektiren sistemlerde olmazsa olmaz olan sisteme giriş sayfası üzerinden adından da anlaşılacağı üzere hazırlanan sistemlerde oturum açma işlemi gerçekleştirilecektir. Bu işlemin senaryosu şu şekilde belirtilebilir.

Öncelikle sisteme kaydolmuş ve hesap onayını gerçekleştirmiş olan kullanıcı, sistemde oturum açmak için kullanıcı adı veya e-mail adresi ve şifresini form üzerinden girerek giriş

yapmak için doğrulamanın yapılacağı fonksiyona iletiyor. Fonksiyon tarafından okunan kullanıcı adı ve şifre doğru olduğu takdirde kayıtlı e-mail adresine bir doğrulama kodu gönderiliyor. Kullanıcı adı veya şifresi yanlış olduğu takdirde ise bir hata mesajı üretilerek kullanıcıya bilgi veriliyor.

Kullanıcı doğrulandıktan ve kayıtlı e-mail adresine doğrulama kodu gönderildikten sonra sisteme giriş sayfası ikinci aşamaya geçerek e-mail adresine gönderilen doğrulama kodunu isteyecektir. Girilen kod ilgili fonksiyon tarafından kontrol edilerek doğru iste sisteme yönlendirecek, hatalı iste bir hata mesajı üreterek kullanıcıya hata bildirimi yapacaktır.

Bu senaryoya göre oluşturulması gereken fonksiyonlar şu şekilde sıralanabilir.

i. JsonResult girisKontrol(string kullaniciAdi, string sifre, string dogrulamaKodu, string durum)

   Bu fonksiyon üzerinden sisteme giriş yapma ile alakalı tüm işlemler gerçekleştirilecektir. Fonksiyon üzerinde parametre ile alınan değişkenlerden durum değişkeni, "birinci" ve "ikinci" şeklinde iki değer alacaktır. Gelen değer "birinci" olduğu takdirde kullanıcı adı ve şifre kontrolü yapacak, doğru ise kayıtlı e-mail adresine sistem tarafından üretilecek karmaşık bir doğrulama kodu gönderecek ve aynı zamanda bu kodu bir session içerisinde kullanıcıdan alacağı değerle karşılaştırmak için tutacak. Buraya kadar bir hata oluşmamışsa eğer giriş işleminin ikinci aşamasına geçmek için onay, hatalı bir durum oluşmuş ise hata mesajı döndürecek. Eğer ki durum değişkeni "ikinci" değerini almış ise o zaman giriş işleminin ikinci aşaması çalışmış demektir. Bu durumda sistem kullanıcı tarafından girilen doğrulama kodunu session içerisinde tuttuğu doğrulama kodu ile karşılaştırarak doğru olduğu takdirde kullanıcıyı sisteme yönlendirecektir. Eğer ki hatalı ise kullanıcıya bir hata mesajı döndürecektir.

ii. rastgeleKod()

   Bu fonksiyon ile sistem üzerinde tahmin edilmesi güç rastgele kodlar üretilecek. Üretilecek kodlar 6 karakterden oluşacak ve klavyede bulunan 32 harf ve 10 rakamdan rastgele seçerek oluşturulacak. Yani toplamda 74^6 farklı şifre oluşturulmuş olacaktır.

c. Şifre yenileme

Şifre yenileme işlemi, sisteme üye olan kullanıcıların giriş yapmak için kullandıkları doğrulama yöntemlerinden birisi olan şifrelerini sıfırlamak için kullanacağı bir işlemdir. Bu işlemin senaryosu şu şekilde belirtilebilir.

Sisteme üye olmuş ve hesabını onaylatmış bir kullanıcı, eğer ki şifresini unutmuş ise şifre yenileme sayfası üzerinden şifre sıfırlama yapabilir. Şifre sıfırlamak için kullanıcı adını veya e-mail adresini giren kullanıcının bilgileri ilgili fonksiyon tarafından kontrol edilerek, eğer ki öyle bir kullanıcı var ise kullanıcının güvenlik sorusunu ekrana göndererek kullanıcıdan bu güvenlik sorusunun cevabı beklenmektedir. Kullanıcı tarafından gönderilen cevap doğru olduğu takdirde yeni şifre oluşturması talep edilecektir ve şifre sıfırlama işlemi tamamlanmış olacaktır.

2- Görev yönetim sistemi ve muhasebe yönetim sistemi

a- Sistemden çıkış

Sistemden çıkış yapma işlemi, oturum açmış olan personelin oturumunu sonlandırmak için kullanılacak olan işlemdir.

b- Oturum kontrolü

Oturum kontrol işlemi, kullanıcı yönetim sistemi tarafından oturum açmış olan kullanıcıların oturum verilerini okuyarak mevcut sistemde de oturum verilerini sürdürmeyi hedeflemektedir.

3.3.2.4. Yapması gereken işlevler için gerekli olan sayfaların tasarlanması.

Hazırlanacak projede yukarıda tanımlanan işlevlerin bazılarının görsel bir arayüze ihtiyaç duymamasına rağmen, bazıları bir form üzerinden kullanıcı ile iletişime geçmektedir. Bu sebepten ötürü yukarıda tanımlanan işlevlerden gerekli olanları aşağıda tanımlayacağım.

1- Kullanıcı Yönetim Sistemi

a- Login

Bu sayfa üzerinden kullanıcıların sisteme giriş yapması, hedeflenmektedir. Yukarıda belirtilen senaryo üzerinden kullanıcının doğrulanıp sisteme erişiminin sağlanması bu sayfa üzerinden gerçekleştirilecektir.

b- Kaydol

Kaydol sayfası üzerinden sisteme yeni kullanıcılar dahil edilecektir. İki aşamalı olarak çalışacak olan kaydol sayfasında ilk aşamada sadece ad soyad, kullanıcı adı ve e-mail adresi alınarak, sistemde kayıtlı olan farklı bir kullanıcıya işaret edip etmediği kontrol edilecektir. İkinci aşamada ise kayıt için herhangi bir engel teşkil etmeyen kullanıcı bilgilerine ek olarak güvenlik sorusu ile cevabı ve kullanıcı şifresi girilerek kayıt işlemi tamamlanacaktır.

c- Şifre Yenile

Şifre yenileme sayası üzerinden sisteme üye olmuş ve şifresini kaybetmiş kullanıcılar için şifresini değiştirme imkanı sunulmaktadır. İki ayrı sayfa olarak çalışacak olan şifre yenileme işlemi için ilk aşamada sisteme kayıtlı olan kullanıcı adı veya e-mail adresi girilerek mevcut bir kullanıcı olup olmadığı kontrol edilir. Eğer ki uygun bir kullanıcı var ise sisteme kayıtlı e-mail adresine bir şifre yenileme bağlantısı gönderilir.

d- Şifre Değiştir

Şifre değiştirme sayfası kullanıcının e-mail adresine gönderilen şifre yenileme bağlantısının yönlendirileceği sayfadır. Bu sayfa üzerinde kullanıcının yapacağı iki işlem vardır. Öncelikle hesabına daha önce kaydetmiş olduğu güvenlik sorusunun doğru cevabını vermek. Doğru cevabı verdiği takdirde ikinci aşamaya geçerek kullanıcının yeni şifresini girmesi talep edilecektir. Kullanıcı yeni şifresini girdikten sonra işlem tamamlanarak sisteme giriş yapmak üzere giriş yap sayfasına yönlendirilir.

e- Doğrula

Doğrula sayfası görsel bir ara yüze sahip olmamakla birlikte sisteme yeni kaydolmuş kullanıcıların hesaplarının doğrulamasının yapıldığı sayfadır. Kullanıcı bu sayfa üzerinden doğrulama işlemi yapılarak giriş yap sayfasına yönlendirilir.

f- Yönlendir

Yönlendir sayfası da bir görsel ara yüzü bulunmayan bir sayfadır. Bu sayfanın vazifesi, giriş yap sayfası üzerinden oturum açan kullanıcının gitmesi gereken alt sisteme yönlendirmesini gerçekleştirmektir. Giriş yap sayfası üzerinden gelen bilgiler doğrultusunda yönlendirme işlemini gerçekleştirerek doğrudan ilgili alt sistemin ana sayfasına yönlendirme yapmaktadır.

2- Muhasebe ve Görev Yönetim Sistemi

a- Ana sayfa

Ana sayfa adından da anlaşılacağı üzere muhasebe ve görev yönetim sistemlerinin açılış sayfası olacaktır. Kullanıcı oturum açmamış ise kayıt ve oturum açma sayfalarına yönlendirmek için butonlar bulunacak. Eğer oturum açılmış ise, oturum açıldığını belirtmek için ekran üzerinde “Hoş geldin { Kullanıcı ad soyad }.” Şeklinde bir karşılama mesajı verilecektir ve aynı zamanda hemen alt tarafta sistemden çıkış yapmak için kullanılacak olan çıkış yap butonu bulunacaktır.

b- Çıkış Yap

Çıkış yap sayfası üzerinden kullanıcılar mevcut oturumlarını sonlandıracaklardır. Bu sayede sistemdeki diğer alt sistemlerden de çıkış yapmış olacaklardır. Ve daha sonra tekrar giriş yapmak üzere giriş yap sayfasına yönlendirileceklerdir.

3.3.2.5. Tasarlanan işlevler ve sayfalar için uygun sınıf ve fonksiyonların belirlenmesi.

Hazırlanacak sistemlerde kullanılacak ve tekrar eden birçok işlem için tekrar tekrar aynı kodun yazılmasının önüne geçmek için tekrar eden içerikleri bir fonksiyon içerisine, eğer daha karmaşık bir sistemse bir sınıf altında toplanmış fonksiyonlar ile yapılacak işlemler kontrol altına alınarak daha düzenli bir sistem elde edilmiş olacaktır. Bu sebeple tekrar eden veya sistemin geliştirildiği düşünüldüğünde tekrar etmesi olası olan işlemler kontrol altına alınmıştır. Tekrar etmesi olası olan işlemler için fonksiyon haline getirilen komutlar aşağıda verilmiştir.

1- Kullanıcı Yönetim Sistemi

   a- public string MailGonder(string EMail, string Konu, string Mesaj)

      Bu fonksiyon ile SMTPClient sınıfını kullanarak bir e-mail oluşturarak istenilen herhangi bir e-mail adresine e-mail gönderilebilir. İşlem sonucu string bir değişken olarak döndürülecek ve e-mail gönderilip gönderilmediği öğrenilmiş olacak.

   b- public string ipAl()

      Bu fonksiyon vasıtası ile sistemde oturum açacak olan kullanıcıların ip adresleri alınacak. Bu işlem için gelen http isteği içerisinde bulunan kullanıcının ip adresi alınacaktır. Ekstra doğruluk için yönlendirme yapılan ip adresleri üzerinde de kontrol yapılarak son ip adresine ulaşılmış olacaktır.

   c- public string rastgeleKod()

      Bu fonksiyon 6 karakterden oluşan rastgele doğrulama kodları oluşturmaktadır. Oluşturulan kodlar klavyede bulunan 32 küçük, 32 büyük harf ve 10 adet sayı karakteri arasından rastgele olarak seçilecektir. Rastgele olarak seçilen bu kodlar toplamda 74 karakter arasından seçileceğinden dolayı 74^6 farklı kombinasyon oluşturulmuş olacaktır.

2- Muhasebe ve Görev Yönetim Sistemi

   a- public bool login()

      Bu fonksiyon kullanıcıların oturum kontrolünü yapacak olan ana fonksiyon olacaktır. Sistem her sayfa yenilediği zaman çalışarak oturum kontrolünü ve süresini sağlamış olacaktır. Oturum sonlandığı zaman “false” değerini, oturum devam ettiği takdirde “true” değerini döndürecektir. Oturum sonlandığı takdirde giriş yapma sayfasına yönlendirilecektir.

3.3.2.6. Kağıt üzerinde hazırlanan sistemin gerçekleştirilmesi.

Planlanması ve tasarlanması tamamlanan sistemin gerçekleştirilmesi işlemine başlanacaktır. Hazır olan iş akışı, fonksiyonlar ve modellerden yola çıkarak nasıl bir sistem gerçekleştirileceği açık ve net olduğu için hızlı bir süreçte sistem gerçekleştirilecektir ve proje tamamlanacaktır.

KAYNAKÇA

- https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication
- https://www.telestax.com/blog/increase-security-with-two-factor-authentication-2fa/
- https://medium.com/@devrimdanyal/parolas%C4%B1z-kimlik-do%C4%9Frulama-12ad4264bdf8
- https://www.onlinewebfonts.com/icon/445488
- https://tr.wikipedia.org/wiki/%C3%87ok_fakt%C3%B6rl%C3%BC_kimlik_do%C4%9Frulamas%C4%B1
- https://www.beyaz.net/tr/guvenlik/makaleler/web_tabanli_single_sign_on_cas_oauth2.html
- https://ceaksan.com/tr/single-sign-on-sso-nedir/