Mobil Kullanıcılar için Konum Tabanlı Rastlantısal Tek Kullanımlık Şifreler

Muhammed ÖZSOY[1], Mustafa BURUNKAYA[2]

[1]Elektronik-Bilgisayar Eğitimi, Gazi Üniversitesi, Ankara, Türkiye
[2]Elektrik-Elektronik Mühendisliği Bölümü, Gazi Üniversitesi, Ankara, Türkiye
muhammedozsoy@hotmail.com, bmustafa@gazi.edu.tr
(Geliş/Received: 05.02.2013; Kabul/Accepted: 24.05.2013)

Özet – Elektronik hesapların hızla arttığı günümüzde kimlik doğrulama en önemli güvenlik meselelerinden biri olarak ortaya çıkmıştır. Konu üzerinde pek çok çalışma yapılmış olup, çoğu etkinliği, yaygınlığı ve düşük maliyeti sebebiyle çözümlerinde mobil cihazların kullanıldığı kimlik doğrulama tasarımlarını tercih etmiştir. Şüphesiz, mobil cihazlar yaşamımızın vazgeçilmez bir parçası durumundadır. Sahip oldukları yetenekler her geçen gün artmaktadır. Şu an itibariyle piyasada yer alan mobil cihazların çoğu Küresel Konumlama Sistemi (GPS) ile donatılmış durumdadır. Bu teknoloji sayesinde mobil cihazın dünya üzerindeki konumu anlık olarak elde edilebilmektedir. Bu çalışmada, kimlik doğrulama zorunluluğu olan ve kullanıcısı için maddi ve manevi değer arz eden her türlü online hesaba erişirken kullanılabilecek konum tabanlı rastlantısal bir Tek Kullanımlık Şifre (TKŞ) tasarımı önerilmiş ve simülasyon ortamında bir uygulama örneği başarıyla gerçekleştirilmiştir. Önerilen tasarımda, biri hizmet alan GPS teknolojisine sahip kullanıcının mobil cihazı, diğeri hizmet veren sunucu donanımı üzerinde çalışan iki farklı yazılım modülü geliştirilmiştir. Bu tasarımla birlikte kullanıcı doğrulamasında konum bilgisi de bir parametre olarak kullanılmıştır. Kolayca her iki tarafa da kurulabilen yazılım modülleri sayesinde, kalıcı şifreler kullanan kimlik doğrulama tasarımlarının sebep olduğu güvenlik açıkları giderilmiştir. Kullanıcı konum bilgisinin bir etken olarak TKŞ üretimine dâhil edilmesi kimlik doğrulama sistemi için daha güvenli ve daha uygun bir özellik olarak tasarımda yerini almıştır.

Anahtar Kelimeler– Tek kullanımlık şifre, SHA-1 hash algoritması, kimlik denetimi, GPS

Location-Based Random One Time Passwords for Mobile Users

Abstract – Recently, user authentication has emerged as one of the most important security issues as a result of the enormous growth of the electronic accounts. A lot of work has been made on the subject, and most of that work has preferred authentication scheme using mobile devices for their own solutions. No doubt, mobile devices have become an indispensable part of our daily lives. Their capabilities are increasing every day. As of now, most of mobile devices on the market is equipped with the Global Positioning System (GPS). The real-time location data of a mobile device can be obtained thanks to this technology. In this paper, a location-based random one time passwords scheme are proposed and an implementation was carried out successfully. When accessing the online accounts that require to be made authentication, proposed scheme will provide high reliability for authentication process. Two separate software modules have been developed. One of those runs over the user's mobile device that has GPS technology and other one runs over the authentication server. With this proposed scheme, location information has been used as a parameter in the process of user authentication. Thanks to software modules that can be installed easily on both sides, security vulnerabilities that are caused by permanent passwords have been fixed. User location information that is included as a factor in the production of OTP has taken part in the proposed scheme for authentication system as a safer and more convenient feature.

Keywords– One time password, SHA-1 Hash algorithm, authentication, GPS

1. GİRİŞ (INTRODUCTION)

Sağladığı faydalar sebebiyle mobil cihazlar günlük hayatta geniş bir kullanım alanına sahiptir. Bu cihazların önemi o kadar artmıştır ki, çoğumuz onlarsız bir hayatı düşünememektedir. Sahip olduğu bu yaygın kullanımdan dolayı birçok sorunun çözümünde kullanılan bu cihazlar bu çalışmanın da konusu olan kullanıcı kimlik doğrulama alanında önemli faydalar sağlamaktadır. Günümüzde piyasaya sürülen mobil cihazların çoğu gerçek zamanlı konum bilgisi sağlayan GPS [1] teknolojisi ile donatılmaktadır.

Gerek mobil cihazların gerekse İnternet hizmetlerinin yaygınlaşmasına bağlı olarak, online işlemler yaşamımızın vazgeçilmez parçası olmuştur. Sanal ortamda gerçekleştirilen bu işlemlerde de, gerçek

dünyada olduğu gibi kullanıcının kimliğinin doğrulanması şartı vardır. Bu işlem, gerçek dünyada biyometrik özellikler, nüfus kimlik kartları, sürücü belgeleri vb. niteliklerle gerçekleştirilirken, sanal ortamda kalıcı şifreler, akıllı kartlar, token adı verilen cihazlar veya TKŞ 'ler ile yapılmaktadır. Bu alandaki belirleyici unsur, kimlik doğrulama yöntemlerinin, güvenlik seviyesini artırmasının yanı sıra, insanlar için kullanımı kolay olmasıdır [2]. Bu sebeple, TKŞ 'ler günümüzde en çok tercih edilen kullanıcı kimlik doğrulama yöntemlerinin başında gelmektedir.

Genel olarak kimlik doğrulama tasarımlarını bağlantılı ve bağlantısız olmak üzere ikiye ayırabiliriz. Bağlantılı tasarımlarda kimlik doğrulama işlemi, doğrulamayı yapan web sunucusu ile doğrulanan kullanıcının mobil cihazı arasında bir iletişim kanalı aracılığıyla gerçekleştirilir. Günümüzde, Özel Sanal Ağlar (VPN) veya Mobil İletişim Operatörlerinin (GSM) sunduğu bir hizmet olan Kısa Mesaj Sistemi (SMS) en çok kullanılan iletişim kanallarıdır. Bağlantısız tasarımlarda ise her iki taraf arasında herhangi bir iletişim kanalına ihtiyaç duyulmaksızın kimlik doğrulama süreci yürütülür. Örnek olarak, Açık Anahtar Altyapısını (PKI) kullanan kimlik doğrulama yöntemleri gösterilebilir [3, 4]. Bağlantılı tasarımların maliyet, kurulum, bakım ve işletim yükleri sebebiyle bu çalışmada bağlantısız tasarım tercih edilmiştir.

Bu çalışmadaki temel amaç basit, verimli ve az maliyetli daha güvenilir bir konumsal TKŞ mekanizması geliştirmektir. Bu yöntem sayesinde kullanıcılar hiçbir maliyet yükü altına girmeden sahip oldukları hesaplara, TKŞ 'lerin sağlamış olduğu yüksek güvenlik ile erişebileceklerdir. Kurulum ve kullanım maliyeti çok düşük olan bu yeni kimlik doğrulama tasarımı, istemci ve sunucu arasında herhangi bir bağlantıya, eş zamanlı çalışmaya, kriptolama ve/veya sertifika kullanımına bağlı ek yazılıma veya donanıma ihtiyaç duymadan çalışabilmekte, aynı zamanda üst düzey bir güvenlik de sağlamaktadır.

Son yıllarda kullanıcı konumunun bir etken olarak kimlik doğrulama tasarımlarında tercih edilmesiyle birlikte kullanıcı konumuna göre giriş izninin verilip verilmemesi ve kullanıcının sistem üzerindeki yetkilerinin belirlenebilmesi gibi birçok yeni özellik kullanılmaya başlanmıştır. Genel olarak Konum Tabanlı Erişim Kontrolü [5] (KTEK) olarak adlandırılan yöntemlerin sağladığı faydalar göz önüne alındığında gelecekte daha çok tercih edileceği rahatlıkla söylenebilir. Bu nedenle geliştirilen bu yeni kimlik doğrulama yöntemi de bu konu dikkate alınarak önerilmektedir.

Bu çalışmanın II. bölümünde kısaca daha önce gerçekleştirilmiş konu ile ilgili çalışmalara, III. bölümünde çalışmanın detaylarına, IV. bölümünde tasarımı test etmek amacıyla gerçekleştirilen bir uygulamanın detaylarına, V. bölümünde de tasarımın etkinlik testlerine ilişkin bir çalışmaya değinilmiştir. Son olarak VI. bölümünde de çalışmanın sonuçlarına yer verilmiştir.

2. İLGİLİ ÇALIŞMALAR (LITERATURE)

Lamport [6] 1981 'de kendi kimlik doğrulama mekanizması olan tek kullanımlık şifre tasarımında tek yönlü hash fonksiyonlarının kullanımını önerdiğinden beri, güvenliği geliştirmek için çeşitli tasarımlar önerilmiştir. Tasarımlarda tek yönlü fonksiyonlardan faydalanılmasının temel sebebi, üretilen şifreden fonksiyona sokulan şifre metninin elde edilememesidir. Güvenliğin gelişmesi ve şifre tablolarının dezavantajları sebebiyle, kullanıcıların her an için farklı şifrelerle giriş yapabilecekleri tek kullanımlık şifre tasarımları önerilmektedir.

Günümüzde en yaygın olarak kullanılan yöntemlerden biri olan zaman tabanlı mekanizma, istemci ve sunucu arasında eş zamanlı çalışan bir zaman değeri kullanılır. Bu mekanizmada şifre belirli bir zaman aralığı için üretilir ve sadece o zaman aralığında geçerli olur. Ancak bu belirlenen zaman aralığı geniş tutulursa, aynı şifrenin tekrar kullanımı söz konusu olur ve bu da kullanıcı hesabına, Phishing olarak adlandırılan araya girme saldırısı aracılığıyla, istenmeyen yetkisiz erişimlere sebep olabilir [7]. Ayrıca, mekanizma istemciden sunucuya erişme zamanını da göz önünde bulundurarak bir zaman sapma değeri de hesaplamak zorundadır [8, 9, 10].

Bir diğer yöntem, olay tabanlı yani sisteme yapılan başarılı erişim sayısına bağlı olarak değişen şifrelerdir. Bu tasarımda, hem istemci hem de sunucu tarafında eş zamanlı çalışan bir sayaç mevcuttur. İstemci, sisteme giriş yapabilmek için tek kullanımlık şifre üretirken sahip olduğu özel anahtarı ve bu sayaç değerini kullanır. Şifre üretiminden sonra sayaç bir artırılır. Sunucu da aynı şekilde kullanıcı tarafından girilen şifrenin doğrulamasını yapabilmek için mevcut kullanıcının özel anahtarını ve sayacının değerini kullanır. Kullanıcı doğrulaması yapıldıktan sonra sunucu tarafındaki ilgili kullanıcıya ait sayaç değeri de bir artırılır. Hem sunucu hem de istemci tarafında aynı değere sahip olması gereken sayaç değeri, istemci tarafında her bağlanma girişimi ile artırılırken, sunucu tarafında sadece başarılı bir doğrulama sonucunda artırılmaktadır. Bu da istemci ve sunucu sayaçları arasında eş zamanlılığın bozulmasına ve geçerli bir kullanıcının sisteme bağlanamamasına sebep olmaktadır. Sunucu, herhangi bir kullanıcı tarafından girilen şifrenin kendi hesapladığı şifre değeri ile eşleşmemesi üzerine, kendi sayaç değerini bir artırarak girilen şifreyi tekrar doğrulamayı dener. Bu işlem sistem yöneticisinin belirlediği bir sayıda devam ettirilir. Eşleşme olmuyorsa kullanıcı doğrulaması yapılmaz yani giriş reddedilir. Fakat bu yöntem de özellikle Brute Force [11] saldırılarında sunucunun çok sayıda hesap yapması gerektiği anlamına gelir. Bu da sunucunun devre dışı kalmasına kadar varan sakıncalı durumları doğurur. Bu deneme sayısı küçük tutulursa bu kez de geçerli bir kullanıcının sisteme bağlanamama gibi bir risk ortaya çıkar [8, 10, 12].

GPS teknolojisinin gelişmesiyle birlikte, bilgisayar dünyasında karşılaşılan birçok problemin çözümü için konum tabanlı yaklaşımlar önerilmektedir. Bu çalışmanın konusu olan kullanıcı kimlik doğrulama alanında

örneğin; Bertolissi ve Fernandez, Rol Tabanlı Erişim Kontrol (RBAC) modeli üzerine bir çalışma yapmışlardır. RBAC [13], kullanıcıların sistemdeki rollerine göre sistem kaynaklarına erişimini sağlayan bir kimlik doğrulama ve yetkilendirme modelidir. İlgili çalışmada, RBAC modeline konum ve zaman parametreleri eklenerek, kullanıcının konumuna ve erişim zamanına bakılarak sisteme giriş hakkı verilip verilmeyeceğini belirleyen TLRBAC adında bir model önerilmiştir [14]. Benzer olarak Damiani ve diğerleri, GEO-RBAC olarak adlandırdıkları çalışmalarında, kullanıcının konumuna göre sistem üzerindeki yetkilerini belirleyen bir yöntem önermişlerdir [15]. Yazarlar 2008 yılında da, GEO-RBAC yönteminin gelişmiş bir versiyonu olan Devamlı GEO-RBAC (GEO-RBAC$_C$) yöntemini önermişlerdir. GEO-RBAC$_C$ yöntemi ile birlikte kullanıcının hareketi sonucu konumunun değişmesine bağlı olarak sistem üzerindeki yetkilerinin de anlık olarak değişebilmesi sağlanmıştır [16].

Berbecaru, Konum Tabanlı Uzak İstemci Kimlik Doğrulama Protokolü (LRAP) olarak adlandırdığı çalışmasında, kullanıcıların, bulundukları konum ve zamana, sahip oldukları bir şeye ve ezberlerinde tuttukları bir şifreye göre kimliklerini doğrulayacak bir yöntemi mobil ortamlar için önermiştir. Çalışmasında güvenli olmayan ağlar üzerinden doğrulama yapmayı amaçlamış ve bu nedenle açık anahtarlama altyapısını kullanmıştır. Ayrıca kullanıcı konumunu belirlemek üzere, GPS yerine Avrupa Galileo programı kapsamında geliştirilen Galileo Local Elements teknolojisini kullanmayı tercih etmiştir [17].

Liao ve Chao, Konum Tabanlı Veri Şifreleme Algoritması (LDEA) olarak adlandırdıkları çalışmalarında, şifreleme amacıyla koordinat verileriyle birlikte bir rastlantısal anahtar değerini birleştirmişlerdir. Bu algoritma ile birlikte alıcının, şifreli mesajı sadece daha önce belirlenmiş bir konumda iken çözebilmesi sağlanmıştır. Ayrıca konumdaki hassasiyet sorununa çözüm olarak Tolerans Mesafesi (TD) olarak adlandırdıkları bir çözüm yolu önermişlerdir [18].

Scott ve Denning, Coğrafi-Şifreleme olarak adlandırdıkları çalışmalarında ise hem konuma hem de zamana bağlı olarak şifreleme yapan bir yöntem önermişlerdir. Bu yöntem ile birlikte, şifreli veri sadece kısıtlı bir bölgede, kısıtlı bir zaman aralığında deşifre edilebilmektedir [19].

Hsieh ve Leu, TLBOTP olarak kısalttıkları Zaman ve Konum Tabanlı Tek Kullanımlık Şifre tasarımlarında, konum ve zaman ikilisine bağlı olarak kullanıcının TKŞ üretebilmesini sağlayan bir yöntem önermişlerdir. Bu yöntem kullanıcı belirli bir doğrultuda ilerlerken, yani konumunu değiştirirken, tekrar tekrar giriş yapmasını gerektirmeyen bir özelliğe de sahiptir. Kullanıcının sisteme girdiği TKŞ üzerinde yapılan bir hesaplamayla kullanıcı konumu elde edilmeye çalışılmakta ve bu elde edilen konum verisi ile kullanıcıya giriş izni verilip verilmeyeceğinin kararı verilmektedir. Ayrıca olabilecek bazı giriş sorunlarına çözüm olarak SMS üzerinden kullanıcının giriş yapabilmesini sağlayacak farklı bir yöntem de önerilmektedir [20].

Kimlik doğrulama sürecinde mobil telefonları kullanan yöntemler üretilen her bir şifrenin üretildiği telefona özgü eşsiz değerlere sahip olabilmesi için ilgili cihaza ait bazı eşsiz özelliklerden faydalanırlar [21]. Bu çalışmada da mobil yazılımın üzerinde çalışacağı telefona ait IMEI ve IMSI numaraları kullanılmıştır. Bu numaralar her bir kullanıcı için sunucu veri tabanında depolanacaktır.

3. KONUM TABANLI RASTLANTISAL TEK KULLANIMLIK ŞİFRELER (LOCATION-BASED RANDOM ONE TIME PASSWORDS)

Bu çalışmada önerdiğimiz tasarımda, her kullanıcı için ilk kayıt sürecinin Açık Anahtar Altyapısı [3, 4] sistemini kullanan güvenli bir kanal üzerinden tamamlandığı varsayılmaktadır. İlk kayıt sürecinden sonra kullanıcı kendi mobil cihazına kurduğu bir yazılım aracılığıyla Konum tabanlı Rastlantısal Tek Kullanımlık Şifre (KRTKŞ) üretebilecektir.

KRTKŞ üretiminde, her bir kullanıcı için farklı olup değişkenlik göstermeyen etkenlerin yanı sıra, kullanıcının hareketine bağlı olarak değişen konum ve her giriş işleminden sonra farklı bir değere sahip olan Değişken PIN (DPIN) faktörleri kullanılmaktadır. KRTKŞ üretiminde kullanılan tüm faktörler Tablo 1 ’de listelenmiştir.

Tablo 1. KRTKŞ üretiminde kullanılan faktörler
(The factors used in the production of KRTKŞ)

Faktörler	Açıklama	Örnek
kullanıcıAdı	Kullanıcının sistemde tanımlı olan adı	kullanici1
spin	(SPIN) Sabit PIN Kodu	tks123.
dpin	(DPIN) Değişken PIN Kodu	s6e7a5
dk	(DK) Rastlantısal Doğrulama Kodu	b12l6m9
imei	(IMEI) Uluslararası Mobil Cihaz Kodu	123456789012345
imsi	(IMSI) Uluslararası Mobil Abone Kodu	123456789012345
k	(K) X, Y değerlerine sahip kullanıcı konum verisi	N39.940, E32.823

KullanıcıAdı, SPIN, IMEI ve IMSI faktörleri her bir kullanıcı için sabit değerlere sahiptirler. İlk kayıt esnasında, doğrulama sunucusuna ait veritabanına kaydedilirler. Kullanıcılar, sisteme yaptıkları başarılı bir Giriş ‘in ardından kendilerine ait bu verileri istedikleri gibi güncelleyebilirler. Bu şekilde, KRTKŞ ürettikleri mobil cihazlarını değiştirebilir veya düzenli olarak SPIN şifrelerini güncelleyebilirler. Kullanıcı mobil cihazının

kopyalanması gibi bir durum sonucunda, saldırganların eline geçebilecek IMEI ve IMSI kodları, SPIN ve DPIN değerleri sebebiyle, sistem üzerinde herhangi bir güvenlik açığı oluşturmaz. Çünkü SPIN değeri, cep telefonu üzerinde saklanmaz ve sadece kullanıcı tarafından bilinebilir. DPIN ise, art arda üretilen KRTKŞ 'lerin birbirlerinden tamamen farklı olması ve aralarında herhangi bir bağlantının bulunmaması amacıyla rastlantısal olarak değişkenlik gösterir. DPIN için, ilk kayıt sırasında hem sunucu hem de istemci tarafına aynı değere sahip bir ilk değer atanır. Bu ilk değer ile sunucu tarafından üretilip Giriş ekranında gösterilen rastlantısal Doğrulama Kodu (DK) 'na XOR işlemi uygulanır. Çıkan sonuç hem KRTKŞ üretiminde kullanılır hem de DPIN 'in yeni değeri olarak atanır. Bu şekilde başarıyla sonuçlanan her bir Giriş işleminden sonra DPIN verisi rastlantısal olarak değişmiş olur. K değeri ise, kullanıcının konum verisi olup kullanıcının hareketine bağlı olarak değişir.

3.1. GPS Kullanıcı Konum Faktörü (GPS User Location Factor)

Tasarımda, GPS koordinat verisi Enlem (X) ve Boylam (Y) değerleri ile kullanılmıştır. Dünya, Ekvator çizgisi ile Kuzey – Güney, ilk(sıfır) boylam çizgisi ile Doğu – Batı şeklinde yarım kürelere bölünmüştür. Coğrafi Koordinat Sistemi (CKS) de bu çizgiler temel alınarak geliştirilmiştir. Örneğin, ülkemiz Ekvator çizgisine göre kuzey yarım kürede, ilk boylam çizgisine göre de doğu yarım kürede yer almaktadır. Bu nedenle ülkemizde yer alan herhangi bir noktanın CKS 'ye göre enlem verisi "N" (North), boylam verisi ise "E" (East) harfleriyle başlamaktadır. Tablo 2 'de genel olarak kullanılan üç farklı coğrafi koordinat sayı formatı gösterilmektedir [1]. Bu çalışmada, kullanımı daha basit olduğu için desimal sayı formatı tercih edilmiştir.

Tablo 2. Coğrafi koordinat sayı formatı tablosu
(Table of geographic coordinate number format)

CKS Sayı Formatı	Açıklama	Örnek	
DD° MM' SS.s"	Derece Dakika Saniye.Salise	N 39° 56' 24.7''	E 32° 49' 23.4''
DD° MM.mmm'	Derece Dakika	N 39° 56.411'	E 32° 49.390'
DD.dddddd°	Derece (Desimal Format)*	N 39.940187	E 32.823162

* Tercih edilen coğrafi koordinat sayı formatı

Şekil 1'de gösterildiği üzere, geliştirilen sunucu yazılımına ait web arayüzü yardımıyla kullanıcının Giriş işlemi yaparken bulunması gereken konum, noktasal değil bölgesel olarak tanımlanmaktadır. CKS Desimal konum formatına göre noktadan sonra altı basamak yer alır. Tasarımda kullanıcı konum verisi için virgülden sonra üç basamak kullanımı tercih edilmiştir. Bu şekilde, kullanıcı konumu bir nokta olarak değil, bir bölge olarak ele alınması planlanmıştır. Bunun sebebi, noktasal kullanıcı konumunun sebep olacağı aşırı hassasiyetin getireceği sorunların önüne geçmektir. Ayrıca doğrulama sürecinde geçerli her bir konum için üretilecek KRTKŞ 'lerin sayısı da önemli oranda düşürülmüş olunur ki bu kimlik doğrulama sürecinin hızına olumlu yönde katkı sağlar.

Şekil 1. Belirlenen geçerli bir Giriş alanı
(Specified a valid input field)

İlk kayıt sürecinde kullanıcının belirlemiş olduğu bir bölge, geçerli bir bölge olarak doğrulama sunucusunun veritabanına ilgili kullanıcı için kaydedilir. Kullanıcı belirlenen bu bölge sınırları içindeyken ilk Giriş işlemini yapar. Bu Giriş işleminden sonra kullanıcı kendi adına, belirlenen bu bölgeyi değiştirebilir veya yeni geçerli bölgeler ekleyebilir. Kullanıcı, eklediği herhangi bir bölgenin içindeyken ürettiği KRTKŞ ile kendini sisteme doğrulatabilir. Aksi halde kullanıcının ürettiği KRTKŞ sistem tarafından tanınmayacak ve kullanıcının girişine izin verilmeyecektir.

3.2. Konum Tabanlı Rastlantısal Tek Kullanımlık Şifre Üretim Süreci (The Processes of Location-Based Random One Time Password)

KRTKŞ değerleri, Tablo 1 'de listelenen faktörlerin, Tablo 3 'te listelenen operatörler kullanılarak formül **(1)**'de gösterildiği gibi kullanılmasıyla elde edilmektedir.

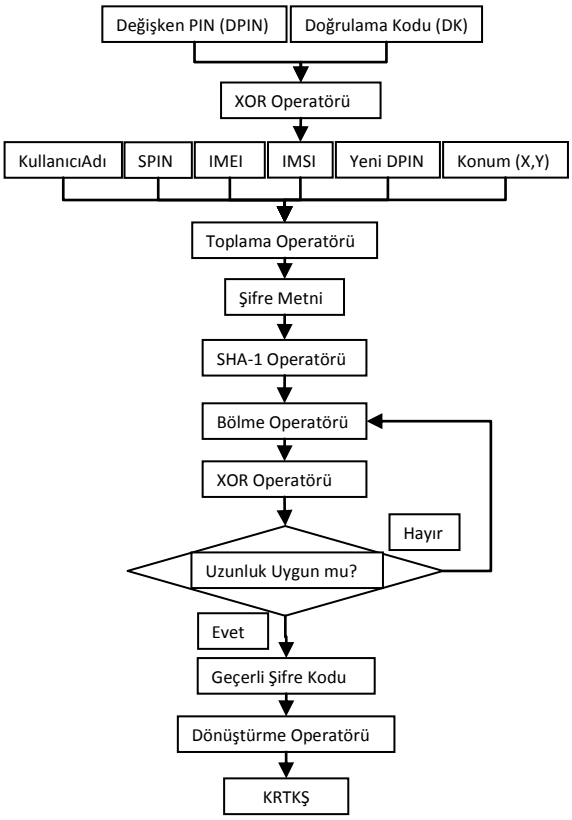
Tablo 3. KRTKŞ üretiminde kullanılan operatörler
(The operators used for the production of KRTKŞ)

Operatörler	Açıklama
h()	Tek yönlü SHA-1 hash fonksiyonu
⊕	XOR operatörü
+	String toplama operatörü
b()	String bölme operatörü
u()	String uzunluk ölçme operatörü
d()	Dönüştürme operatörü

KRTKŞ üretim formülü;

$$
\begin{aligned}
dpin_1 &= (dpin_0 \oplus dk) \\
krtk\S_1 &= h(kullanıcıAdı+spin+imei+imsi+dpin_1+k) \\
krtk\S_{2a} &= b(krtk\S_1(0, [u(krtk\S_1)/2])) \\
krtk\S_{2b} &= b(krtk\S_1((u(krtk\S_1)/2)+1,u(krtk\S_1))) \\
krtk\S_2 &= krtk\S_{2a} \oplus krtk\S_{2b} \qquad (1) \\
krtk\S_{3a} &= b(krtk\S_2(0, [u(krtk\S_2)/2])) \\
krtk\S_{3b} &= b(krtk\S_2((u(krtk\S_2)/2)+1,u(krtk\S_2))) \\
krtk\S_3 &= krtk\S_{3a} \oplus krtk\S_{3b} \\
KRTKŞ &= d(krtk\S_3)
\end{aligned}
$$

Şekil 2 'de KRTKŞ üretim algoritmasında da gösterildiği üzere kullanıcı hesabının bulunduğu sisteme giriş yapmak istediğinde, Giriş Sayfasında gösterilen DK değerini mobil cihazı üzerinde çalıştırdığı yazılım modülüne girer. Bu değer DPIN olarak adlandırılan ve cihazın hafızasında saklanan bir değer ile XOR operatörüne sokulur. Çıkan sonuç hem yeni DPIN olarak hafızaya, bir önceki değerin üzerine, yazılır hem de şifre üretme sürecinde kullanılmak üzere diğer etkenlerle birlikte toplama operatörüne parametre olarak verilir. Toplama operatörü kullanıcı adını ve SPIN şifresini kullanıcıdan, IMEI ve IMSI değerlerini mobil cihazın sistem kaynaklarından ve konum verisini de mobil cihaz üzerinde yüklü olan GPS yazılımından birer parametre olarak alır. Sırasıyla tüm bu değerleri birleştirir ve yapılmak istenen Giriş işlemi için eşsiz bir değer olan Şifre Metnini üretir. Bu Şifre Metni, güvenli SHA-1 hash fonksiyonuna [22] parametre olarak verilir. Çıkan sonuç kırk karakter uzunluğunda düz bir metindir. Tasarımda bu metnin uzunluğu on karakter olarak istendiği için sırasıyla bölme ve XOR operatörlerine sokulur. Bölme operatörü düz metni eşit uzunlukta iki parçaya ayırır ve XOR operatörüne parametre olarak verir. Bu işlem art arda iki kez tekrarlandıktan sonra istenen şifre Geçerli Şifre Kodu üretilmiş olur. Daha sonra bu kod basit bir dönüştürme operatörü ile nihai hali olan KRTKŞ 'ye çevrilir.

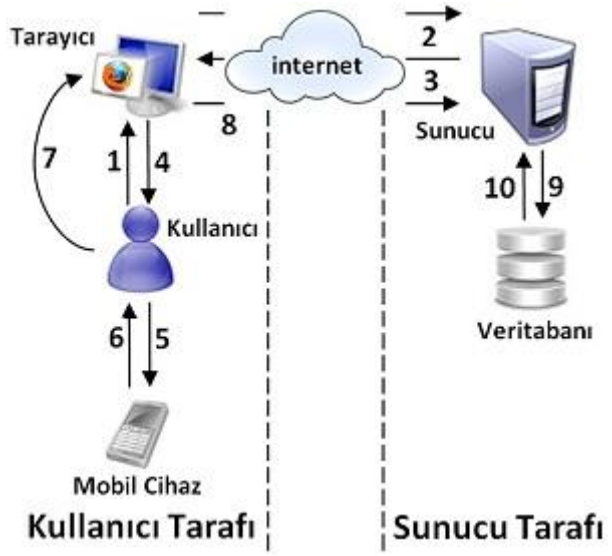


Şekil 2. Konum Tabanlı Rastlantısal TKŞ algoritması
(The Algorithm of Location-Based Random One Time Password)

Algoritmada, özetleme operatörü olarak SHA-1 Hash fonksiyonunun tercih edilme sebebi, girdi parametresinin karakter uzunlu ne olursa olsun, sonuçta sabit 40 karakterden oluşan bir çıktı üretmesidir. Bu çıktı değeri, sırasıyla önce iki eşit parçaya bölünür ve parçalar üzerinde XOR işlemi uygulanır. Bu işlem art arda olmak üzere iki kez tekrarlanır ve sonuç olarak 10 karakterden oluşan Geçerli Şifre Kodu elde edilir. Elde edilen bu koddan, özetleme fonksiyonun çıktı değerine ulaşmak imkânsızdır. Bu nedenle, tercih edilen özetleme fonksiyonunun açıkları, doğrulama sistemi üzerinde herhangi bir güvenlik riski oluşturmaz.

3.3. Kullanıcı Kimlik Doğrulama Süreci
(The Authentication Process On The Client Software)

Şekil 3'de gösterildiği üzere kullanıcı kimlik doğrulama süreci on adımdan oluşmaktadır.

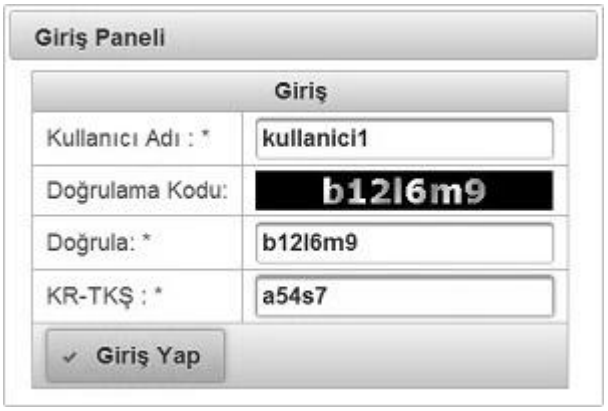


Şekil 3. Kullanıcı kimlik doğrulama süreci
(The Authentication Process on the Client Software)

Adım 1. Kullanıcı hesabına erişmek amacıyla bir web tarayıcı aracılıyla sisteme istekte bulunur.
Adım 2. Kullanıcı isteği web tarayıcısı tarafından İnternet üzerinden sunucuya iletilir.
Adım 3. Sunucu gelen isteğe cevaben, kullanıcı için rastlantısal olarak ürettiği DK ile birlikte Giriş sayfasını tarayıcıya gönderir.
Adım 4 ve 5. Kullanıcı, giriş sayfasında yer alan DK değerini okur ve mobil cihazı üzerinde çalışan uygulamaya, kullanıcı adı ve SPIN değerleriyle birlikte, bu değeri girer.
Adım 6. Mobil uygulama, parametre olarak aldığı DK değerinin yanı sıra, cihazın sistem kaynağından IMEI ve IMSI değerlerini okur. Ayrıca, mobil cihaz üzerinde var olan GPS uygulamasından da konum verisini alarak yeni bir KRTKŞ değeri üretir.
Adım 7. Kullanıcı üretilen KRTKŞ değerini mobil cihazından okur ve tarayıcıda açık olan Giriş sayfasındaki uygun alana girer. Ayrıca DK değerini de Giriş sayfasına tekrar girer.
Adım 8. Kimlik doğrulama isteği sunucuya iletilir.
Adım 9. Sunucu istekte bulunan kullanıcı için veritabanından kullanıcının doğrulama faktörleriyle birlikte ilgili kullanıcı için geçerli tüm konum verilerini de alır.
Adım 10. Kullanıcının geçerli her bir konum verisi için ayrı ayrı KRTKŞ üretir ve kullanıcının girdiği KRTKŞ değeri ile karşılaştırır. Ürettiği KRTKŞ değerlerinden herhangi biri kullanıcının girdiği KRTKŞ değeri ile uyuşursa kullanıcı doğrulaması gerçekleşir. Aksi halde, giriş isteği reddedilir.
Son adımda da belirtildiği gibi, kullanıcı tarafından daha önce belirlenmiş olan muhtemel konum bölgelerinin her biri için sunucu tarafından bir KRTKŞ değeri üretilir. Çünkü doğrulama sunucusu kullanıcının konumunu bilmemektedir. Bu nedenle, muhtemel tüm geçerli bölgeleri dener.

4. KONUM TABANLI RASTLANTISAL TEK KULLANIMLIK ŞİFRE UYGULAMASI (APPLICATION OF LOCATION-BASED RANDOM ONE TIME PASSWORDS)

Bu bölümde, tasarıma ait simülasyon ortamında geliştirilen uygulamanın detaylarına yer verilmiştir. Planlandığı üzere, kimlik doğrulama sunucusuna ve kullanıcı mobil cihazına, Java platformu üzerinde geliştirilen yazılım modüleri kurulduktan sonra sistem aktif hale gelir. Kullanıcı, kayıt sürecinde belirlemiş olduğu bölge sınırları içindeyken, hesabının bulunduğu sisteme giriş talebinde bulunur. Bu talep herhangi bir web tarayıcısı üzerinden gerçekleştirilebilir. Kimlik doğrulama sunucusu tarafından, Şekil 4 ’te gösterilen giriş sayfası ile bu talep cevaplanır.



Şekil 4. Kimlik doğrulama uygulaması Giriş sayfası
(The login page for the authentication application)

Doğrulama Kodu (DK) Giriş sayfasında küçük bir resim karesi içinde yer almaktadır. Kullanıcı, bu kodu hem Şekil 4 ’te gösterildiği gibi Giriş Sayfasındaki, hem de Şekil 5 ’te gösterildiği gibi hali hazırda mobil cihazında çalışan uygulamadaki ilgili alana girer.

Şekil 5. Mobil uygulama DK giriş ekranı görüntüsü
(The login page on the mobile application for DK)

Mobil uygulama, DK değerini aldıktan sonra Tablo 1 'de listelenen örnek parametrelerle KRTKŞ üretim sürecini başlatır. Yapılan ilk işlem, kullanıcı tarafından girilen DK ile hafızada tutulan DPIN değerlerinin XOR operatörüne sokulmasıdır. DK değerinin karakter uzunluğu rastlantısal olarak değişim gösterdiği için bu iki parametreden kısa olanının sonuna sıfır (0) değeri eklenerek, uzunluk olarak diğerine eşitlenir. Sıfır değeri, XOR operatöründe etkisiz eleman olduğu için seçilmiştir. Çıkan sonuç, kullanıcı adı, SPIN, IMEI, IMSI ve konum verileriyle birleştirilerek düz bir şifre metni oluşturulur. Aynı zamanda, çıkan bu sonuç yeni DPIN değeri olarak bir sonraki şifre üretiminde kullanılmak üzere hafızaya kaydedilir. Oluşturulan şifre metni, Formül 1 'de gösterilen işlemlerden geçirilerek istenen uzunlukta nihai KRTKŞ değeri elde edilir. Şekil 6 'da gösterildiği gibi elde edilen KRTKŞ değeri mobil cihazın ekranında gösterilir.

Şekil 6. KRTKŞ değerinin gösterildiği ekran görüntüsü
(KRTKŞ value shown on the mobile screen)

Kullanıcı, mobil cihazının ekranından okuduğu KRTKŞ değerini Şekil 4 'te gösterilen Giriş Ekranındaki ilgili alana girip "Giriş Yap" butonuna tıklayarak Giriş isteğini kimlik doğrulama sunucusuna iletir. Sunucu ilk olarak DK değerinin Giriş ekranındaki ilgili alana doğru girilip girilmediği kontrolünü yapar. Sunucu, DK değeri doğru girilmişse bir sonraki adıma geçer, aksi takdirde bir uyarı mesajı ile birlikte Giriş sayfasını tekrar kullanıcı web tarayıcısına gönderir. Bu işlemin diğer bir amacı da, Kaba Kuvvet (Brute Force) saldırısı adı verilen bir yöntemle sisteme Giriş isteğinin gönderilmesinin önüne geçilmesidir [23]. Bu saldırıda, bilgisayar korsanlarınca geliştirilmiş bir yazılımın ürettiği rastgele şifrelerle doğrulama sunucusuna art arda giriş isteğinde bulunur. Yapılan her istek sunucuda değerlendirilir ve bu da yetkisiz bir Giriş yapılması ihtimali artırır. Önerilen tasarımda, resim formatında olan DK değerinin bir insan tarafından okunup Giriş Sayfasındaki ilgili alana girilmesi istendiği için bu tehdit ortadan kaldırılmıştır.

Doğrulama sunucu yazılımı, Giriş isteği yapan kullanıcı ile ilgili tüm gerekli veriyi kendi veritabanından çeker ve mobil cihaz üzerinde çalışan yazılımın kullandığı ile aynı algoritmayı kullanarak, ilgili kullanıcı için geçerli tüm alanlara ait KRTKŞ değerlerini üretir. Sırasıyla tüm KRTKŞ 'ler, kullanıcının girmiş olduğu KRTKŞ ile karşılaştırılır. Herhangi biri için eşleşme başarılı olursa, Giriş izni verilir, aksi halde Giriş isteği reddedilir.

5. ÖNERİLEN TASARIMIN ETKİNLİK TESTLERİ (RELIABILITY ASSESSMENT)

Bu çalışmada kullanıcı konumuna ve rastlantısal bir değere bağlı olarak üretilen bir, tek kullanımlık şifre tasarımı önerilmiştir. Biri kullanıcı mobil cihazı, diğeri doğrulama sunucusu üzerinde çalışacak iki ayrı yazılım modülü geliştirilmiş ve mobil yazılım, Sun Wireless Toolkit (SWT) aracıyla test edilmiştir [24]. Uygulama yazılımı ise JBoss Uygulama Sunucusu (JBoss AS 7) üzerinde çalıştırılmıştır [25].

Bu bölümde, önerilen tasarımın sağladığı faydalara ve diğer doğrulama yöntemlerine göre üstünlüklerine yer verilmiştir. İlk olarak, önerilen tasarım açık bir algoritmaya sahiptir. Algoritmanın üçüncü kişiler tarafından biliniyor olması üretilen şifrelerin bu kişiler tarafından elde edilebileceği anlamına gelmez. Bunun sebebi algoritmanın rastlantısallık temeli üzerine kurulmasıdır.

Olay ve zaman tabanlı TKŞ üretim algoritmalarında olduğu gibi eş zamanlı çalışma gerektiren bir mekanizma gerektiren yöntemlerde karşılaşılan taraflar arasındaki eş zamanlığın bozulması sebebiyle, geçerli kullanıcılar için kimlik doğrulama yapılamaması gibi problemler yaşanabilmektedir [8, 12]. Eş zamanlılık gerektiren bir mekanizmaya ihtiyaç duyulmaması sebebiyle önerilen yöntemde bu tip problemler görülmez. Eş zamanlılığın bozulması veya başka bir sebeple, SMS gibi herhangi bir bağlantı üzerinden kimlik doğrulaması yapan yöntemlerde ise gidip gelen veri paketlerinin çalınması, buna bağlı olarak üretilen şifrelerin elde edilmesi gibi problemler yaşanabilmektedir [20]. Örneğin SMS üzerinden haberleşme yapan yöntemlerin güvenliği tercih edilen GSM operatörünün sisteminin güvenliği kadardır. Bağlantı gerektiren bir mekanizmaya ihtiyaç duyulmaması sebebiyle önerilen yöntemde bu tip problemler yaşanmaz.

Kullanıcı hareketine bağlı olarak doğrulama ve yetkilendirme yapan mekanizmalarda, zamana göre kullanıcı konumunda gerçekleşen değişimler temel alınmaktadır [16, 20]. Bu yöntemlerde de benzer şekilde zaman bilgisinde taraflar arasında yaşanan eş zamanlılık problemleri ve konum ölçümünde ki hassasiyet kayıpları, bu yöntemlerde yaşanabilecek problemler arasındadır. Önerilen tasarımda geçerli bölge kavramı getirildiği için kullanıcı konum ölçümünde yeterli miktarda tolerans sağlanmıştır.

Önerilen tasarımın, mevcut tüm sistemlere kolay ve maliyetsiz bir şekilde kurulup kullanılması amaçlanmıştır. Ek bir donanım veya ücretli herhangi bir yazılım gerekmemektedir. Kullanıcılar başarılı bir şekilde sisteme giriş yaptıktan sonra kendilerine ait geçerli bölgeleri düzenleyebilmektedir. Yani sistemin yönetimi, büyük

oranda kullanıcılara açılmıştır. Bu nedenle, bir sistem yöneticisi tarafından işletilmesi gerekmez. Geçerli bir bölge için üretilen TKŞ yaşam süreleri, yapılan başarılı giriş işlemine bağlıdır. Gerçekleşen her bir giriş işleminden sonra TKŞ yeni bir değere sahip olur. Tablo 4 'te geleneksel kimlik doğrulama yöntemi ile önerilen yöntem arasında yapılan karşılaştırmalara değinilmiştir. Tablo 5 'te ise günümüzde en çok tercih edilen, TKŞ bazlı kimlik doğrulama yöntemleri ile bu çalışmada önerilen yöntem arasında yapılan karşılaştırmalar gösterilmektedir.

Tablo 4. Önerilen yöntem ile geleneksel kimlik doğrulama yönteminin karşılaştırılması
(Comparison of proposed method with the conventional method of authentication)

	Geleneksel Yöntem	Önerilen Yöntem
Şifre Yaşam Süresi	**Kalıcı**	**Başarılı Bir Giriş**
Kullanıcı Konumu	**Yok**	**Var**
Saldırılara Karşı Açıkları	**Yüksek**	**Düşük**
Şifre Ezberleme	**Var**	**Yok**
Kurulum, Kullanım ve Bakım Maliyeti	**Yok**	**Yok**

Tablo 5. Önerilen yöntem ile diğer TKŞ bazlı kimlik doğrulama yöntemlerinin karşılaştırılması
(Comparison of the proposed method with other TKŞ authentication methods)

	Zaman Bazlı Yöntemler	SMS Bazlı Yöntemler	Önerilen Yöntem
Şifre Yaşam Süresi	**Belirli Bir Süre**	**Belirli Bir Süre**	**Başarılı Bir Giriş**
Kullanıcı Konumu	**Yok**	**Yok**	**Var**
Kullanım ve Bakım Maliyeti	**Yok**	**Var**	**Yok**
Eşzamanlı Çalışma Zorunluluğu	**Var**	**Yok**	**Yok**
Bağlantı Gereksinimi	**Yok**	**Var**	**Yok**
Şifre Üretimi	**Hemen**	**Beklemeli**	**Hemen**
Kullanıcı için Doğrulama Süreci	**Basit**	**Karmaşık**	**Basit**

6. SONUÇLAR (CONCLUTIONS)

Bu çalışmada, kullanıcı konumuna ve rastlantısal bir değere bağlı olarak üretilen bir, tek kullanımlık şifre tasarımı önerilmiştir. Biri kullanıcı mobil cihazı, diğeri doğrulama sunucusu üzerinde çalışacak iki ayrı yazılım modülü geliştirilmiştir. Her iki yazılım modülü için de Java platformu tercih edilmiştir. Mobil yazılım, Sun Wireless Toolkit (SWT) aracıyla test edilmiştir. Java MIDP 2.0 çalıştırabilen herhangi bir mobil cihaz üzerinde sorunsuz bir şekilde kullanılabilmektedir. TKŞ üretim faktörlerinden olan DPIN değerinin saklanması dışında ekstra bir bellek ihtiyacı gerekmemektedir. Uygulamanın çalıştırıldığı mobil cihazın, kullanıcı konumunu elde edilebilmesi için, GPS özelliğine sahip olması gerekmektedir. Uygulama yazılımı ise JBoss Uygulama Sunucusu (JBoss AS 7) üzerinde çalıştırılmıştır. Uygulama yazılımını çalıştıran sunucu üzerinde JDK (Java Development Kit) yazılımının kurulu olması gerekmektedir. Sunucu, kendisinin de bulunduğu yerel ağ üzerinde, kullanıcı bilgilerini depolamak ve sorgulamak amacıyla bağlanabileceği bir veri tabanına ihtiyaç duymaktadır. Kimlik doğrulama yazılımı Java programlama dili ile geliştirildiği için platform bağımsızdır ve bahsi geçen yazılım altyapısına sahip, web sunucusu olarak konfigüre edilmiş, her türlü donanım üzerinde sorunsuz bir şekilde çalışacaktır. Tekil olarak merkezi bir sunucu üzerine kurulan Uygulama yazılımı ile kendisiyle aynı yerel ağı paylaşan, farklı birçok web uygulamasına, kullanıcı kimlik doğrulama hizmeti sunulabilir. Bu şekilde, bir kez kimliğini doğrulatan kullanıcı, birbirinden bağımsız olarak çalışan farklıuygulamalar arasında, tekrar kimliğini doğrulatmaya gerek olmaksızın geçiş yapabilecektir.

Yapılan testler sonucunda kimlik doğrulama işleminin başarıyla gerçekleştirildiği görülmüştür. Amaçlanan hedef doğrultusunda, tek kullanımlık şifreler, herhangi bir bağlantı veya eş zamanlı çalışma gerektiren bir mekanizmaya ihtiyaç duymadan üretilmiştir. Tek kullanımlık şifrelerin sağladığı faydalar sayesinde kimlik doğrulama sistemlerinin güvenilirliği artırılmıştır.

KAYNAKLAR (REFERENCES)

[1] I. Getting, The global positioning system, IEEE Spectrum (1993) 36–47.

[2] K. Bıçakçı, Kullanışlı Güvenlik için Temel Prensipler. ISCTURKEY, pp.102-107, 2010.

[3] S. Wakid, Entity Authentication Using Public Key Cryptography. FIPS Pub 196, National Inst Of Standards And Technology Gaithersburg Md, 1997.

[4] D. Whitefield, M. Hellman, New directions in cryptography. IEEE Transactions on Information Theory, vol. 22, Issue 6, pp. 644-654, Nov. 1976.

[5] A. Cleeff, W. Pieters, R. Wieringa. Benefits of Location-Based Access Control: A Literature Study. IEEE Computer Society, 978-0-7695-4331-4/10, 2010.

[6] L. Lamport, 1981, Password authentication with insecure communication. Communications of the ACM, 24 (11); sayfa: 770-772.

[7] H. Karacan, S. Özdemir İnternet Bankacılığı içim İmgesel Bağıl-Konum-Tabanlı Tek-Kullanımlık Şifre Sistemi. ISCTURKEY, pp.194-199, 2010.

[8] I. Lin, C. Chang. A countable and time-bound password-based user authentication scheme for the applications of electronic commerce. Information Sciences 2009;179:1269–1277.

[9] H. C. Kim, H. W. Lee, K. S. Lee, M. S. Jun. A Design of One-Time Password Mechanism using Public Key Infrastructure. Fourth International Conference on Networked Computing and Advanced Information Management. DOI 10.1109/NCM.2008. 77, 978-0-7695-3322-3/08 © 2008 IEEE.

[10] Y. S. Lee, H. T. Lim, H. J. Lee. A Study on Efficient OTP Generation using Stream Cipher with Random Digit. Advanced Communication Technology (ICACT). 2010;2 pp: 1670-1675.

[11] J. S. Cho, S. S. Yeo, S. K. Kim. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. Computer Communications 2011; 34:391–397.

[12] S. Liao, Q. Zhang, C. Chen ve Y. Dai. A Unidirectional One-Time Password Authentication Scheme without Counter Desynchronization. ISECS International Colloquium on Computing, Communication, Control, and Management 2009. 978-1-4244-4246-1/09.

[13] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-based access control models. IEEE Computer Society, 29(2):38–47, 1996.

[14] C. Bertolissi, M. Fernandez. Time and Location Based Services with Access Control. New Technologies, Mobility and Security, 2008. pp.1-6, 5-7 Nov. 2008 doi: 10.1109/NTMS.2008.ECP.98.

[15] M. L. Damiani, E. Bertino, B. Catania, and P. Perlasca. GEO-RBAC: A spatially Aware RBAC. ACM Transactions on Information and System Security (TISSEC), 10(1), 2007.

[16] M. L. Damiani, E. Bertino, C. Silvestri. An Approach to Supporting Continuity of Usage in Location-based Access Control. 12th IEEE International Workshop on Future Trends of Distributed Computing Systems, p.199-205, October 21-23, 2008.

[17] D. Berbecaru. LRAP: A Location-Based Remote Client Authentication Protocol for Mobile Environments. Parallel, Distributed and Network-Based Processing (PDP), 2011 19th Euromicro International Conference on. pp.141-145, 9-11 Feb. 2011 doi: 10.1109/PDP.2011.32.

[18] H. C. Liao, Y.H. Chao. A New Data Encryption Algorithm Based on the Location of Mobile Users. Information Technology Journal. 7(1) 63-69, 2008.

[19] L. Scott and D. Denning. Geo-encryption: using GPS to enhance data security. GPS World, 40-49, 2003.

[20] W. B. Hsieh, J. S. Leu. Design of a Time and Location Based One-Time Password Authentication Scheme. Wireless Communications and Mobile Computing Conference (IWCMC). pp.201-206, 4-8/07/2011 doi: 10.1109/IWCMC. 2011. 5982418.

[21] F. Aloul, S. Zahidi, W. El-Hajj. Multi Factor Authentication Using Mobile Phones. IEEE/ACS International Conference on Computer Systems and application, pp. 641-644, 2009.

[22] Draft FIPS PUB 180-4. Secure Hash Standard (SHS). Information Technology Laboratory, National Institute of Standards and Technology, March 2012.

[23] C. JS, Y. SS, K. SK, Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. Computer Communications 2011; 34:391–397.

[24] oracle.com. Sun Java™ Wireless Toolkit for CLDC Version 2.5.2 Basic Customization Guide, Sun Microsystems, Inc. September 2012. URL: http://www.oracle.com/technetwork/java/index-jsp-137162.html [Son Erişim: Ocak 2013.

[25] jboss.org. JBoss Application Server 7 Doc. Red Hat, Inc. [Son Erişim: Ocak 2013] URL: https://docs.jboss.org/author/display/AS7/Documentation.