

**MOBİL TELEFONDA ÜRETİLEN TEK KULLANIMLIK
ŞİFRE İLE RASTLANTISAL DEĞİŞKEN VE KONUMSAL
BAZLI KİMLİK DOĞRULAMA**

Muhammed ÖZSOY

**YÜKSEK LİSANS TEZİ
ELEKTRONİK BİLGİSAYAR EĞİTİMİ ANABİLİMDALİ**

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

**HAZİRAN 2013
ANKARA**

Muhammed Özsoy tarafından hazırlanan MOBİL TELEFONDA ÜRETİLEN TEK KULLANIMLIK ŞİFRE İLE RASTLANTISAL DEĞİŞKEN VE KONUMSAL BAZLI KİMLİK DOĞRULAMA adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Mustafa BURUNKAYA
Tez Yöneticisi

Bu çalışma, jürimiz tarafından oy birliği / oy çokluğu ile Elektronik Bilgisayar Eğitimi Anabilim Dalında Yüksek lisans tezi olarak kabul edilmiştir.

Başkan : Prof. Dr. O. Ayhan ERDEM

Üye : Yrd. Doç. Dr. Mustafa BURUNKAYA

Üye : Yrd. Doç. Dr. Hüseyin POLAT

Tarih : 19/06/2013

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü fikir ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Muhammed ÖZSOY

MOBİL TELEFONDA ÜRETİLEN TKŞ İLE RASTLANTISAL DEĞİŞKEN VE KONUMSAL BAZLI KİMLİK DOĞRULAMA

(Yüksek Lisans Tezi)

Muhammed ÖZSOY

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

HAZİRAN 2013

ÖZET

Bu çalışmada, kimlik doğrulama zorunluluğu olan ve kullanıcısı için maddi ve manevi değer arz eden her türlü online hesaba erişirken kullanılabilecek yeni bir kimlik doğrulama tasarımı önerilmiş ve bir uygulama örneği başarıyla gerçekleştirilmiştir. Tasarımda konum ve rastlantısal değişken tabanlı Tek Kullanımlık Şifreler (TKŞ) kullanılmıştır. Tasarımda, biri hizmet alan Küresel Konumlama Sistemi (KKS) teknolojisine sahip kullanıcının mobil cihazı, diğeri hizmet veren sunucu donanımı üzerinde çalışan iki farklı yazılım modülü geliştirilmiştir. Gerçekleştirilen tasarım, istemci ve sunucu yazılım modülleri arasında herhangi bir iletişim kanalına veya kurulum ve kullanım maliyetine ihtiyaç duymaksızın çalışabilmektedir. Ayrıca, eş zamanlı çalışma, şifreleme veya sertifika kullanımına bağlı herhangi bir ek yazılım ve donanım gerektirmez. Aynı zamanda, her iki taraf içinde yüksek bir güvenlik düzeyi sağlar. Önerilen tasarım, şifre iletim güvenliği, istemci ve sunucu arasında eş zamanlı çalışma gereksinimi, kullanıcı tarafından sunucu doğrulama ve yüksek maliyet gibi mevcut kullanıcı doğrulama mekanizmalarında karşılaşılan problemlere de çözüm sunmaktadır. Gerçekleştirilen tasarımda, kullanıcı doğrulaması işlemi için konum bilgisi de ilave bir parametre olarak kullanılmıştır. Ek olarak, önerilen kimlik doğrulama mekanizması istemci tarafı ve doğrulama sunucusu tarafı arasında karşılıklı bir kimlik doğrulamayı

mümkün kılmaktadır. Kolayca her iki tarafa da kurulabilen yazılım modülleri sayesinde, kalıcı şifreler kullanan kimlik doğrulama tasarımlarının sebep olduğu güvenlik açıkları giderilmiştir. Kullanıcı konum bilgisinin bir parametre olarak TKŞ üretimine dâhil edilmesi kimlik doğrulama sisteminin güvenliğini artırmıştır. Tasarımın simülasyon ortamında testleri yapılmış ve başarılı sonuçlar alınmıştır.

Bilim Kodu	:	702.3.006
Anahtar Kelime	:	tek kullanımlık şifre, kullanıcı kimlik doğrulama, karşılıklı kimlik doğrulama, konumsal kimlik doğrulama
Sayfa Adedi	:	68
Tez Yöneticisi	:	Yrd. Doç. Dr. Mustafa BURUNKAYA

**AUTHENTICATION BASED ON POSITION AND RANDOM VARIABLE
THROUGH ONE TIME PASSWORD PRODUCED IN MOBILE PHONE**

(M. Sc. Thesis)

Muhammed ÖZSOY

**GAZİ UNIVERSITY
INFORMATICS INSTITUTE**

JUNE 2013

ABSTRACT

In this paper, a new authentication scheme that will provide high reliability for authentication process when accessing the online accounts that require to be made authentication are proposed and an implementation was carried out successfully. The scheme includes location and random variables based One Time Passwords (OTP). Two separate software modules have been developed. One of those runs over the user's mobile device that has Global Positioning System (GPS) technology and other one runs over the authentication server. This new authentication scheme can work without need for any link between client and server software modules, and with its any installation and usage costs. Also, it would not require any synchronized-work, encryption and additional software or hardware related to use of certification. At the same time, it provides a high-level security. The proposed scheme provides a solution to the problems of the available user authentication mechanisms such as the security of password transmission, synchronization between client and server, server verification by user and high cost. With this proposed scheme, location information has been used as a parameter in the process of user authentication. In addition, the proposed authentication mechanism allows a mutual authentication between the client side and the authentication server side. 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 parameter in the production of OTP has increased security level of proposed authentication system. This proposed authentication system has been tested in the simulation environment and successful results have been achieved.

Science Code	:	702.3.006
Key Words	:	one time password, user authentication, mutual authentication, spatial authentication
Page Number	:	68
Adviser	:	Assist. Prof. Dr. Mustafa BURUNKAYA

TEŞEKKÜR

Bu çalışmanın gerçekleştirilmesi esnasında desteğini ve yardımlarını esirgemeyen, bilgi ve tecrübesi ile bana yol gösteren, her zaman iyi niyet, sabır ve hoşgörüsünü koruyan sayın danışmanım Yrd. Doç. Dr. Mustafa BURUNKAYA'ya, çalışmalarına kıymetli bilgi ve önerileri ile katkıda bulunan tez izleme komitesi üyeleri Sayın Prof. Dr. O. Ayhan ERDEM ve Yrd. Doç. Dr. Hüseyin POLAT'a, verdikleri destekten ötürü her zaman minnetle anacağım Türkiye Elektrik İletim A.Ş. PMUM Bilgi Sistemleri Müdürlüğü mesai arkadaşlarıma, son olarak öğrenim hayatımda geldiğim noktada en büyük pay sahibi sayın aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

	Sayfa
ÖZET.....	iv
ABSTRACT	vi
TEŞEKKÜR.....	viii
İÇİNDEKİLER.....	ix
ŞEKİLLERİN LİSTESİ	xi
ÇİZELGELERİN LİSTESİ.....	xii
SİMGELER ve KISALTMALAR	xiii
1. GİRİŞ	1
2. TEMEL KAVRAMLAR VE İLGİLİ ÇALIŞMALAR	6
2.1. Kimlik Doğrulama ve Erişim Kontrolü.....	6
2.2. Karşılıklı Kimlik Doğrulama	7
2.3. Tek Kullanımlık Şifreler	7
2.3.1. Matematiksel algoritma tabanlı olanlar	7
2.3.2. Akıllı kart tabanlı olanlar.....	8
2.3.3. Eşzamanlı token tabanlı olanlar.....	9
2.3.4. Kısa mesaj (SMS) tabanlı olanlar	10
2.4. Günümüzde Kullanım Alanları	11
2.5. Güçlü Kimlik Doğrulama Tasarımı.....	12
2.6. Tek Kullanımlık Şifre Tasarım Çeşitleri.....	15
2.6.1. Challenge-Response tabanlı kimlik doğrulama.....	15
2.6.2. S/Key kimlik doğrulama mekanizması	17
2.6.3. Zaman tabanlı kimlik doğrulama.....	19
2.6.4. Sayaç tabanlı kimlik doğrulama	21

2.7.	SHA-1 Özet Fonksiyonu	22
2.8.	Coğrafi Koordinat Sistemi	23
2.9.	Konum Tabanlı Kimlik Doğrulama	24
3.	RASTLANTISAL DEĞİŞKEN TABANLI KONUMSAL KİMLİK DOĞRULAMA TASARIMI	28
3.1.	Tasarımın Detayları	30
3.2.	Kimlik Doğrulama Süreci	35
3.3.	Cep Telefonu ve Doğrulama Sunucusu Arasındaki Şifre İletişimi	37
3.4.	Tek Kullanımlık Şifre Üretim Süreci	38
3.5.	Geliştirilen Kimlik Doğrulama Sunucusu Yazılımı Sınıf Yapısı	41
3.6.	Tasarımın Grafikselsel Kullanıcı Arayüzleri	44
3.6.1.	İstemci TKŞ üretim süreci	44
3.6.2.	Sunucu TKŞ üretim süreci	49
3.6.3.	Son onay süreci	51
3.6.4.	Geçerli bölgeleri ve kişisel bilgileri güncelleme sayfası	52
3.7.	Kimlik Doğrulama Sürecinde Gerçekleşen İşlem Çıktıları	54
4.	ÖNERİLEN TASARIMIN GÜVENİLİRLİK VE ETKİNLİK TESTLERİ	57
5.	SONUÇ	64
	KAYNAKLAR	65
	ÖZGEÇMİŞ	68

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 2.1. Asenkron mekanizma işlemleri.....	16
Şekil 2.2. S/Key kimlik doğrulama işlemleri	18
Şekil 2.3. Senkron mekanizma işlemleri.....	20
Şekil 3.1. İstemci yazılımı için kimlik doğrulama süreci.....	31
Şekil 3.2. Doğrulama sunucusu yazılımı için kimlik doğrulama süreci.....	33
Şekil 3.3. Kimlik doğrulama sürecinde gerçekleştirilen adımlar	35
Şekil 3.4. Taraflar arasındaki TKŞ değiş tokuş döngüsü.....	38
Şekil 3.5. Tek kullanımlık şifre algoritması.....	39
Şekil 3.6. Doğrulama sunucu yazılımı için sınıf yapısı.....	42
Şekil 3.7. Örnek geçerli bir birim bölge gösterimi.....	43
Şekil 3.8. İstemci yazılımı açılış ekranı	45
Şekil 3.9. İstemci yazılımı parametre giriş ekranı.....	46
Şekil 3.10. İstemci yazılımı konum tipi seçim ekranı	47
Şekil 3.11. İstemci TKŞ değeri gösterimi ve sunucu TKŞ giriş talebi.....	48
Şekil 3.12. Doğrulama sunucusu açılış sayfası	49
Şekil 3.13. Doğrulama sunucusu giriş sayfası.....	50
Şekil 3.14. Sunucu TKŞ gösterim sayfası	50
Şekil 3.15. İstemci yazılımı sunucu TKŞ doğrulama sonuç ekranı	51
Şekil 3.16. Geçerli bölgeleri ve kişisel bilgileri güncelleme sayfası	52
Şekil 3.17. Doğrulama sunucusu yeni kullanıcı ekleme sayfası	53
Şekil 4.1. Birinci örneklem kümesi için karakter uzunluklarına göre TKŞ sayıları	57
Şekil 4.2. İkinci örneklem kümesi için karakter uzunluklarına göre TKŞ sayıları ..	58
Şekil 4.3. Birinci örneklem kümesi için istemci ve sunucu değişkenlerinin karakter sayılarına göre değişim oranı grafiği.....	58
Şekil 4.4. İkinci örneklem kümesi için istemci ve sunucu değişkenlerinin karakter sayılarına göre değişim oranı grafiği.....	59

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 2.1. HMAC fonksiyonu ifadeleri ve açıklamaları.....	8
Çizelge 2.2. Coğrafi koordinat sayı formatı çizelgesi.....	24
Çizelge 3.1. TKŞ üretiminde kullanılan faktörler	28
Çizelge 3.2. Tek kullanımlık şifre algoritmasında yer alan işlem operatörleri	40
Çizelge 3.3. Tek kullanımlık şifre algoritmasının matematiksel ifadesi.....	40
Çizelge 3.4. Tasarımda yer alan örnek konum tipleri ve açıklamaları.....	42
Çizelge 3.5. İstemci TKŞ hesaplama işlemleri çıktıları	54
Çizelge 3.6. İstemci TKŞ doğrulama işlemleri çıktıları.....	55
Çizelge 3.7. Sunucu TKŞ hesaplama işlemleri çıktıları.....	55
Çizelge 3.8. Sunucu TKŞ doğrulama işlemleri çıktıları.....	56
Çizelge 4.1. İstemci TKŞ ile geçerli şifre eşleştirme ve istemci değişkenini elde etme	60
Çizelge 4.2. Sunucu TKŞ ile geçerli şifre eşleştirme ve sunucu değişkenini elde etme	60
Çizelge 4.3. Güvenilirlik sınaması parametreleri ve açıklamaları	61
Çizelge 4.4. Bu çalışma ile sunulan yöntem ile geleneksel kimlik doğrulama yönteminin karşılaştırılması	63

SİMGELER ve KISALTMALAR

AAA	Authentication, Authorization and Accounting (Kimlik doğrulama, Yetkilendirme ve Hesap erişim kontrolü)
KKS	Küresel Konumlama Sistemi
DoS	Denial of Service Attack (Hizmet Durdurma Saldırısı)
GEO-RBAC	Geo-Spatial Role Based Access Control (Coğrafi Konumsal Rol Tabanlı Erişim Kontrolü)
TLRBAC	Temporal and Location Role Based Access Control (Geçici ve Konumsal Rol Tabanlı Erişim Kontrolü)
TLBOTP	Time and Location Based One Time Password (Zaman ve Konum Tabanlı Tek Kullanımlık Şifre)
GPS	Global Positioning System (Küresel Konumlama Sistemi)
GSM	Global System for Mobile Communication (Küresel Mobil İletişim Sistemi)
H	Hash Özetleme Fonksiyonu
HMAC	Hash based Message Authentication Code (Hash tabanlı Mesaj Kimlik Doğrulama Kodu)
HOTP	HMAC based One Time Password (HMAC tabanlı Tek Kullanımlık Şifre)
IMEI	International Mobile Equipment Identity (Uluslararası Mobil Cihaz Kodu)
IMSI	International Mobile Subscriber Identity (Uluslararası Mobil Abone Kodu)
KTEK	Konum Tabanlı Erişim Kontrolü
LDEA	Location Based Data Encryption Algorithm (Konum Tabanlı Veri Şifreleme Algoritması)
LRAP	Location Based Remote Client Authentication Protocol (Konum Tabanlı Uzak İstemci Kimlik Doğrulama Protokolü)
MAC	Message Authentication Code (Mesaj Kimlik Doğrulama Kodu)
MD5	MD5 Hash Özetleme Fonksiyonu
OTP	One Time Password (Tek Kullanımlık Şifre)

(devam)

PIN	Personal Identification Number (Kişisel Tanımlama Numarası)
RAM	Random Access Memory (Rastgele Erişimli Hafıza)
RBAC	Role Based Access Control (Rol Tabanlı Erişim Kontrolü)
ROM	Read Only Memory (Sadece Okunabilir Hafıza)
SHA	SHA Hash Özetleme Fonksiyon Ailesi
SIM	Subscriber Identity Module (Abone Kimlik Modülü)
SMS	Small Message System (Kısa Mesaj Sistemi)
SWT	Sun Wireless Toolkit (Sun Kablosuz Cihaz Simülasyon Aracı)
TKŞ	Tek Kullanımlık Şifre
TLRBAC	Temporal and Location Role Based Access Control (Geçici ve Konumsal Rol Tabanlı Erişim Kontrolü)
USB	Universal Serial Bus (Evrensel Seri İletişim Yolu)
XOR	XOR Operatörü
VPN	Virtual Private Network (Özel Sanal Ağ)

1. GİRİŞ

Bu çalışmadaki temel amaç basit, kullanımı kolay ve maliyetsiz daha güvenilir bir tek kullanımlık şifre mekanizması geliştirmektir. Bu tasarım sayesinde kullanıcılar hiçbir maliyet yükü altına girmeden sahip oldukları hesaplara, tek kullanımlık şifrelerin sağlamış olduğu yüksek güvenlik ile erişebileceklerdir. Kurulum ve kullanım maliyeti olmayan bu yeni kimlik doğrulama tasarımı, istemci ve sunucu arasında herhangi bir iletişim kanalına, eş zamanlı çalışmaya, şifreleme ve/veya sertifika kullanımına bağlı ek yazılıma veya donanımına ihtiyaç duymadan çalışabilmektedir.

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

Gerek mobil cihazların gerekse internet hizmetlerinin yaygınlaşmasına bağlı olarak, online işlemler de hızla günlük hayatın vazgeçilmez bir parçası haline gelmiştir. 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. Günümüzde, TKŞ' ler en çok tercih edilen kullanıcı kimlik doğrulama yöntemlerinin başında gelmektedir.

Genel olarak kimlik doğrulama tasarımları bağlantılı ve bağlantısız olmak üzere ikiye ayrılabilir. 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 kanallarının başında gelmektedir. Bağlantısız tasarımlarda ise her iki taraf arasında herhangi bir iletişim kanalına ihtiyaç duyulmaksızın kimlik doğrulama işlemi gerçekleştirilir. Bağlantılı tasarımların maliyet, kurulum, bakım ve işletim yükleri sebebiyle bu çalışmada bağlantısız tasarım tercih edilmiştir.

Kimlik doğrulama amacıyla tek kullanımlık şifrelerin veya şifre üretmek için kullanılan kodların herhangi bir kriptoloji yapılmadan SMS aracılığıyla iletilmesi, sistemleri Man In The Middle adı verilen bir saldırı türüne karşı açık hale getirmektedir [2]. Bu yöntemde bilgisayar korsanları, kurmuş oldukları sahte baz istasyonlarından veya GSM operatörünün kullandığı sistem üzerindeki açıklardan faydalanmaktadırlar. Bu şekilde, kayıtlı bir kullanıcı adına, tek kullanımlık şifre talebinde bulunup, elde ettikleri bu tek kullanımlık şifre ile gerçek kullanıcının haberi olmaksızın hesabına yetkisiz erişim yapabilmektedirler. Bu tip doğrulama mekanizmaları bilgisayar korsanlarına, bu yöntem ile birçok kez aynı hesaba erişme fırsatı vermektedir [3]. İstemci ile doğrulama sunucusu arasındaki veri iletişiminin genel anahtar alt yapısı kullanılarak şifrlenmesi güvenliği belirli bir seviyeye çıkarır. Ancak bu tür tasarımlar doğrulama prosedürünü işletmek üzere, şifreleme ve sertifikasyon işlemleri için ek donanım ve yazılım gereksinimlerine ihtiyaç duyarlar. Bu da maliyeti artırmakta ve kullanıcılara ek yükler getirmektedir [4]. Ayrıca, GSM operatörleri şifre bilgisini içeren SMS' in sorunsuz bir şekilde iletileceğini garanti etmez. İletişimdeki bir sorun kullanıcıların çalışmakta olan sistemlere erişememelerine sebep olacaktır. GSM operatörünün hizmet alanı dışında yer alan kullanıcıların yaşadığı, SMS' in geç gelmesi veya hiç gelmemesi gibi sorunlar sebebiyle, sistemler küresel çapta hizmet verememekte sadece belirli bir bölgeyle sınırlı kalmaktadırlar. SMS gibi kimlik doğrulama amacıyla veri iletişimi gerektiren tasarımlar ilave ücret ödemeyi gerektirir, bu sebeple düşük maliyet isteyen çözümler için pratik olmaktan çıkarlar [5]. Gerçekleştirilen kimlik doğrulama sisteminde istemci yazılımı ile doğrulama sunucusu arasında herhangi bir iletişim kanalı üzerinden bağlantı kurulması söz konusu değildir. Dolayısıyla, iletişimden kaynaklanan problemlerin ve araya girme saldırılarının da önüne geçilebilmektedir.

TKŞ üretimi için en çok tercih edilenlerin başında gelen zaman ve olay tabanlı kimlik doğrulama mekanizmalarında, doğrulama sunucusu ile kullanıcının sahip olduğu cihaz arasındaki eş zamanlı çalışma büyük önem taşımaktadır. Herhangi bir sebeple taraflar arasındaki eş zamanlı çalışmada meydana gelebilecek bir bozulma, geçerli bir kullanıcının sisteme bağlanamaması anlamına gelmektedir. Bu probleme çözüm olarak geliştirilen, sunucunun toleranslı, yani zaman tabanlı çalışan mekanizmada sunucu saatini ileri-geri alarak veya olay tabanlı mekanizmada sayaç değerini artırarak, TKŞ üretmesi beraberinde ek işlem yükü getirmekte ve performans kaybına neden olmaktadır. Bir saldırı durumunda sunucu ağır bir işlem yükü altında kalabilmektedir. Dahası doğrulama işleminde bir dizi TKŞ kullanıldığı için bilgisayar korsanlarının denemiş olduğu sahte şifrenin doğrulanma olasılığı da artmaktadır. Söz konusu probleme çözüm olarak geliştirilen bir başka yaklaşım ise istemci yazılımının TKŞ istemesi veya eş zamanlı çalışmayı tekrar sağlamak için herhangi bir veri iletişim yolu aracılığıyla doğrulama sunucusuna bağlanmasıdır [6]. Bu çözüm yolu, SMS ile doğrulama yapan bağlantılı tasarımlarda olduğu gibi kurulum ve işletim maliyeti, şifreleme gereksinimleri, gidip gelen veri paketlerinin bilgisayar korsanları tarafından ele geçirilmesi veya söz konusu kişilerin gerçek kullanıcı rolüne bürünüp doğrulama sunucusundan geçerli TKŞ elde etmesi gibi problemlere sebep olmaktadır [4,7-9]. Gerçekleştirilen kimlik doğrulama sisteminde her iki taraf için de eş zamanlı çalışması gereken herhangi bir mekanizmaya ihtiyaç duyulmamaktadır. Bu sebeple eş zamanlı çalışmadan dolayı kaynaklanan problemlerin hiçbiri gerçekleştirilen sistem için geçerli değildir.

Tek kullanımlık şifre üretmek için Token adı verilen cihazları kullanan doğrulama mekanizmalarında ise zaman ve olay tabanlı TKŞ algoritmalarında olduğu gibi eş zamanlılık problemleri ve bir cihaz kullanıldığı için her iki tarafa da getirilen ek yükler söz konusudur. Söz konusu sistemde hizmeti veren taraf için, kullanılan cihazın sisteme tanıtılması, sistem ile eş zamanlanması, kullanıcıya ulaştırılması, karşılaşılan teknik problemlerin çözümüne destek verilmesi gibi birçok olumsuz yön mevcuttur. İstemci tarafında ise, token cihazını sürekli yanında bulundurma; düşürme, çaldırma, kaybetme gibi durumlarda şifre üretilmediği için sisteme giriş yapamama ve yeni bir token için ek ücret ödeme gibi birçok olumsuz durumla

karşılaşılmaktadır [10]. Bu çalışmada ise kullanıcı tarafında, mobil bir cihaz üzerinde çalışacak olan bir yazılım söz konusudur. Hizmet sağlayıcısı tarafında ise mevcut doğrulama sunucusu üzerine çok kolay adapte edilebilir, bir yazılım modülü tasarlanmıştır. Hiçbir ek masraf yapılmadan kurulabilecek olan bu yazılımlar ile kullanıcı istediği an istediği yerden, hiçbir ücret ödmeden kolayca kimliğini doğrulatabilecektir.

Üretilen şifrelerin kullanıldıktan sonra üçüncü şahısların eline geçmesinin bir güvenlik sorunu meydana getirmemesi tasarımın önemli avantajlarından biridir. Çünkü üretilen şifrede, doğrulamada kullanılacak olan geçerli şifre ve bir sonraki şifre üretiminde kullanılacak rastlantısal değer tamamen rastlantısal olarak iç içe geçmiş halde bulunmaktadır. Bu yüzden, üretilen tek kullanımlık şifrenin, hangi karakterlerinin geçerli şifreye, hangi karakterlerinin bir sonraki şifre üretiminde kullanılacak rastlantısal değışkene ait olduğu, şifreyi üreten gerçek kullanıcı dahil hiç kimse tarafından bilinmemektedir. Tasarımın bir diğer önemli avantajı ise doğrulama mekanizmasının çift yönlü çalışmasıdır. Bu özellik sayesinde hizmet sağlayıcısının kullanıcı doğrulama yapmasının yanı sıra kullanıcının da hizmet sağlayıcısını doğrulaması mümkün hale gelmektedir. Bunun için doğrulama sunucusu, kullanıcı kimlik doğrulamasını gerçekleştirdikten sonra kullanıcının da hizmet verecek olan sistemi doğrulayabilmesi için bir Sunucu TKŞ değeri üretmektedir. Cep telefonu yazılımı bu değeri sınyarak kullanıcının geçerli olan hizmet sistemine giriş yapıp yapmadığını kontrol eder. Bu sayede kullanıcının, geçerli sistemleri taklit ederek kullanıcı bilgilerini elde etmek amacıyla bilgisayar korsanları tarafından kurulup yönetilen sahte sistemler üzerinde işlem yapması önlenmiş olmaktadır.

Tasarım, bir felaket senaryosu olan kullanıcının tüm bilgilerinin saldırganların eline geçmesi ve geçerli şifreyi üreterek kullanıcının hesabına erişmesi durumunda kullanıcı için önemli bir avantaj sağlayacak bir özelliğe sahiptir. Hesap erişim kontrolü olarak adlandırılan bu özellik, üretilen geçerli şifrenin her iki tarafta da kayıt altında tutulan istemci ve sunucu değışkenlerine bağılı olmasıdır. Bilgisayar korsanlarının yapmış oldukları bu yetkisiz erişim sonrasında doğrulama sunucusu ile

kullanıcı mobil cihazında kayıtlı olan istemci ve sunucu değişkenleri farklı değerlere sahip olacaktır. Bu da gerçek kullanıcının saldırıdan sonra sisteme erişemeyeceği anlamına gelmektedir. Bu, olumsuz bir durum gibi görünse de, asıl amaçlanan gerçek kullanıcıdan farklı bir kişinin hesaba yetkisiz bir erişim yaptığıının ortaya çıkarılmasıdır. Bu yaklaşım, diğer kimlik doğrulama mekanizmalarında bulunmayan yeni bir özellik olarak bu çalışmada sunulmaktadır.

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 KTEK olarak adlandırılan yöntemlerin sağladığı faydalar göz önüne alındığında gelecekte daha çok tercih edileceği rahatlıkla söylenebilir [11]. Bu nedenle, bu yeni kimlik doğrulama mekanizması da bu konu dikkate alınarak geliştirilmiştir.

Bu çalışmada mevcut yöntemlerde var olan problemler dikkate alınarak cep telefonu gibi mobil cihazlar üzerinde herhangi bir iletişim kanalına ihtiyaç duymadan çalışacak yeni bir rastlantısal şifre üretme algoritması geliştirilmiştir. Son kullanıcılar için, ek hiçbir yük söz konusu olmaksızın, hızlı ve basit bir işlemle kimliklerini doğrulatabilmeleri sağlanmıştır. Gerçekleştirilen çözüm, yeni veya mevcut web uygulamalarına herhangi bir ek donanım veya yazılıma gereksinim duymadan basit bir şekilde entegre edilebilmektedir. Tasarım günümüzde kullanılan statik şifre mekanizmalarında olduğu gibi bir şifre tablosu veya bir doğrulama tablosu da gerektirmemektedir.

2. TEMEL KAVRAMLAR VE İLGİLİ ÇALIŞMALAR

Bu bölümde kimlik doğrulama hakkında genel bilgiler, tek kullanımlık şifre çeşitleri ve tasarımlarıyla birlikte bu alanda yapılmış olan çalışmalara yer verilmiştir.

2.1. Kimlik Doğrulama ve Erişim Kontrolü

Kimlik doğrulama, bir kişinin veya bir uygulamanın gerçekte iddia ettiği kişi veya uygulama olduğunun tespit edilmesi amacıyla yapılan işlemlere verilen addır. Kimlik doğrulama tasarımları ise, bir kullanıcıyı ya da uzaktaki bir sunucuyu güvenli olmayan ağlar üzerinden tanıyıp doğrulama yapabilen mekanizmalardır. Leslie Lamport 1981’ de kendi kimlik doğrulama mekanizmasını önerdiğinden beri, sistemlerin güvenliğini daha üst noktalara taşımak amacıyla çeşitli tasarımlar önerilmiştir. Güvenliğin gelişmesi ve şifre tablolarının dezavantajları sebebiyle, uzmanlar kullanıcıların her an için farklı şifrelerle giriş yapabilecekleri tek kullanımlık şifre tasarımları önermişlerdir.

Güvenlik için diğer önemli mekanizmalardan biri olan erişim kontrolü ise, hizmete sunulan kaynaklara, sadece ilgili kaynak için yetkili kullanıcıların erişebilmesine ve yetkileri kapsamında işlem yapabilmesine olanak tanıyan mekanizmalara verilen addır. Geleneksel olarak güvenlik mekanizması, kimlik doğrulama ve erişim kontrolü olarak ikiye ayrılır. Bunların bütünleşik bir tasarımı daha çok kabul görür. Bu sebeple, bazı uzmanlar, işletim karmaşıklığını azaltmak için kimlik doğrulama ile erişim kontrolünü birleştirmişlerdir [12].

Kullanıcı doğrulaması, güvenli olmayan ağlar üzerinden, güvenli iletişim ve sistem kaynaklarının paylaşımını sağlamak için yukarıda bahsi geçen güvenlik mekanizmasının kullanımının bir sonucudur. Özellikle, tek kullanımlık şifrelerin amacı kısıtlı kaynaklara yetkisiz erişim yapmayı daha zor hale getirmektir. Geleneksel kimlik doğrulama sistemleri gibi şifre dosyaları kullanmak yerine, birçok araştırmacı, sistemlerin kurcalanma riskini ve bakım maliyetlerini azaltmak için eşzamanlı tokenler, akıllı kartlar veya kısa mesaj servisleri gibi çeşitli tek kullanımlık şifre

tasarımları uygulamışlardır. Ancak, bu tasarımlar her yerde bulunmayan donanım cihazları ve altyapı gereksinimlerinden dolayı pratik değildirler.

2.2. Karşılıklı Kimlik Doğrulama

Karşılıklı kimlik doğrulama, kullanıcı ve doğrulama sunucu arasında gerçekleşen ve her iki tarafında birbirlerini doğrulamasını mümkün hale getiren mekanizmalardır [13]. Bu sayede geçerli kullanıcıların geçerli sisteme bağlandıkları garanti edilir. Dahası, gerçek sistemlerin taklit edilerek kullanıcı bilgilerinin çalınma riski ortadan kalkar. Bu çalışma ile sunulan kimlik doğrulama mekanizması da karşılıklı kimlik doğrulama yapmaktadır.

2.3. Tek Kullanımlık Şifreler

Tek kullanımlık şifreler, adından da anlaşılacağı üzere, geçerli bir kullanıcı tarafından hizmet sunucusuna yapılan her bir kimlik doğrulama işlemi için farklı bir değere sahip olan şifrelere verilen genel bir addır. Tek kullanımlık şifrelerin amacı erişimi kısıtlanmış kaynaklara yetkisiz erişimi daha da zor hale getirmektir. Alışıldık sabit şifreler yeterli deneme şansı ve zaman verildiği takdirde yetkisiz kişiler tarafından aşılabilmektedirler. TKŞ uygulamalarında, şifre sürekli değiştiği için bu risk büyük oranda azaltılmış olur. TKŞ tasarımları temel olarak dört sınıfa ayrılabilir. Bu tasarımlara yazının devamında alt başlıklar halinde yer verilmiştir.

2.3.1. Matematiksel algoritma tabanlı olanlar

1981 yılında, Lamport, ilk olarak tek kullanımlık şifre tasarımlarında tek yönlü hash fonksiyonlarının kullanımını önermiştir [14]. İletilen mesajın kimin tarafından oluşturulduğu ve bütünlüğünde bir değişim olup olmadığını kontrol etmek amacıyla geliştirilen MAC mekanizmasını temel alarak geliştirilen HMAC mekanizması matematiksel algoritma tabanlı TKŞ üretimine bir örnektir. MAC algoritması iletilmek istenen mesaj ile gizli anahtarın tek bir kez hash algoritmasından geçirerek sonuç çıktısı üretir. Bu yaklaşımın zaman içinde yeterli olmadığı ve çeşitli

yöntemlerle kırılabildiği ortaya çıkmıştır. Bu sebeple, HMAC adında yeni bir algoritma önerilmiştir. Bu algoritmanın şimdiye kadar bilinen bir açığı ortaya çıkmamıştır. Geliştirilen bu algoritma, iletmek istenen mesajı gizli anahtarla birlikte, bir iç ve bir de dış olmak üzere, art arda iki kez hash fonksiyonuna sokmayı önermektedir. Algoritma Eş. 2.1' de ifade edildiği gibi olup Çizelge 2.1' de gerekli açıklamalara yer verilmiştir.

$$H_i = H(\text{anahtar} \oplus \text{ipad}) \parallel \text{mesaj} \quad (2.1)$$

$$\text{HMAC}(\text{anahtar}, \text{mesaj}) = H(\text{anahtar} \oplus \text{opad}) \parallel H_i)$$

Çizelge 2.1. HMAC fonksiyonu ifadeleri ve açıklamaları

İfade	Açıklama
H	kriptografik bir özet fonksiyonu,
Anahtar	gizli bir şifreleme anahtarı,
Mesaj	kimlik doğrulama için kullanılan bir veri dizisi,
	veri birleştirme operatörü,
⊕	xor operatörü,
opad	heksadesimal bir sabit değer (0x5c5c5c5c...5c5c),
ipad	heksadesimal bir sabit değer (0x363636...3636)

Formülde yer alan H hash fonksiyonu için MD5, SHA-1, SHA-2 gibi hash fonksiyonları tercih edilir. Tercih edilen hash fonksiyonuna göre HMAC algoritması HMAC-MD5, HMAC-SHA-1, HMAC-SHA-2 olarak adlandırılır. TKŞ üretim algoritmalarının büyük çoğunluğu bu HMAC algoritmasını kullanmaktadır [15].

2.3.2. Akıllı kart tabanlı olanlar

Akıllı kartlar günümüzde sıklıkla kullanılan manyetik şeritli kartlardan veri depolama, kendine özgü işletim komutlarını işletebilmesi özellikleriyle farklılık gösterir. Akıllı kartlar aritmetik işlemleri çabucak gerçekleştirebilen özelleştirilmiş gömülü bir mikroişlemci, giriş/çıkış birimi, RAM ve bazı mesajları saklayan ROM bellek türü donanımları içerirler. Bundan dolayı sunucuda şifre veya doğrulama

tablosu tutmaya ihtiyaç yoktur. Bu yapısıyla akıllı kartlar küçük bir bilgisayara benzemektedirler. Akıllı kartlar farklı hafıza kapasitesi ve teknik özelliklerine göre çeşitli uygulama alanlarında kullanılmaktadırlar. Manyetik şeritli kartlar ile karşılaştırıldığında, akıllı kartlar yüzlerce defa daha yüksek kapasiteye sahiptir, daha dayanıklıdır ve ileri derecede şifreleme gibi mekanizmalar nedeniyle çok daha güvenlidir. Karta kaydedilen verinin şifrelenerek güvenliği sağlanır. Bu sayede yetkisiz kişilerce kartta bulunan verilerin okunması, silinmesi ve değiştirilmesi engellenmiş olur. Akıllı kartların sağladığı en önemli avantajlar taşınabilirlik ve sağladığı üstün güvenlik özellikleridir. Kişiye ait kimlik işlemlerinde kullandığı gizli bilgiler kartta güvenli bir şekilde depolanabilmektedir. En önemli özelliklerinden birisi de içindeki bilgilerin kopyalanamamasıdır. Kredi kartlarındaki manyetik şerit kopyalanabilir ve bilgiler kullanılabilirken akıllı kart tabanlı kredi kartlarında kopyalama gibi bir işlemin yapılması mümkün değildir. Akıllı kartlar güvenlik seviyeleri ve erişim yetkilerinin tasarlandığı bir sistemde kapıyı açmak için, kullanıcıların kendi bilgisayarlarında oturum açabilmesi için ya da alışveriş yaparken ödeme yapabilmeleri için kullanılabilir. Aynı şekilde internet bankacılığı sistemlerinde kimlik doğrulanma amacıyla bu kartlardan faydalanılabilir. Bu yöntem günümüzde kullanılan şifre ile kimlik doğrulama işlemlerinden çok daha güvenlidir. Dış müdahalelere direnç ve şifre dosyasının yönetimindeki kolaylık sebebiyle, akıllı kartlar uzak kimlik doğrulama tasarımlarının birçoğunda yaygın olarak kullanılmıştır. Fakat kartları ve okuyucuyu taşımak kullanıcılar için bir yük olmaya devam etmektedir. Kart ve okuyucular her yerde bulunmadığından, bu engel akıllı kart tabanlı kimlik doğrulama tasarımına sahip uygulamaları kısıtlamıştır [16].

2.3.3. Eşzamanlı token tabanlı olanlar

Kimlik doğrulama amacıyla kullanılan yazılımsal ve donanımsal olmak üzere iki tür token vardır. Eşzamanlılık prensibine göre çalışan tokenlerin içine ya kimlik doğrulaması yapan sunucu saati ile senkronize edilmiş bir saat ya da her iki tarafta da gerçekleştirilen giriş sayısına göre artırılan bir sayaç yerleştirilmiştir. Kimlik doğrulama amacıyla kullanılan gömülü sistemler olarak da adlandırılabilirler. Yazılımsal tokenler, herhangi bir programlama dili aracılığıyla tek kullanımlık şifre

retmesi iin kodlanan uygulamalardır. Bu alıřmada hedeflenen amalar doęrultusunda tek kullanımlık řifre retebilmek iin bu sistem tercih edilmiřtir. Geliřtirilen yazılım her tr mobil cihaz zerinde alıřabilme imkânına sahiptir. Fiziksel tokenlar, akıllı kart tabanlı tasarımlarla benzer sebepler olan, tek kullanımlık řifre cihazları ve altyapı gereksinimlerinden dolayı kullanım oranları ok dřk olmuřtur [10].

2.3.4. Kısa mesaj (SMS) tabanlı olanlar

SMS, tm telefonlarda mevcut olan ve her yerde bulunan bir iletiřim kanalıdır. Kimlik doęrulama amacıyla SMS kullanımı gnmz sistemlerinde en ok tercih edilen yntemlerden birisidir. Bu yntemde kullanıcı hizmet sunucusuna baęlandığında sahip olduęu kullanıcı adı ve sabit řifresini girer. Bu deęerlerin doęrulaması yapıldıktan sonra istek geerli bir kullanıcıdan geliyorsa, kullanıcı iin tanımlanmıř telefon numarasına rastgele retilmiř bir řifre deęeri gnderilir. Kullanıcı SMS mesajı olarak telefonuna gelen bu deęeri aynı řekilde hizmet sunucusunun web sayfasında belirlenmiř yere girer. Kullanıcı telefonuna gnderilen deęer ile girilen bu deęerin karřılařtırılması sonucunda isteęin geerli bir kullanıcıdan geldięi garanti edilmiř olur. Ancak, SMS en etkin eriřim aracı olmasına raęmen, GSM řirketi SMS' in ulařıp ulařmayacaęını veya belirli bir srede ulařtıracaęını garanti etmez. Belirtmek gerekir ki, bir gvenlik zellięi olarak tek kullanımlık řifrelerin bir sreliğine geerli olması gerekmektedir. Ayrıca, SMS tabanlı tasarım ilave cret demeyi gerektirir, bylece dřk maliyet isteyen zmler iin pratik olmaktan ıkar [6, 17, 18].

SMS tabanlı mekanizmalarda gz ardı edilemeyecek nemli bir gvenlik sorunu mevcuttur. Bu sorun, doęrulama sunucusu tarafından retilen TKř deęerinin GSM operatr zerinden kullanıcı telefonuna iletimi sırasında oluřur. Herhangi bir řifreleme altyapısı kullanılmadan iletilen TKř deęeri, araya girme veya dinleme adı verilen eřitli saldırı trleri ile elde edilebilmektedir. Bu sebeple hem doęrulama sunucusu zerine hem de kullanıcı cep telefonu zerine kurulacak bir řifreleme

altyapısı ile bu tehdit giderilmeye çalışılmıştır. Bu yöntem soruna çözüm sağlamakla beraber, maliyeti de artırmaktadır [18, 19].

Kullanıcıların bir bağlantı kanalı kurmadan TKŞ üretebildikleri yöntemlerde yaşadığı, herhangi bir sebeple şifre üretememe veya ürettiği şifre ile sisteme kendini doğrulatacama gibi durumlarda, doğrulama sunucusuna SMS aracılığıyla bağlantı yapıp şifre isteyebilmektedir. Kullanıcı tarafından gönderilen şifre istek mesajına kullanıcı bilgileri eklenip şifrelenerek sunucuya gönderilmektedir. Sunucu yazılımı şifrelenmiş bir SMS mesajını aldığı anda ilk önce bu mesajı çözmekte ve daha sonra içerdiği bilgilerin geçerli bir kullanıcıya ait olup olmadığını kontrol etmektedir. Geçerli bir kullanıcıdan bu istek gelmişse sistem tarafından geçerli sayılacak bir tek kullanımlık şifre üretilir, bu şifreyi bir şifrelenmiş SMS mesajı formatında doğrudan kullanıcının cep telefonuna iletmektedir. Kullanıcının cep telefonu bu cevap SMS mesajını aldığı anda gerekli şifre çözme işlemlerini yerine getirip geçerli şifreyi cep telefonu ekranına yansıtmak suretiyle kullanıcıya göstermektedir [6].

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 [6]. Bu çalışmada da mobil yazılımın üzerinde çalışacağı telefona ait IMEI ve IMSI numaraları kullanılmıştır. Bu numaralar her bir kullanıcı için sunucu veri tabanında depolanacaktır.

2.4. Günümüzde Kullanım Alanları

İnternet bankacılığıyla ilgili gelişmeleri takip edenlerin de bildiği üzere, 1 Ocak 2010 tarihinden itibaren internet bankacılığına giriş sırasında tek kullanımlık şifre kullanımı zorunlu hale getirilmiştir. Söz konusu karar BDDK tarafından alınmış ve bir sene boyunca, konuyla ilgili gerekli altyapı çalışmalarının tamamlanmasını sağlamak için geçiş süresi olarak kabul edilmiştir.

Tek kullanımlık şifreler için bankaların önünde birkaç seçenek bulunmaktadır. Bunlardan ilki minimal bir altyapı yatırımı gerektiren sistemle üretilen tek

kullanımlık şifrelerin (genelde dört ila altı karakterden oluşan bir sayısal değerdir) bir GSM şirketi gateway'i üzerinden müşterinin sistemde tanımlı cep telefonuna gönderilmesidir. Müşteri gönderilen şifreyi karşısına çıkan ekrana girerek kimlik doğrulamayı sağlamış olur. Burada güvenlik açısından en büyük sorun bankalardan ziyade GSM şirketlerinin SIM kart yenileme süreçlerinden kaynaklanmaktadır. Kötü niyetli kişiler kimlik bilgisini elde ettikleri kişiler adına sahte kimlikler oluşturup, telefon kartlarını kaybedip yenisini almak için başvuruyormuş gibi yaparak yeni hattı üzerlerine almaktadırlar. SIM kart sahibinin orijinal hattı bloke olup, bu süreçte sahte kimlikle hattı alan kişi veya kişiler internet bankacılığından müşterinin hesabını boşaltabilmektedirler.

Tek kullanımlık şifre üreten elektronik cihazların (token) satın alınması ve bunların internet kullanıcılarına dağıtılması da ikinci bir seçenek olarak durmaktadır. Cihazın kurulumu sırasında bir güvenlik şifresi olup, bu şifreyi girince tek kullanımlık şifre üretilmektedir. Üretilen şifre müşterinin karşısına çıkan ekrana girilmek suretiyle güvenlik aşaması geçilmektedir. Fiziksel token kullanımının özellikle müşteriye iletilmesi konusunda lojistik açıdan sıkıntı yaşanmaktadır. Bu cihazların senkronize edilmesi veya kayıp edilmesi durumunda iptali, yeni bir tokenin müşteriye iletilmesi, bu iletilen cihazın tekrar senkronize edilmesi gibi bazı sıkıntılar da beraberinde gelmektedir.

Tek kullanımlık şifre üreten programlar ise günümüzde bu konuda en iyi alternatifi oluşturmaktadırlar. Bankalar, kullanıcıları için basit anlamda java destekleyen cep telefonları için şifre üreten bir program sunmaktadırlar. Cep telefonuna kurulan bu yazılıma kurulum anında belirlenmiş sabit bir şifre ile giriş yapıldığında, tek kullanımlık bir şifre üretilip, ekranda görüntülenmektedir [20].

2.5. Güçlü Kimlik Doğrulama Tasarımı

Güçlü kimlik doğrulama, kimlik doğrulama amacıyla iki veya daha fazla faktörden faydalanan tasarımlara verilen genel bir addır. Güçlü bir kimlik doğrulama, kullanıcı adı ve parolalardan daha yüksek seviyede güvenlik sağlar. Güçlü kimlik

doğrulamanın genel formu “bildiğiniz bir şey, sizde bulunan bir şeydir.” Bu nedenle gizli bir bilgi (“bildiğiniz bir şey”) ve bir doğrulayıcı; örneğin kart, bir USB aygıt ya da sertifika (“sizde bulunan bir şey”) bu ikisinin birden kontrolü kullanıcı adı ve parola (“sadece bildiğiniz bir şey”) ya da biyometrik kontrollerinden daha güvenlidir [17, 21]. Güçlü kimlik doğrulamayı muhakkak kullanması gereken uygulamalar:

- Çok fazla değer arz eden işlemler.
- Gizliliğin çok önemli olduğu ya da yasal zorunlulukların bulunduğu uygulamalar (sağlık ve hastane kayıtları, hükümet kayıtları, vs.)
- Birtakım işlemler sırasında, örneğin bankacılık uygulamalarında, kayıt tutulması zorunlu ve bu kayıtlarla insanlar arasında güçlü bir bağ gerektiği zaman kullanılmalıdır.
- Çok değerli ya da çok kritik sistemlere yönetimsel erişim yapılacağı zaman kullanılmalıdır.

Günümüzde dijital kimliklerin korunması daha fazla önem kazanmaktadır. Kimlik doğrulama için şifre kullanımı artık yeterli ve güçlü kimlik doğrulama düzenleri gerektirir. Güçlü kimlik doğrulama çözümleri, sıklıkla, kullanıcılar için zahmetli ve servis sağlayıcılar için maliyetli ek bir cihaz gerektiren iki tanımlayıcı faktör kullanmaktadır. Ek bir cihaz kullanımını önlemek için, cep telefonunu güvenlik tokeni olarak kullanma genel olarak kabul görmüştür.

İncelenen literatür araştırmalarına göre, güçlü kimlik doğrulamanın üzerinde uzlaşılan ve açık bir tanımı yoktur. Uzmanlara göre, güçlü kimlik doğrulama, ağ üzerinden bir şifre iletmeksizin, ağ kullanıcıları kimliklerinin, istemcilerin ve sunucuların doğrulamasını yapabilen bir bilgisayar güvenliği yöntemidir. ABD Ulusal Standartlar ve Teknoloji Enstitüsü kimlik tanımlamanın dört seviyesini aşağıdaki gibi tanımlamaktadır;

- Seviye 1: Kimlik tanımlayıcı olmadan,
- Seviye 2: Tek faktörlü,
- Seviye 3: Çok faktörlü,

- Seviye 4: Şifreleme protokolleri aracılığıyla bir anahtar tanımlayıcı ile.

Üçüncü seviye çok faktörlü kimlik doğrulama kesinlikle güçlü bir kimlik doğrulama olarak kabul görür. Güçlü bir kimlik doğrulamanın çok faktöre sahip olması gerekmediği de açıktır. Güçlü bir kimlik doğrulama, aşağıdaki kimlik doğrulama faktörlerinden en az ikisini birleştiren bir tasarım olan iki faktörlü kimlik doğrulama ile başlayabilir.

- Bildiğin bir şey;
Şifre, Kimlik doğrulama bilgisi
- Sahip olduğun bir şey;
Tek kullanımlık şifre tokenleri, Dijital sertifikalar, Grid kartlar
- Sahip olduğun bir özellik;
Biyometrik özellikler
- Hakkında bilinen bir şey;
Kimlik doğrulama kimliğin, Aygıt ID' si
- Küresel konumun;
GPS koordinat verileri

Çoğu iki faktörlü kimlik doğrulama tasarımı, “Bildiğin bir şey” ile “Sahip olduğun bir şey” özelliklerini birleştirir. İki faktörlü kimlik doğrulama özellikleri, kullanıcıdan gelen ekstra bakım ve servis sağlayıcıdan gelen yönetim istekleri sebebiyle ek bir cihaz kullanımını gerektirir [17]. Güçlü kimlik doğrulama yapan sistemler, tek kullanımlık şifreleri üretme ve teslim etme yöntemleri, kullanıcı doğrulama ve sahip oldukları güvenlik kısıtları bakımından farklılık gösterirler.

2.6. Tek Kullanımlık Şifre Tasarım Çeşitleri

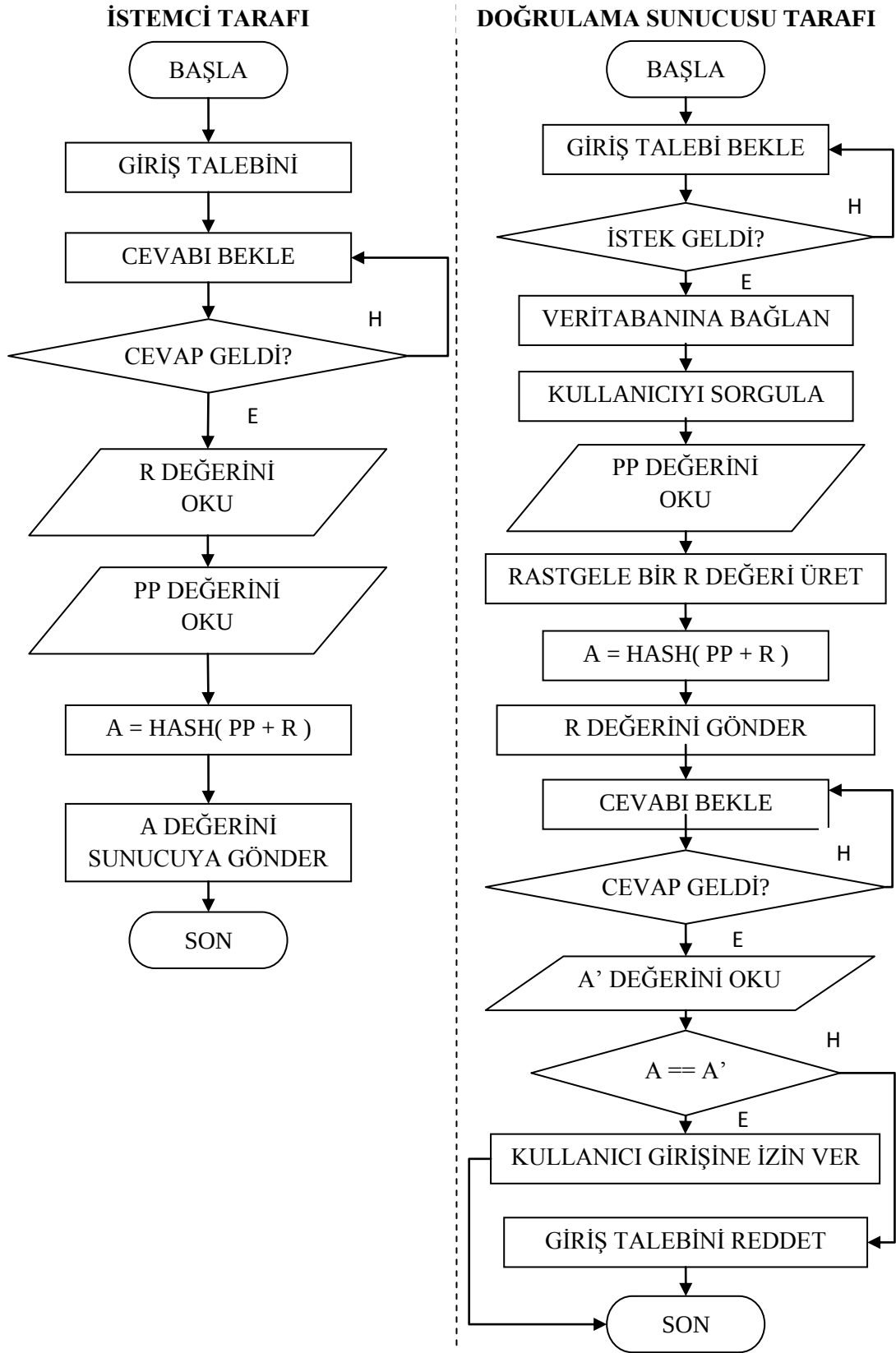
Son zamanlarda, ticarileşme yoluyla ürün olarak ortaya çıkan birçok pratik tek kullanımlık şifre mekanizması vardır. Şifre üretmek için kullanılan, bazı tek kullanımlık şifre mekanizmaları, S/Key kimlik doğrulama, challenge-response kimlik doğrulama ve zaman tabanlı kimlik doğrulama olarak sınıflandırılabilir [22].

2.6.1. Challenge-Response tabanlı kimlik doğrulama

Bu metot, asenkron tek kullanımlık şifre mekanizması olarak adlandırılır. Bir kullanıcı sisteme ilk kez kaydedilirken, sahip olduğu özel anahtar değeri de doğrulama sunucusuna ait veritabanına ilgili kullanıcı adına kaydedilir. Şekil 2.1' de gösterildiği gibi kullanıcı bir giriş talebi yaptığında, doğrulama sunucusu rastlantısal bir değer olan R ile bu talebe cevap verir. Ardından ilgili kullanıcıya ait özel anahtar değeri ile bu R değerini birleştirir. Üretilen bu değeri bir kez Hash fonksiyonuna sokarak A değerini elde eder. Kullanıcı da giriş talebine karşılık olarak aldığı R değeriyle kendi özel anahtarını birleştirir ve bu değeri bir kez Hash fonksiyonuna sokar. Hash fonksiyonunun çıktısı olan A değerini, doğrulamak üzere sunucuya iletir. Doğrulama sunucusu kullanıcıdan gelen A değerini, kendi ürettiği A değeri ile karşılaştırır. Bu iki değer eşleşiyorsa kullanıcının kimliği doğrulanır. Özetle;

- Kullanıcı giriş talebini sunucuya iletir,
- Sunucu rastlantısal R değerini üretip, istemciye iletir,
- Sunucu kendi veri tabanında ilgili kullanıcı için eşleşen gizli anahtarı arar,
- İstemci gelen R değeri ile birlikte kendi gizli anahtarını kullanarak A değerini üretir ve sunucuya kimlik doğrulama isteği ile birlikte iletir,
- Sunucu kendi üretmiş olduğu sonuç ile gelen sonucu karşılaştırarak cevabı istemciye iletir.

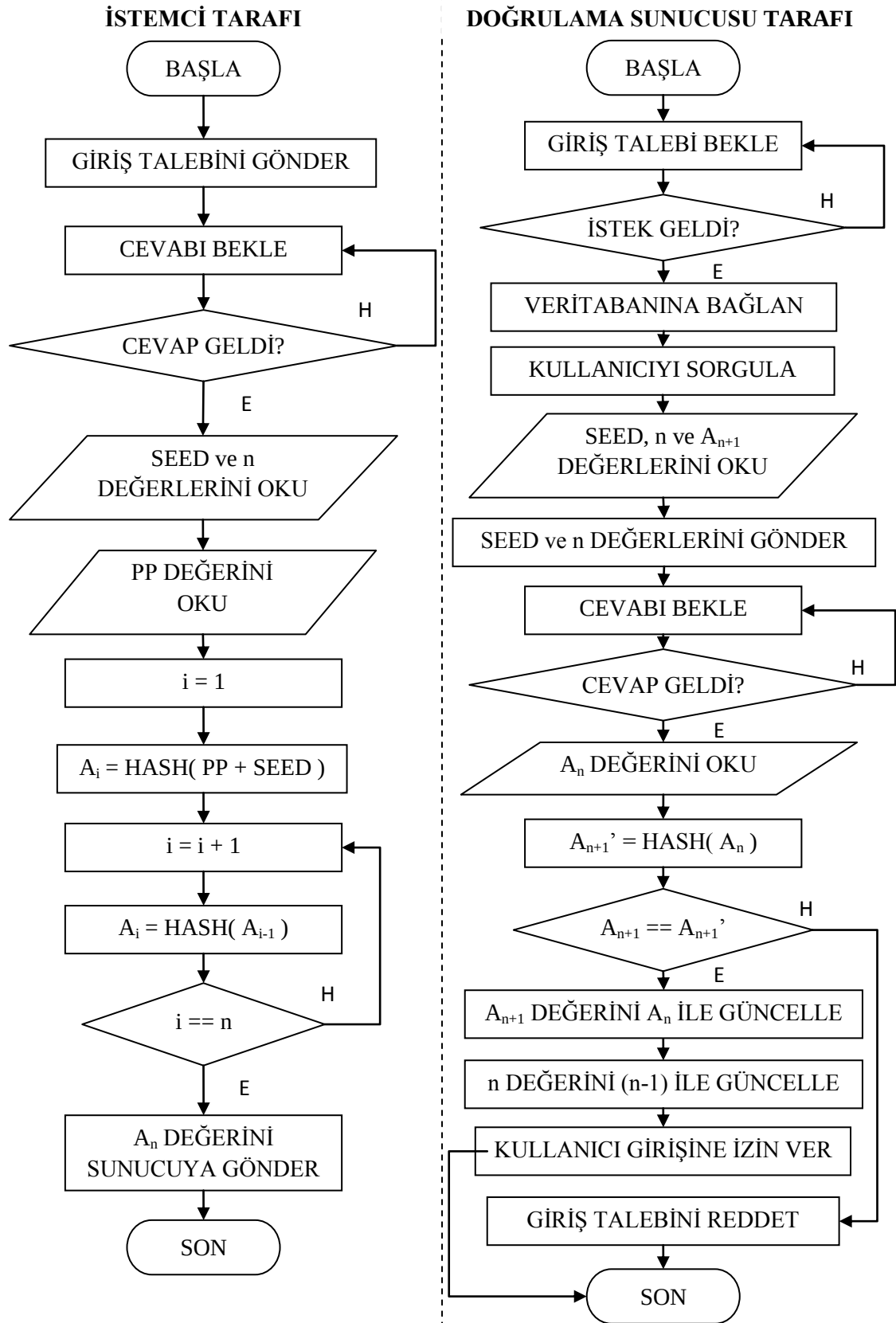
Her iletim zamanında matematiksel fonksiyonlar kullanıldığı için iletişim kurma hızında bir düşüş yaşanır.



Şekil 2.1. Asenkron mekanizma işlemleri

2.6.2. S/Key kimlik doğrulama mekanizması

S/Key kimlik doğrulama mekanizması, şifre doğrulamayı, donanımsal olarak değil yazılımsal metotlar kullanılarak kayıt ve kimlik doğrulamadan oluşan iki aşamada sınıflandırır. Özellikle, kullanıcının gizli anahtarı uygulama sunucusu üzerinde kayıtlı olmadığı için, gizli anahtar çalınmasına karşı güçlü bir çözüm sunmaktadır. Bir kullanıcının sisteme ilk kaydı sırasında, S/Key algoritmasının ilk işlemi, kullanıcının sahip olduğu PP olarak adlandırılan özel anahtarı ile hem kullanıcı hem de doğrulama sunucusu tarafından paylaşılan bir SEED değerinin birleştirilerek bir şifre metni oluşturmaktır. Daha sonra, elde edilen bu şifre metni için, bir Hash fonksiyonu kullanılarak özet bir değer üretilir. Üretilen bu değerde aynı şekilde Hash fonksiyonuna sokulur. Bu işlem art arda $n+1$ kez tekrar edilir. Sonuçta A_{n+1} adı verilen bir kimlik doğrulama değeri elde edilmiş olur. Bu değer ile birlikte n ve SEED değerleri de doğrulama sunucusu veritabanına ilgili kullanıcı adına kaydedilir. Şekil 2.2' de gösterildiği üzere, kullanıcı sisteme giriş yapmak istediğinde, kendi adına kaydedilmiş n ve SEED değerleri ile karşılaşır. Kullanıcı, sahip olduğu özel anahtarı ile SEED değerini birleştirerek şifre metnini ve bu şifre metnini n kez tekrar edecek olan bir Hash zincirine sokarak A_n değerini üretir. Ürettiği bu değeri doğrulama sunucusuna ileterek kimliğinin doğrulanmasını talep eder. Kullanıcıdan A_n değerini alan doğrulama sunucusu, bu değeri bir kez daha Hash fonksiyonuna sokarak A_{n+1} değerini elde eder. Elde ettiği bu değeri, kullanıcı kaydı sırasında kullanıcı adına kaydettiği A_{n+1} değeri ile karşılaştırır. Bu iki değer eşleşirse kullanıcı doğrulanır ve sisteme giriş izni verilir. Doğrulama sunucusu, bir sonraki doğrulama işleminde kullanmak amacıyla, ilgili kullanıcı için kayıtlı olan A_{n+1} değerini A_n değeriyle ve n değerini de $n-1$ değeri ile günceller. Bu şekilde doğrulama sunucusu, kullanıcıdan gelecek bir sonraki giriş talebine karşılık olarak SEED ve $n-1$ değerini karşı tarafa iletebilir.



Şekil 2.2. S/Key kimlik doğrulama işlemleri

S/Key kullanılan kimlik doğrulama işlemlerinin detayları aşağıda listelenmiştir;

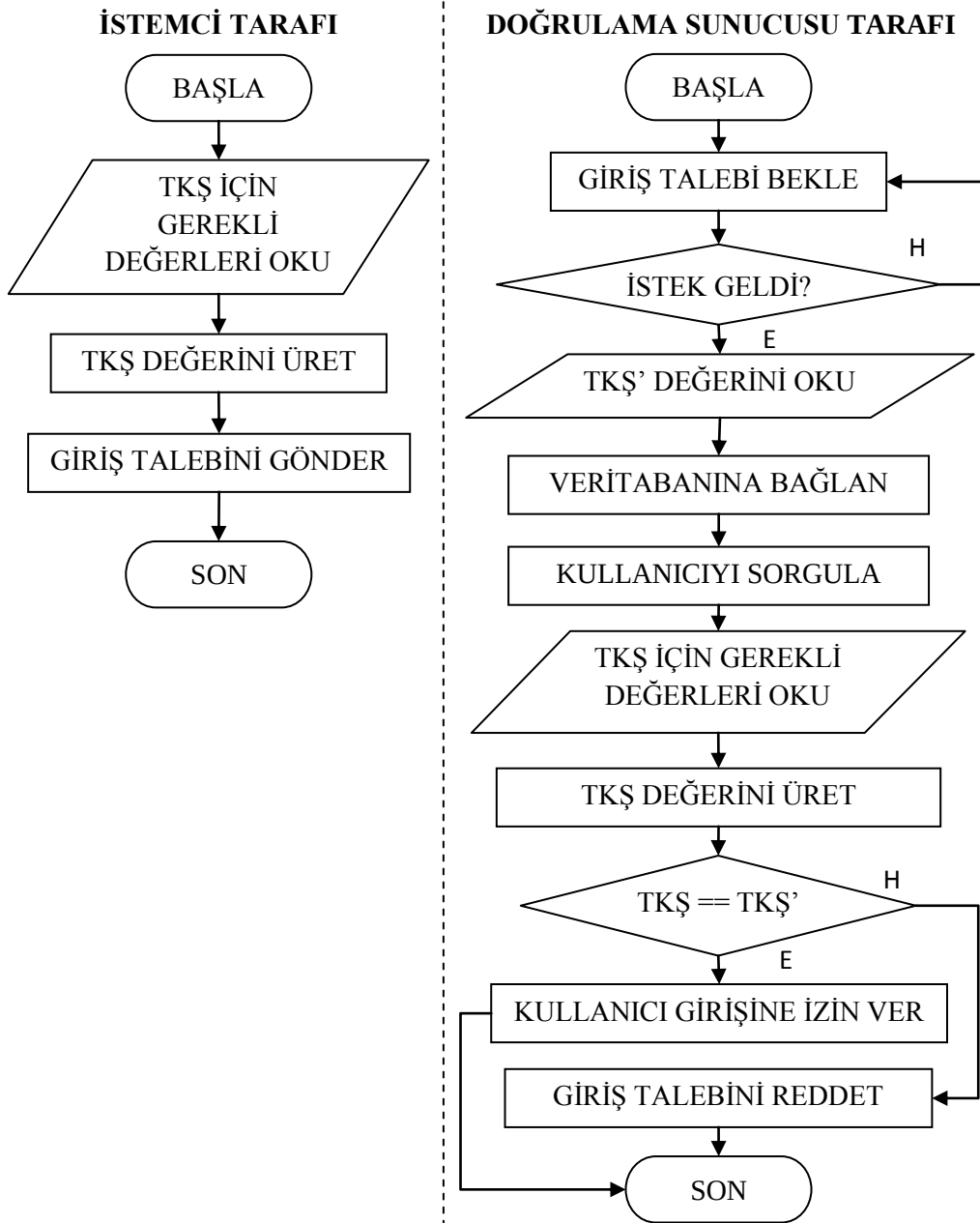
- İstemci, kullanıcı gizli anahtarını da kullanarak şifre cümlesini üretir.
- Sunucu n ve SEED değerlerini istemciye iletir.
- İstemci n , SEED ve üretmiş olduğu şifre cümlesini kullanarak A_n değerini üretir.
- İstemci bu değerle birlikte kimlik doğrulama isteğini sunucuya iletir.
- Sunucu, istemciden gelen A_n değeri ile A_{n+1} değerini üretir.
- Üretilen bu değer ile kayıt sırasında depolanmış A_{n+1} değeri karşılaştırılır.
- İstemciye kimlik doğrulama sonucu iletilir.

S/Key tabanlı kimlik doğrulamada izin verilebilir kimlik doğrulama sayısında kısıtlama yaşanabilmektedir ve sistemin güvenliği tek yönlü fonksiyonun güvenilirliğine bağlıdır. Ayrıca, seçilen gizli anahtarın kısa tutulması sözlük saldırılarına ve iletilen n ve SEED değerleri aldatma saldırılarına maruz kalabilir.

2.6.3. Zaman tabanlı kimlik doğrulama

Günümüzde en yaygın olarak kullanılan yöntemlerden biri olan zaman tabanlı mekanizma, istemci ve sunucu arasında eş zamanlı çalışan bir zaman bilgisi 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. Ayrıca, mekanizma istemciden sunucuya erişme zamanını da göz önünde bulundurarak bir zaman sapma değeri de hesaplamak zorundadır [4,7,9]. Kullanıcıların sisteme ilk kaydı sırasında, TKŞ üretmek amacıyla gereken tüm parametreler her iki tarafta da kayıt altına alınır. Eş zamanlama olarak adlandırılan bu işlem sayesinde, istenilen herhangi bir anda her iki tarafta aynı değere sahip TKŞ üretebilmektedirler. Şekil 2.3' te verilen istemci tarafına ait TKŞ üretim sürecinde, kullanıcının sahip olduğu parametrelerden faydalanılarak bir TKŞ değeri üretilir. Üretilen bu TKŞ değeriyle birlikte, kullanıcının sistemde tanımlı olan kullanıcı adı doğrulama sunucusuna iletilir. Doğrulama sunucusu, gelen giriş talebi içinde yer alan kullanıcı adına göre kendine ait veritabanında sorgulama yapar.

Talepte bulunan kullanıcıya ait parametreleri kullanarak bir TKŞ değeri üretir. Üretilen bu değer, kullanıcının giriş talebiyle birlikte gönderdiği TKŞ ile karşılaştırılır. Bu iki değer eşleşiyorsa kullanıcının kimliği doğrulanır.



Şekil 2.3. Senkron mekanizma işlemleri

- İstemci, kullanıcının gizli anahtarını ve zaman parametresini kullanarak bir şifre üretir ve PIN değeri ile birlikte sunucuya iletir,

- Sunucu gelen PIN değeri ile eşleşen kullanıcı gizli anahtarını ve kendi zaman parametresini kullanarak bir şifre üretir,
- Ürettiği bu şifre ile istemciden gelen şifre değerini karşılaştırır ve sonucu istemciye iletir.

F. Aloul, S. Zahidi, W. El-Hajj zaman tabanlı kimlik doğrulama yaptıkları çalışmalarında cep telefonunu kullanarak çok faktörlü kimlik doğrulaması yapmışlardır. Çalışmalarının temel amacı token adı verilen ve tek kullanımlık şifre üreten donanımsal bir cihaz yerine, çok yaygın bir şekilde kullanılan cep telefonların tek kullanımlık şifre üretilmesinde kullanılmasıdır. Bu şekilde kullanıcılar pahalı donanımlar olan bu cihazlar yerine cep telefonlarının kullanarak hizmet alabilecekleri sistemlere erişirken yapılan kimlik doğrulamasında kullanılan şifrelerini ürettirebileceklerdir. Şifre üretim süreci kullanıcı bilgilerini ve kullanıcının sahip olduğu cep telefonu bilgilerini kapsadığı için bu çalışma çok faktörlü kimlik doğrulama olarak adlandırılmıştır. Üretilen şifrenin tek kullanımlık olabilmesi için zaman bilgisi de bu faktörler arasına dâhil edilmiştir. Zaman bilgisi hem istemci tarafında hem de sunucu tarafında eşzamanlı olarak işlemektedir. Yazarlar, şifre üretme sürecinde bağlantılı ve bağlantısız olmak üzere iki ayrı yöntem uygulamışlardır. Bağlantısız yöntemde cep telefonu bir bağlantı kanalı kurmaksızın şifre üretmekte ve bu şifre aynı şekilde sunucuda da üretilip on dakika boyunca sunucu veritabanında saklanmaktadır. Bu cep telefonunun ürettiği şifrenin on dakika boyunca geçerli olacağı anlamına gelmektedir. Kullanıcı ürettiği bu şifre ile doğrulama sunucusuna on dakikalık bir zaman periyodu içerisinde kendini doğrulatabilmekte ve sahip olduğu hesaba erişip hizmet alabilmektedir [6].

2.6.4. Sayaç tabanlı kimlik doğrulama

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 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 saldırılarında sunucunun çok sayıda hesap yapması gerektiği anlamına gelir [23]. 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 [7-9].

2.7. SHA-1 Özet Fonksiyonu

Lamport, 1981’ de kendi kimlik doğrulama mekanizması olan tek kullanımlık şifre tasarımında tek yönlü hash fonksiyonlarının kullanımını önerdiğinden beri, güvenliği geliştirmek için çeşitli tasarımlar önerilmiştir [14]. Tasarımlarda tek yönlü fonksiyonlardan faydalanılmasının temel sebebi, üretilen şifreden fonksiyona sokulan şifre metninin elde edilememesidir.

Amerika ulusal güvenlik kurumu tarafından tasarlanmış ve ilk olarak 1993 yılında yayınlanmıştır. SHA-0, SHA-1, SHA-256, SHA-384 ve SHA-512 olmak üzere 5 türü vardır. SHA-1 birçok uygulamada yaygın olarak kullanılmaktadır. Bu algoritmaların hepsi yinelemeli hash fonksiyonunu baz alarak oluşturulmuştur. SHA, 160 bit ve daha üzeri mesaj özeti üretir. Uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir. Bu işlem sırasında ilk önce mesajı 512 bitlik bloklara ayırır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar. SHA-1 çalışma prensibi olarak R. Rivest tarafından tasarlanan MD5 özet fonksiyonuna

benzer ve yinelemeli bir yapısı vardır. Her yinelemede bir sıkıştırma fonksiyonu kullanılır. Bu fonksiyon mesajın 512 bitlik bloğunu alır ve 16 bitlik ($m_0, m_1, \dots, m_{15}$) kelimelere çevirir. Daha sonra bu kelimeler $m_i = (m_{i-3} + m_{i-8} + m_{i-14} + m_{i-16})$, $i > 1$ fonksiyonu kullanılarak 2560 bite genişletilir ve her biri 20 fonksiyon içeren 4 tur çalıştırılır, nihayetinde 160 bitlik mesaj özeti elde edilir. Bu çalışmada tek kullanımlık şifre üretim algoritmasında yer alan hash fonksiyonu için SHA-1 tercih edilmiştir.

2.8. Coğrafi Koordinat Sistemi

GPS, düzenli olarak kodlanmış bilgi yollayan bir uydu ağıdır ve uydularla arasındaki mesafeyi ölçerek Dünya üzerindeki kesin konumu tespit etmeyi mümkün kılar. Bu sistem, ABD Savunma Bakanlığı'na ait, yörüngede sürekli olarak dönen uydulardan oluşur. Bu uydular radyo sinyalleri yayarlar ve yeryüzündeki GPS alıcısı bu sinyalleri alarak konum saptamada kullanır. Günümüz akıllı cep telefonlarında gömülü bir sistem olarak yer alan GPS alıcıları, herhangi bir anda dünya çevresinde kendi yörüngelerinde bulunan 24 uydudan en az 4 tanesinin sürekli yaydığı sinyalleri alarak, sinyalin varış zamanına dayanan mesafe kestirimi yapar. Bu mesafe kestirimi sözde mesafe (pseudorange) olarak adlandırılır, çünkü alınan GPS işaretinde hatalar mevcuttur. Günümüzde kullanılan konum belirleme yöntemi, nonlinear sözde mesafe denklemlerini lineerleştirir ve önceden tanımlı başlangıç konum noktasından yararlanarak, iteratif yolla kullanıcı konumunu belirlemeye çalışır. GPS sistemi ile alıcının konumunu belirleme işlemi, dört bilinmeyenli bir denklemi çözmektir. Bu bilinmeyenler, kartezyen konum koordinatları x, y, z ve GPS saat hatasıdır. Bu çözüme ulaşmak için kullanıcı GPS alıcısı en az 4 adet uydunun görüşünde olmalıdır.

Yer bilgisi öncelikle gezi uygulamaları, turistik amaçlı uygulamalarda yaygın olarak kullanılmıştır, fakat günümüzde farklı amaçlara hizmet eden birçok uygulamada kullanılmaktadır. Bu uygulamaların başında coğrafi bilgi sistemleri, turistik amaçlı sistemler, lojistikte kullanılan sistemler gelmektedir [24]. Bu tür uygulamalarda yer bilgisini elde edebilmek için iki farklı yöntemden faydalanılabilir. Bunlar; “Küresel Konumlama Sistemi” ve “GSM Hücre Bilgisi ile Yer Belirleme Sistemi” dir. Bir

mobil cihazda GSM Hücre Bilgisi ile yer belirlendiğinde, cihazın hali hazırda bağlı bulunduğu hücresel sistemlerin özelliklerinden faydalanılır. Ancak küresel konumlama sistemi ile yer belirleme sisteminde dahili veya harici bir GPS cihazından faydalanılır.

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. KKS’ 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 KKS’ ye göre enlem verisi “N” (North), boylam verisi ise “E” (East) harfleriyle başlamaktadır. Çizelge 2.2’ de genel olarak kullanılan üç farklı coğrafi koordinat sayı formatı gösterilmektedir [1]. Bu çalışmada, kullanımı daha basit olduğu için desimal sayı formatı tercih edilmiştir.

Çizelge 2.2. Coğrafi koordinat sayı formatı çizelgesi

Coğ. K. 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.ddddd°	Derece (Desimal Format)*	N 39.940187 E 32.823162
* Tercih edilen coğrafi koordinat sayı formatı		

2.9. Konum Tabanlı Kimlik Doğrulama

Konumsal kimlik doğrulamanın, yaygın olmamakla birlikte son yıllarda, ilgili teknolojilerin gelişmesiyle sonucunda tercih edilmeye başlanmıştır. Kimlik doğrulama işleminde kullanıcının konumunu da dikkate alan bu yaklaşım sayesinde sistem güvenlik seviyesi bir adım ileri taşınmıştır. Yazının devamında konu üzerinde yapılmış olan çalışmalara değinilmiştir.

G. T. Becker, S. C. Lo, D. S. De Lorenzo, P. K. Enge, C. Paar çalışmalarında amaçları çeşitli uygulamaların güvenliğini artırmak olan, küresel boyutta yeni

güvenli bir konumsal doğrulama mekanizmasının güvenlik analizini incelemişler ve kullanılabilirliğini değerlendirmişlerdir. Bu yeni yöntem SAGA(GNSS Uygulamaları için Güvenli Kimlik Doğrulama) olarak adlandırılmıştır. Yazarlar yaptıkları çalışmada iki yaklaşım açıklamışlardır. Birincisi konumsal doğrulama (location verification); örneğin A varlığından B varlığına güvenli bir konumsal doğrulama ile B varlığı t zamanında A varlığının yerinin LA olduğundan emin olabilmektedir. İkincisi kendini doğrulama (location self-verification); örneğin A varlığı t zamanında yerinin LA olduğundan emin olabilmektedir [25]. Yazarlar yaptıkları inceleme sonucunda konumsal doğrulamanın kırılmaz olmadığını, fakat sistemlere yapılacak saldırıları çok zorlaştırdığı için sistemlerin güvenlik seviyesini yükselttiğini belirtmişlerdir. Bu tür sistemlerin güvenlik seviyesini yükseltmesinin ana sebebi, kaybolduğunda güvenlik açığına sebep olan veya saldırganlar tarafından sonradan kullanılabilecek bilgilere dayanmadığı, yazarlar tarafından vurgulanmıştır.

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, RBAC modeli üzerine bir çalışma yapmışlardır [26]. RBAC, 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 [27]. Benzer olarak Damiani ve diğerleri, GEO-RBAC olarak adlandırdıkları çalışmalarında, kullanıcının konumuna göre sistem üzerindeki yetkilerini belirleyen bir yöntem önermişlerdir [28]. Yazarlar 2008 yılında da, GEO-RBAC yönteminin gelişmiş bir versiyonu olan Devamlı GEO-RBAC (GEO-RBACC) yöntemini önermişlerdir. GEO-RBACC yöntemi ile birlikte kullanıcının hareketi sonucu konumunun değişmesine bağlı olarak sistem üzerindeki yetkilerinin de anlık olarak değişebilmesi sağlanmıştır [29].

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 genel anahtar altyapısını kullanmıştır. Ayrıca kullanıcı konumunu belirlemek üzere, GPS yerine Avrupa Galileo programı kapsamında geliştirilen Galileo Local Elements teknolojisini kullanmayı tercih etmiştir [30].

Liao ve Chao, 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 sorunu için belirli bir tolerans mesafesi kullanarak bir çözüm yolu önermişlerdir [31].

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 [32].

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 [33].

A. Durresi, M. Durresi, V. Paruchuri ve L. Barolli çalışmalarında cep telefonlarını kullanarak konumsal kimlik doğrulama yapmışlardır. Günümüz cep telefonlarındaki GPS özelliğini kullanarak iki farklı yaklaşım ile yöntemlerini gerçekleştirmişlerdir. Birinci yaklaşımları konumsal olarak belirli bir konumda yer alan bir sensör

aracılığıyla kullanıcının kimlik doğrulaması yapabilmesidir. Kullanıcı sensörün yer aldığı konumda iken cep telefonundaki yazılım aracılığı ile doğrulama sunucusuna bulunduğu konum bilgisini gönderir. Sunucuda kayıtlı olan kullanıcı bilgileri sayesinde doğrulama sunucusu, konum bilgisini gönderen kullanıcının geçerli bir kullanıcı olduğunu ve geçerli bir konuma ait koordinat bilgisi gönderdiğini doğrular. Rastgele üretmiş olduğu bir doğrulama değerini hücresel altyapıyı kullanarak kullanıcı cep telefonuna gönderir. Kullanıcı bu değeri sensöre okutmak suretiyle kimlik doğrulamasını yapmış olur. Yazarların bu konu ile ilgili olarak önermiş oldukları ikinci yaklaşım ise belirli bir konumdan değil web üzerinden alınan bir hizmet için kimlik doğrulaması yapılmasıdır. Bu yaklaşımda kullanıcı hizmeti alabilmesi için uygun bir konuma geldikten sonra hem hücresel altyapıya hem de doğrulama sunucusuna konum bilgisini gönderir. Hücresel altyapı aldığı bu konum bilgisini doğrulama sunucusuna iletir. Doğrulama sunucusu hem kullanıcıdan hem de hücresel altyapıdan aldığı konum bilgisini karşılaştır. Konum bilgisi uygun olarak değerlendirilmesi durumunda hücresel altyapı üzerinden rastgele üretmiş olduğu doğrulama değerini kullanıcı cep telefonuna gönderir. Kullanıcı cep telefonuna gelen bu değeri doğrudan doğrulama sunucusuna ileterek kimlik doğrulamasını yapmış olur [34].

3. RASTLANTISAL DEĞİŞKEN TABANLI KONUMSAL KİMLİK DOĞRULAMA TASARIMI

Bu çalışma ile sunulan tasarımda, her kullanıcı için ilk kayıt sürecinin Genel Anahtar Altyapısı sistemini kullanan güvenli bir kanal üzerinden tamamlandığı varsayılmaktadır [35]. İlk kayıt sürecinden sonra kullanıcı kendi cep telefonuna kurduğu bir istemci yazılımı aracılığıyla Tek Kullanımlık Şifre üretebilecektir. TKŞ üretiminde, her bir kullanıcı için farklı olup değişkenlik göstermeyen faktörlerin yanı sıra, kullanıcının hareketine bağlı olarak değişen konum verisi ve her giriş işleminden sonra farklı değerlere sahip olan İstemci ve Sunucu Değişkenleri kullanılmaktadır. TKŞ üretiminde kullanılan tüm faktörler Çizelge 3.1’ de verilmiştir.

Çizelge 3.1. TKŞ üretiminde kullanılan faktörler

Faktörler	Açıklama	Örnek
KullanıcıAdı	Kullanıcının sistemde tanımlı olan adı	muhammed
PIN	PIN verisi	tk4test.
IMEI	Uluslararası Mobil Cihaz Kodu	123456789012345
IMSI	Uluslararası Mobil Abone Kodu	123456789012345
İstemci Değ.	İstemci tarafından üretilen rastlantısal kod	b12l6
Sunucu Değ.	Sunucu tarafından üretilen rastlantısal kod	s6e7a
K	X, Y değerlerine sahip kullanıcı konum verisi	(39,940000 / 32,823000)

Kullanıcı cep telefonuna ait IMEI ve IMSI değerleri sabit kalmakla beraber, kullanıcı adı ve PIN değerleri isteğe bağlı olarak güncellenebilmektedir. İstemci ve sunucu değişkenlerinin değerleri kullanıcının yaptığı her başarılı giriş sonrasında arka planda otomatik olarak değişeceklerdir. K, kullanıcının konum verisi olup kullanıcının hareketine bağlı olarak değişkenlik göstermektedir.

PIN değeri, sadece geçerli kullanıcının doğru İstemci TKŞ üretebilmesi için kullanılan bir parametredir. İstemci yazılımı doğru PIN değerinin girilip girilmediğini kontrol etmeksizin bir İstemci TKŞ değeri üretecektir. Şayet, yanlış bir PIN değeri girilmişse, üretilen İstemci TKŞ’ de yanlış olacak ve kullanıcının kendini sunucu yazılımına doğrulaması mümkün olmayacaktır. Bu şekilde, geçerli

kullanıcıdan başka herhangi birinin, geçerli bir TKŞ üretebilmesinin önüne geçilmiştir. Kullanıcı adı ile PIN sadece geçerli kullanıcının sahip olduğu verilerdir. Bu veriler asla mobil telefonun hafızasında depolanmaz. Sadece TKŞ üretmek için kullanılırlar ve daha sonra derhal silinirler. PIN değerinin, tahmin edilmesini zorlaştırmak amacıyla içinde nümerik karakterleri ve noktalama işaretlerini de barındıran, en az sekiz karakterden oluşması önerilmektedir.

İstemci değişkeni, TKŞ' lerin her bir başarılı giriş işlemi için farklı bir değere sahip olabilmesi için kullanılan bir koddur. Bu kodun her bir karakteri sıralı olmak üzere üretilen geçerli şifrenin içerisine rastlantısal bir dağılımla eklenir. Sunucu yazılımı hem şifreyi doğrulayabilmek hem de bu kodu ayırt edebilmek için kullanıcının girmiş olduğu İstemci TKŞ içerisinde kendi üretmiş olduğu geçerli şifrenin, sıralı olmak koşuluyla, her bir karakterini arar. Geçerli şifrenin her bir karakteri, İstemci TKŞ içerisinde sıralı olarak yer alıyorsa, kullanıcının kimlik doğrulaması yapılır ve geriye kalan karakterler yeni istemci değişkeni olarak bir sonraki şifre üretiminde kullanılmak üzere veritabanına kaydedilir. İstemci yazılımı da aynı şekilde, rastlantısal olarak yalnızca kendinin değer atayabildiği bu değişkeni bir sonraki şifre üretiminde kullanmak amacıyla hafızasında saklayacaktır. İstemci değişkeninin karakter uzunluğu, rastlantısal olarak değişmektedir. Karakter sayısının alt sınırı üç, üst sınırı da beş olarak belirlenmiştir. Buradaki amaç mümkün olduğu kadar kullanışlı ve esnek bir şifre oluşturabilmektir. Bu kodun uzunluğunun değişmesi nihai İstemci TKŞ uzunluğunu da etkileyecektir. Bu da üretilen TKŞ' leri saldırılara karşı daha dayanıklı hale getirmektedir.

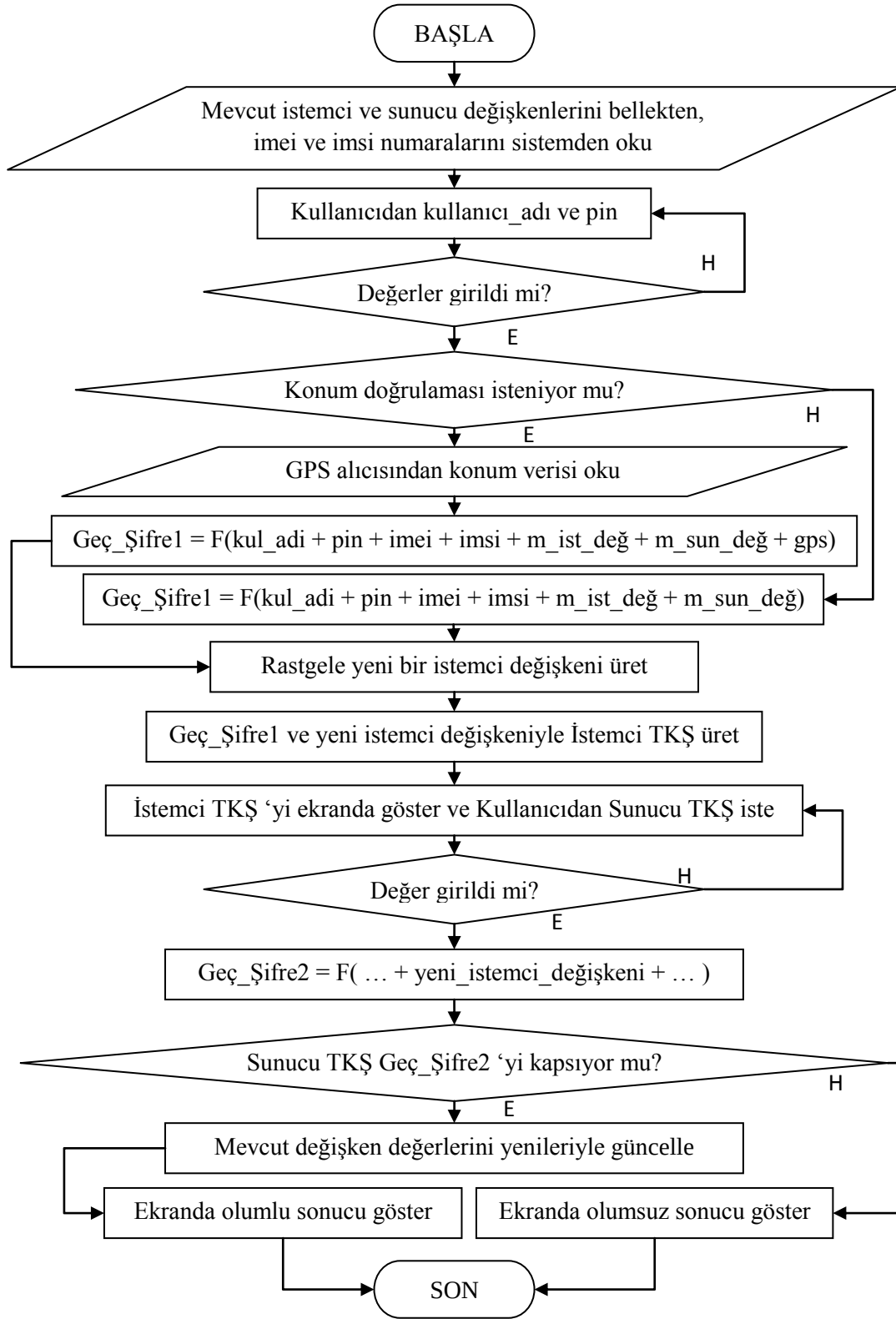
Sunucu değişkeni de TKŞ' lerin her bir başarılı giriş işlemi için farklı bir değere sahip olabilmesi için kullanılan bir koddur. Bu kod istemci değişkeni ile birlikte bir sonraki şifre üretim sürecine sokulmaktadır. Bu amaçla bu değişken hem istemci yazılımı hem de sunucu yazılımı tarafından saklanmaktadır. İstemci değişkeni ile birlikte kullanılarak üretilen TKŞ' lerin eşsiz olmalarını garanti eder. Sunucu değişkeninin değerini yalnızca sunucu yazılımı değiştirebilir, istemci yazılımı hiçbir şekilde bu değişkene değer atayamaz. Karakter uzunluğu rastlantısal olarak değişmekle birlikte, alt sınırı üç, üst sınırı da beş olarak belirlenmiştir.

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 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 KKS' ye göre enlem verisi "N" (North), boylam verisi ise "E" (East) harfleriyle başlamaktadır. Çizelge 2.2' de genel olarak kullanılan üç farklı coğrafi koordinat sayı formatı gösterilmektedir. Bu çalışmada, kullanımı daha basit olduğu için desimal sayı formatı tercih edilmiştir.

Tasarımda konumsal kimlik doğrulama tercihi kullanıcıya bırakılmıştır. Kayıt sürecinden sonra üretilen ilk TKŞ herhangi bir konuma bağlı değildir. Bu ilk TKŞ ile sisteme kendini tanıtan kullanıcı, isterse doğrulama sunucusu tarafından sağlanan ekranlar üzerinden konumsal doğrulama seçeneğini aktif hale getirebilmektedir. Aynı ekranlar üzerinden, giriş yaparken bulunması gereken konumları belirleyip, sisteme kaydedebilmektedir. Kayıtlı konum verileri üzerinde ekleme ve çıkarma işlemleri yapabilmektedir. İstemci yazılımında da, kullanıcıya bulunduğu konuma bağlı olarak İstemci TKŞ üretmek isteyip istemediği sorulmaktadır.

3.1. Tasarımın Detayları

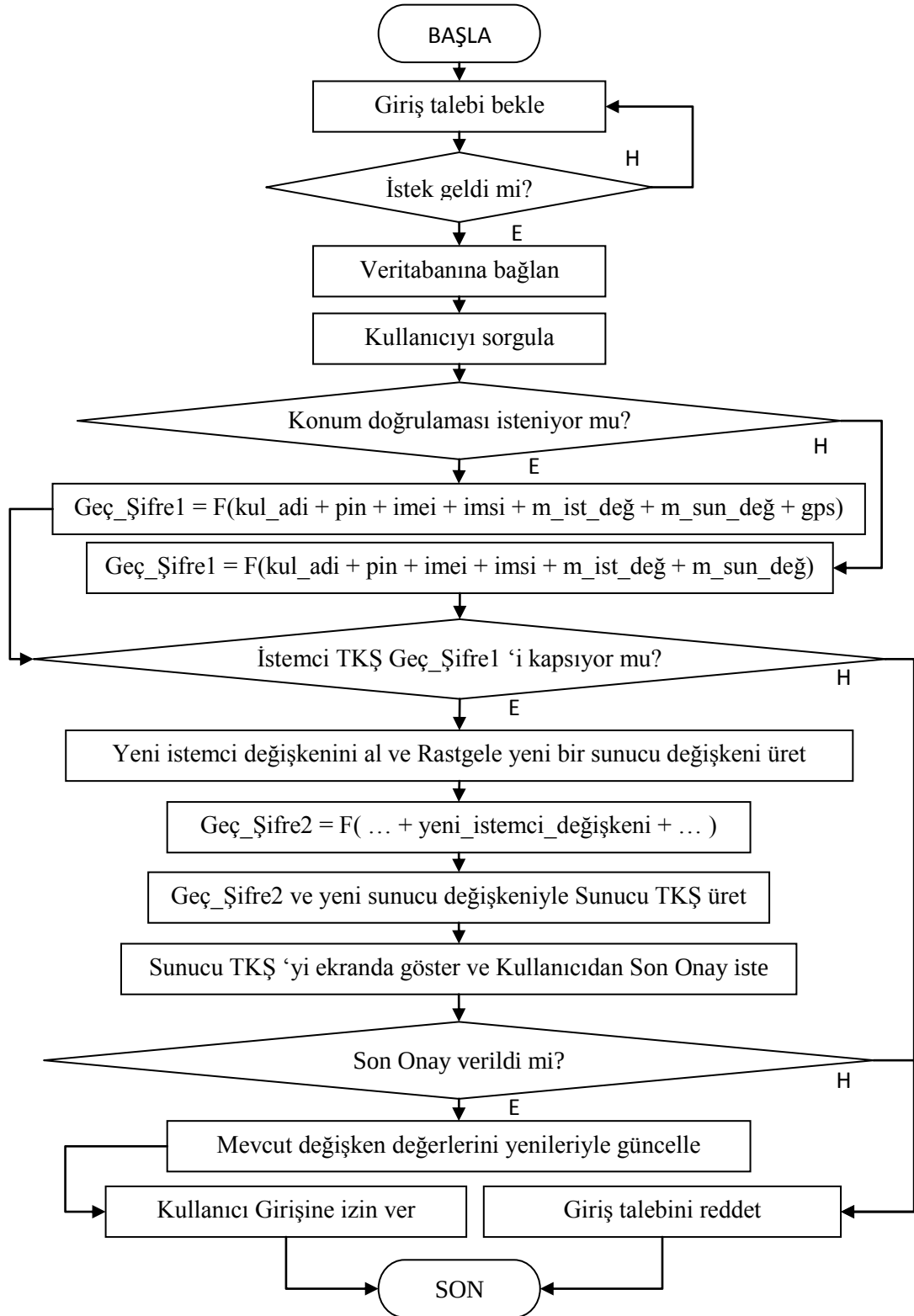
Bu çalışmada, genel kabul görmüş TKŞ üretim yöntemlerine alternatif olarak, rastlantısal değerlere bağlı yeni bir yaklaşım geliştirilmiştir. Bu yaklaşımda, hem istemci hem de sunucu yazılımının ürettiği rastlantısal birer değişken çifti ile TKŞ üretilmesi sağlanmıştır. Değişkenler üretildikleri kaynağa göre isimlendirilmiştir. Bu yöntem de kullanıcıdan, yazılımı cep telefonuna ilk kez kurup çalıştırdığında, telefon ve sunucu üzerinde kayıtlı başlangıç değerlerine sahip istemci ve sunucu değişkenleri ile ilk TKŞ' yi üretmesi istenmektedir. Şekil 3.1' de verilen süreç izlenerek, üretilen bu ilk İstemci TKŞ ile birlikte, tasarımın amaçları arasında yer alan değişken değerlerinin rastlantısal değerlere sahip olmaları garanti altına alınmıştır.



Şekil 3.1. İstemci yazılımı için kimlik doğrulama süreci

Şekil 3.1’ de görüldüğü üzere, istemci yazılımı geçerli şifre içine eklenecek yeni istemci değişkenini, rastlantısal bir yöntem kullanarak üretir. Bu değer, bir sonraki şifre üretim sürecinde kullanılacak olup, üretilen geçerli şifre içine rastlantısal olarak eklenir. Daha sonra üretilen TKŞ kullanıcının görebilmesi için cep telefonu ekranına yansıtılır. Kullanıcı bu İstemci TKŞ’ yi kullanarak sisteme giriş yaptıktan sonra sunucu yazılımının benzer şekilde üretmiş olduğu Sunucu TKŞ ile karşılaşır. Bu Sunucu TKŞ’ de aynı İstemci TKŞ’ de olduğu gibi geçerli bir şifre ve bir sonraki şifre üretiminde kullanılacak rastlantısal sunucu değişkeni değerini içermektedir. Kullanıcı bu şifreyi, cep telefonu üzerinde hali hazırda çalışmakta olan istemci yazılımına girer. İstemci yazılımı, girilen bu Sunucu TKŞ kodunu doğrular. Doğrulama başarılı ise Sunucu TKŞ’ nin içerdiği rastlantısal sunucu değişkeni ve sürecin başında üretilen rastlantısal istemci değişkeni, kaydedilerek süreç başarıyla sonuçlandırılır. Doğrulama başarısız ise, istemci yazılımı süreci iptal eder ve daha önceki istemci ve sunucu değişken değerlerini korur. Bu yöntem sayesinde hem kullanıcı hem de hizmet veren uygulama sunucusunun doğrulanması karşılıklı olarak gerçekleştirilmiştir. Sonuç olarak, geçerli kullanıcı hesabının bulunduğu gerçek sisteme kimliğini doğrulamıştır.

Şekil 3.2’ de ise karşılıklı kimlik doğrulama sürecinin, doğrulama sunucusu tarafında gerçekleştirilen işlem adımları gösterilmiştir.



Şekil 3.2. Doğrulama sunucusu yazılımı için kimlik doğrulama süreci

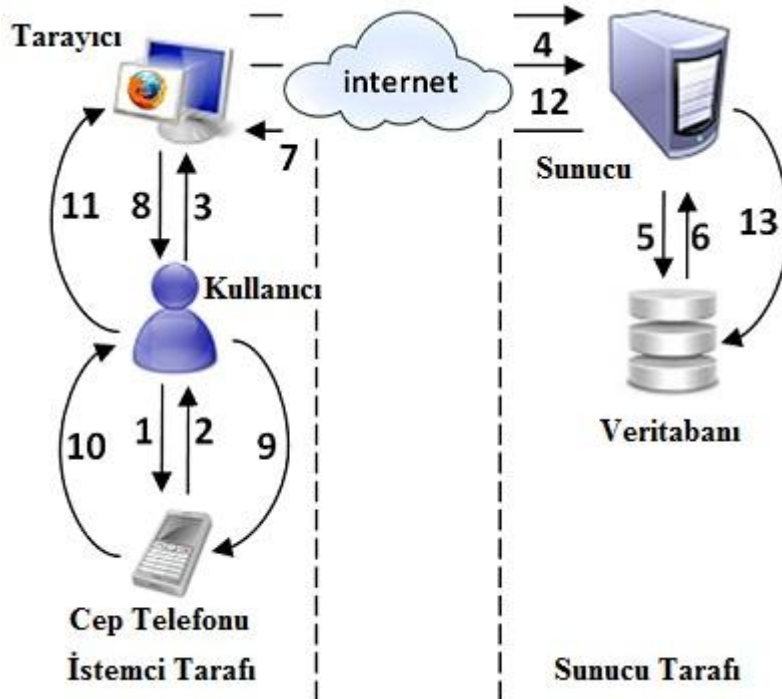
Doğrulama sunucusu tarafında, sisteme yapılmak istenen her bir giriş isteği için, kullanıcı adı ve İstemci TKŞ parametreleri kullanılmaktadır. Doğrulama sunucusu, kullanıcı adı parametresi ile eşleşen kullanıcıyı bulabilmek için mevcut kullanıcılar arasında bir arama yapar. İstek var olan bir kullanıcıdan geliyorsa o kullanıcıya ait bilgiler kullanılarak geçerli şifre üretilir. Şekil 3.2’ de görüldüğü üzere, kullanıcının girmiş olduğu İstemci TKŞ içerisinde bu değer aranır. Çünkü İstemci TKŞ rastlantısal bir dizilimle hem geçerli şifre hem de rastlantısal yeni istemci değişkenini içermektedir. Doğrulama sunucusu bu İstemci TKŞ’ nin kendi üretmiş olduğu geçerli şifreyi içerip içermediğini kontrol eder. Şifre değerleri eşleşiyorsa kullanıcının kimliği doğrulanmış olur ve mevcut İstemci TKŞ içerisinde yer alan yeni istemci değişkenini kullanıcıdan gelecek olan en son onay ile birlikte kaydetmek üzere geçici hafızaya alınır. Doğrulanmış İstemci TKŞ sonrası sunucu yazılımı bir sonraki şifre üretim sürecinde kullanılacak olan sunucu değişkeni için rastgele yeni bir değer üretir. Üretilen bu yeni sunucu değişken değeri, az önce elde edilen yeni istemci değişkeniyle, sistemde var olan mevcut sunucu değişkeni kullanılarak üretilen geçerli şifre içerisine rastlantısal olarak eklenir. Sunucu TKŞ olarak adlandırılan bu TKŞ, kullanıcı giriş ekranından bir sonraki ekranda kullanıcıdan bu değeri cep telefonuna girmesini isteyen bir uyarı mesajı ile birlikte görüntülenir. Kullanıcı bu değeri istemci yazılımına girdiğinde, sunucu yazılımı üzerinde gerçekleşen doğrulama adımları istemci yazılımı üzerinde de işletilir. Sunucu TKŞ’ nin doğrulanması sonucunda, her iki rastlantısal değişken de yeni değerler alır ve bu durum sürecin başarıyla tamamlandığını içeren bir mesaj ile birlikte cep telefonu ekranına yansıtılır. Kullanıcı, doğrulamanın yapılp, değişkenlerin güncellendiğini web tarayıcısı üzerinden sunucu yazılımına iletir. Bu şekilde hem doğrulama sunucu yazılımı hem de istemci yazılımı, kullanıcıdan gelecek bir sonraki bağlantı isteğinde doğrulama yapabilmek için üreteceği TKŞ için kullanacakları rastgele istemci ve sunucu değişkenlerini güncellemiş olacaklardır.

Karşılıklı üretilen şifreler, tek kullanımlık oldukları ve hangi karakterlerin geçerli şifreye hangi karakterlerin rastlantısal değişkenlere ait olduğu bilinemediği için, üçüncü kişilerin eline geçmesi durumunda gerek kullanıcı için gerek sistem için herhangi bir probleme yol açmayacaktır. Ayrıca bu yöntem ile kullanıcıya doğrulama

sunucusu ve cep telefonu yazılımına şifre girişi dışında, fazladan hiçbir işlem yükü getirilmemektedir.

3.2. Kimlik Doğrulama Süreci

Bu çalışma ile sunulan kimlik doğrulama süreci, hem hizmet sunan sistemler için kullanıcı kimlik doğrulamayı hem de kullanıcılar için hizmet aldıkları sistemleri doğrulama amacı ile geliştirilmiştir. Bu karşılıklı doğrulama süreci ile geçerli bir kullanıcının gerçek sisteme giriş yapması garanti altına alınır. Kimlik doğrulama süreci istemci tarafında; İstemci TKŞ üretimi, Sunucu TKŞ doğrulaması ve sonucun karşı tarafa iletilmesi ile birlikte toplam üç aşamadan oluşur. Doğrulama sunucusu tarafında da; İstemci TKŞ' nin sınanması, Sunucu TKŞ üretimi ve karşıdan gelen onay ile süreci sonlandırma olmak üzere üç aşamadan oluşur. Şekil 3.3' te bu aşamalar ve sürecin detaylı adımları açıklamaları ile birlikte verilmiştir.



Şekil 3.3. Kimlik doğrulama sürecinde gerçekleştirilen adımlar

İstemci Tarafı 1. Aşama

1. Kullanıcı, Kullanıcı Adı ve PIN ile istemci yazılımına giriş yapar. Bu işlemin amacı kimlik doğrulamak değildir. İstemci yazılımı girilen Kullanıcı Adı ve PIN ne olursa olsun bir TKŞ üretecektir. Geçerli TKŞ sadece doğru değerler girildiği sürece üretilebilecektir.
2. Cep Telefonu ekranında İstemci TKŞ görüntülenir.
3. Kullanıcı herhangi bir web tarayıcı üzerinden eriştiği doğrulama sunucusu giriş ekranına Kullanıcı Adı ve İstemci TKŞ değerini girer.
4. Giriş isteği sunucuya iletilir.

Sunucu Tarafı 1. Aşama

5. Sunucu kullanıcı bilgilerini sorgulamak üzere veritabanına bağlanır.
6. Veritabanı geçerli kullanıcı bilgilerini doğrulama sunucusuna verir. Sunucusu bu bilgiler ile geçerli şifreyi üreterek kimlik doğrulaması yapar.

Sunucu Tarafı 2. Aşama

7. Kimlik doğrulama başarılı ise sunucu bir Sunucu TKŞ değeri üreterek bunu karşı tarafa gösterir ve kaydedildi bilgisini kullanıcıdan ister.

İstemci Tarafı 2. Aşama

8. Kullanıcı, Sunucu TKŞ değerini ekrandan okur.
9. Bu kod kullanıcı tarafından istemci yazılımına girilir.
10. İstemci yazılımı kodu doğrular. Doğrulama başarılı ise yeni istemci ve sunucu değişkenini hafızaya kaydeder ve kaydedildi bilgisini ekranında görüntüler.

İstemci Tarafı 3. Aşama

11. Kullanıcı, kaydedildi bilgisini tarayıcı üzerinden onaylar.
12. Kaydedildi bilgisi doğrulama sunucusuna iletilir.

Sunucu Tarafı 3. Aşama

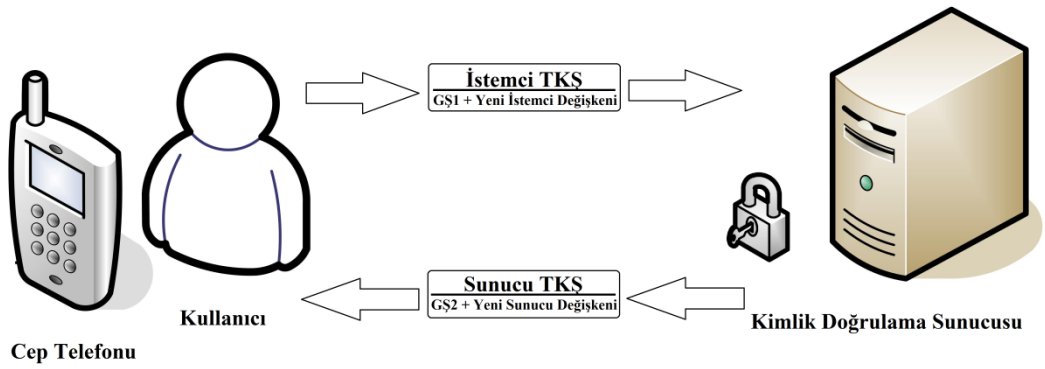
13. Sunucu, istemci yazılımının yaptığı gibi ilgili kullanıcı için istemci ve sunucu değişkeni değerlerini yenileri ile günceller.

Sürecin altıncı aşamasında, şayet ilgili kullanıcı için konumsal doğrulama yapılması aktif durumdaysa, sunucu yazılımı, her bir geçerli konum için bir geçerli şifre üretir ve kullanıcının girdiği İstemci TKŞ değeri ile karşılaştırır. Ürettiği geçerli şifre değerlerinden herhangi biri İstemci TKŞ içinde ile yer alıyorsa, kullanıcı doğrulaması gerçekleşir. Aksi halde, giriş isteği reddedilir. Daha öncede belirtildiği gibi, kullanıcı tarafından daha önce belirlenmiş olan muhtemel konum bölgelerinin her biri için sunucu tarafında bir geçerli şifre değeri üretilir. Çünkü doğrulama sunucusu kullanıcının konumunu bilmemektedir. Bu nedenle, muhtemel tüm geçerli bölgeleri dener. İstemci TKŞ değerinin doğrulanmasının ardından, aynı konum dikkate alınarak bu kez de Sunucu TKŞ değeri üretilir. Kullanıcı bulunduğu konumu değiştirmeden önce bu Sunucu TKŞ' yi istemci yazılımına doğrulatması gerekmektedir. Aksi takdirde süreç başarısız bir şekilde sonlanır.

3.3. Cep Telefonu ve Doğrulama Sunucusu Arasındaki Şifre İletişimi

Kullanıcı, hesabına erişmek istediğinde cep telefonuna yüklediği yazılım aracılığıyla üretmiş olduğu İstemci TKŞ değerini doğrulama sunucu yazılımının giriş ekranı üzerinden sunucuya iletir. Kullanıcının girmiş olduğu şifre geçerli ise doğrulama sunucu yazılımı üretmiş olduğu Sunucu TKŞ değeri giriş ekranından sonra kullanıcıya gösterilen onay ekranı üzerinden kullanıcıya iletilir. Kullanıcı da bu Sunucu TKŞ değerini cep telefonu yazılımına girer. Cep telefonu yazılımı bu değeri, doğrulama sunucu yazılımının yaptığı gibi geçerlilik kontrolüne sokar. Sunucu TKŞ değerinin geçerli olup olmadığı cep telefonu ekranında gösterilir. Bu şekilde, hem kimlik doğrulama süreci bitmekte hem de sunucunun hizmet alınacak olan geçerli sunucu olduğu doğrulanmaktadır. Şekil 3.4' te iki taraf arasında değiş tokuş edilen TKŞ ve içerikleri gösterilmektedir. Her bir doğrulama döngüsü için, İstemci TKŞ; o an için geçerli olan şifre (GŞ1) ve yeni istemci değişkeni değerinin rastlantısal bir

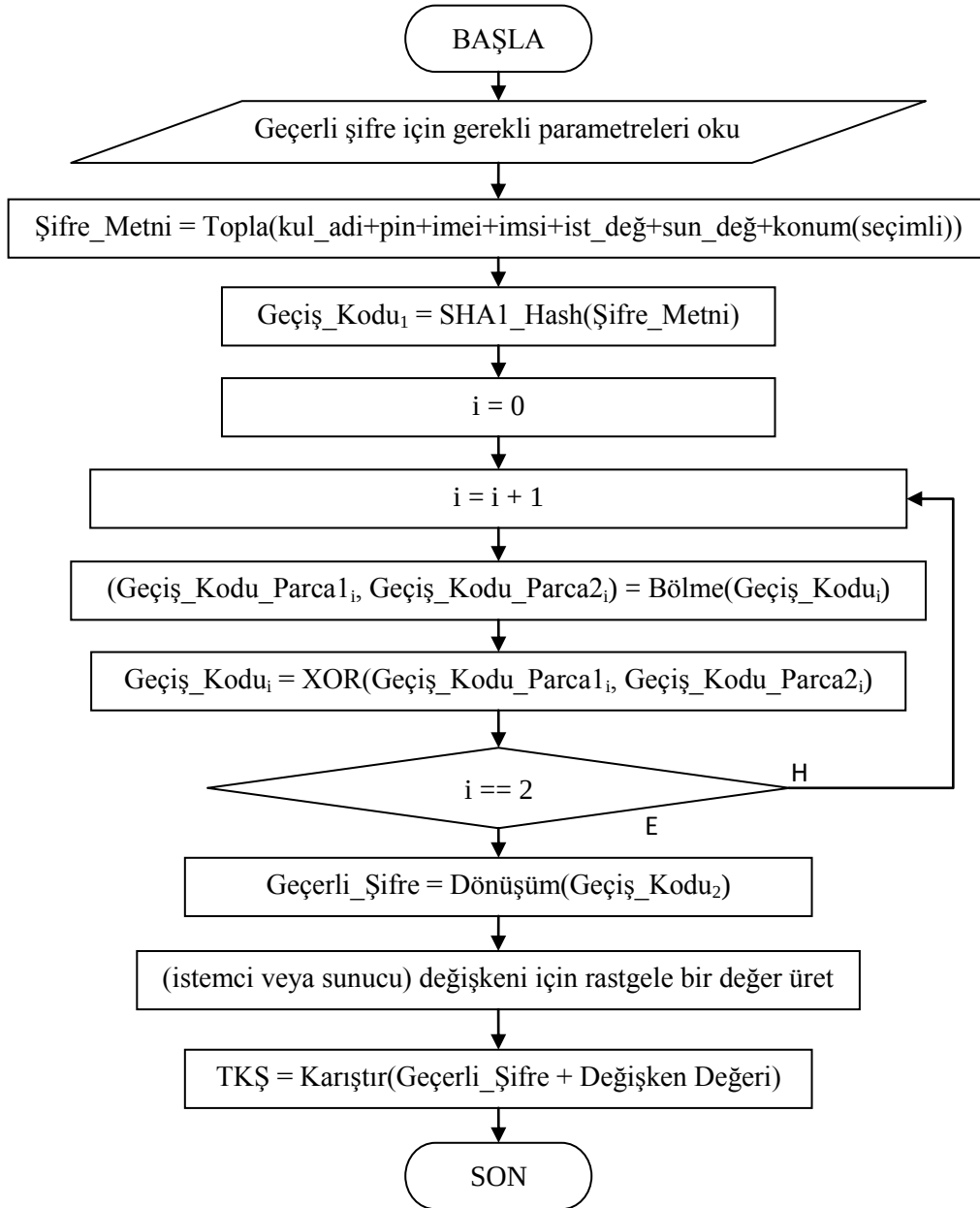
dizilimini, Sunucu TKŞ ise; o an için geçerli şifre (GŞ2) ve yeni sunucu değişkeni değerinin rastlantısal bir dizilimini içermektedirler. Hem istemci hem de sunucu tek kullanımlık şifrelerinde yer alan geçerli şifreler birbirlerinden farklı ve bağımsızdırlar. Şekil 3.4' te gösterilen doğrulama döngüsünün tam bir turu, geçerli bir kullanıcının sistem üzerinde, kimliğinin doğrulandığı anlamına gelir. Döngü bu haliyle, her bir kimlik doğrulaması için bir kez işletilen, sonsuz bir karaktere sahiptir.



Şekil 3.4. Taraflar arasındaki TKŞ değiş tokuş döngüsü

3.4. Tek Kullanımlık Şifre Üretim Süreci

Tek kullanımlık şifre üretim algoritması, her iki tarafta da Çizelge 3.1' de listelenen parametreleri kullanarak geçerli şifre üretmektedir. Bu şekilde üretilen geçerli şifreler aynı değerlere sahip olmakta ve karşılıklı doğrulamayı mümkün hale getirmektedir. Şekil 3.5' te algoritmanın parametreleri ve işlem adımları gösterilmiştir.



Şekil 3.5. Tek kullanımlık şifre algoritması

Şekil 3.5’ te verilen TKŞ algoritmasında da gösterildiği üzere kullanıcı hesabının bulunduğu sisteme giriş yapmak istediğinde, cep telefonu üzerinde kurulu olan yazılımı başlatır. Açılış sayfasından sonra, kullanıcı adı ve PIN değerleri ile konumsal doğrulama yapıp yapılmayacağını seçimi kullanıcıdan istenir. İstemci yazılımı, konumsal doğrulama seçimine göre cep telefonu donanımında gömülü olan GPS alıcılarından, mevcut konum koordinat verilerinin alınmasına gerek olup olmadığına karar verir. Bu nedenle, koordinat verilerinin algoritmaya parametre

olarak verilir verilmeyeceği kullanıcı seçimine bağlıdır. IMEI ve IMSI değerleri ise cep telefonu sistem kaynaklarından elde edilir. İstemci ve sunucu değişken değerleri ise cep telefonu hafızasında tutulan bir dosya üzerinden okunmak suretiyle elde edilirler. Tüm bu parametreler Çizelge 3.2’ de listelenen operatörler arasında bulunan Toplama operatörüne sokularak kullanıcı ve o anki giriş için eşsiz bir değere sahip olan Şifre Metni elde edilir. Çizelge 3.3’ te gösterilen Eş. 3.1’ de bu işlem ve devamında yer alan diğer işlemlerin matematiksel ifadesi gösterilmektedir.

Çizelge 3.2. Tek kullanımlık şifre algoritmasında yer alan işlem operatörleri

Operatörler	Açıklama
$h()$	Tek yönlü SHA-1 hash operatörü
$\oplus$	XOR operatörü
$+$	String toplama operatörü
$b()$	String bölme operatörü
$l()$	String uzunluk ölçme operatörü
$d()$	Dönüştürme operatörü

Çizelge 3.3. Tek kullanımlık şifre algoritmasının matematiksel ifadesi

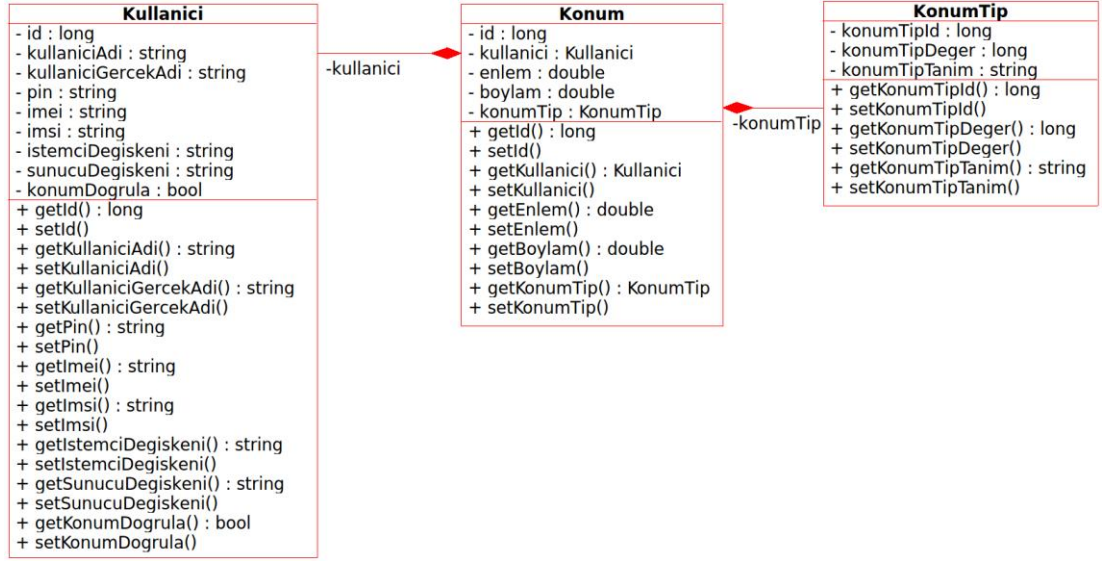
Şifre Metni	= kullanıcı adı+PIN+IMEI+IMSI+istemci değişkeni+sunucu değişkeni+ X_1+Y_1	
GeçişKodu1	= $h(\text{Şifre Metni})$	
$l\text{GeçişKodu1}$	= $l(\text{GeçişKodu1}) / 2$	
XOR_{1a}	= $b_{\text{GeçişKodu1}}(0, l\text{GeçişKodu1})$	
XOR_{1b}	= $b_{\text{GeçişKodu1}}(l\text{GeçişKodu1} + 1, l(\text{GeçişKodu1}))$	
GeçişKodu2	= $\text{XOR}_{1a} \oplus \text{XOR}_{1b}$	(3.1)
$l\text{GeçişKodu2}$	= $l(\text{GeçişKodu2}) / 2$	
XOR_{2a}	= $b_{\text{GeçişKodu2}}(0, l\text{GeçişKodu2})$	
XOR_{2b}	= $b_{\text{GeçişKodu2}}(l\text{GeçişKodu2} + 1, l(\text{GeçişKodu2}))$	
GeçŞifreKodu	= $\text{XOR}_{2a} \oplus \text{XOR}_{2b}$	
GeçŞifreMetni	= $d(\text{GeçŞifreKodu})$	

Toplama operatörü, sırasıyla tüm bu parametreleri birleştirir ve yapılmak istenen Giriş işlemi için eşsiz bir değer olan Şifre Metnini üretir. Bu Şifre Metni, güvenli SHA-1 hash operatörüne parametre olarak verilir. Çıkan sonuç kırk karakter uzunluğunda onaltılık sayı düzeninde 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 ilk önce onluk sayı düzenine ardından da nihai hali olan Geçerli Şifre Metnine çevrilir. Dönüşüm için, $[a, b, \dots, z]$ ve $[0, 1, \dots, 9]$ karakter setlerinden sırayla birer karakter alınarak oluşturulmuş $[a, 0, b, 1, \dots, 3, y, 4, z, 5]$ karakter dizisinden faydalanılır. Onluk düzene çevrilmiş Geçerli Şifre Kodu sayı dizisi ikişerli gruplara ayrılır ve her bir grupta yer alan iki basamaklı sayı için karakter dizisinin toplam uzunluğu olan 52 sayısına göre modüler değeri hesaplanır. Çıkan sonuç karakter dizisinde indis değeri olarak kullanılır ve karşılığındaki karakter nihai Geçerli Şifre' yi oluşturmak üzere kaydedilir. Tüm gruplar üzerinde aynı işlem uygulandığında istenilen Geçerli Şifre elde edilmiş olur.

3.5. Geliştirilen Kimlik Doğrulama Sunucusu Yazılımı Sınıf Yapısı

Doğrulama sunucusu için geliştirilen yazılım temel olarak üç varlık nesnesinden oluşmaktadır. Bunlar, Şekil 3.6' da gösterildiği üzere, her bir kullanıcıyı temsil eden Kullanıcı nesnesi, kullanıcıların oluşturduğu her bir geçerli konumu temsil eden Konum nesnesi ve her bir konum nesnesinin tipini temsil eden KonumTip nesnesidir. Tasarıma ait veritabanı da benzer bir şekilde sınıflarla aynı adlara sahip tablolardan oluşmaktadır. Nesneler arasındaki ilişki; bir kullanıcı birçok konuma sahip olabilir ve birçok konum bir konum tipine sahip olabilir şeklindedir. Tersten gidilecek olursa; bir konum tipinden birçok konum varlığı olabilir ve birçok konum tek bir kullanıcıya ait olabilir şeklindedir.



Şekil 3.6. Doğrulama sunucu yazılımı için sınıf yapısı

Tasarımda, kullanıcılar için konum belirleme amacıyla örnek dört adet konum tipi tanımlanmıştır. Bu konum tipleri Çizelge 3.4’ te gösterildiği üzere her konumun harita üzerinde kapladığı alanı belirtmektedir.

Çizelge 3.4. Tasarımda yer alan örnek konum tipleri ve açıklamaları

Konum Tipi	Virgülden sonra	Örnek bir bölge (Enlem/Boylam)
Birim Bölge	Üç basamak	(39,940000/32,823000), (39,940999/32,823999)
Dar Bölge	İki basamak	(39,940000/32,820000), (39,949999/32,829999)
Orta Bölge	Bir basamak	(39,900000/32,800000), (39,999999/32,899999)
Geniş Bölge	Sıfır basamak	(39,000000/32,000000), (39,999999/32,999999)

Kullanıcı konumunu noktasal olarak TKŞ üretim sürecine sokmak çeşitli sakıncalara sebep olmaktadır. Başlıca sebep, kendini doğrulatmak isteyen bir kullanıcının belirlenen noktaya tam olarak konumlanmasının gerekliliğidir. Bu aşırı hassasiyet gerektirdiği için günlük kullanıma uygun değildir. Bu hassasiyeti gidermek ve işlemi daha kullanıcı dostu hale getirebilmek için kullanıcı konumunun noktasal olarak değil, bölgesel olarak belirlenmesi benimsenmiştir. Bu şekilde kullanıcı belirlediği bölge sınırları içinde olduğu sürece belli bir toleransla TKŞ üretebilecektir. Çizelge 3.4’ te gösterildiği üzere dört adet bölge tipi mevcuttur. Bu bölge tipleri, benzer şekilde kullanıcı için kolaylık sağlama amacına yönelik olarak tasarıma eklenmiştir. Kullanıcı doğrulama sunucusunun sağlamış olduğu bir ekran üzerinden bu tiplere

uygun olarak geçerli bölgeler ekleyebilmektedir. Birim bölge, Şekil 3.7' de görüldüğü üzere yaklaşık olarak $\sim 8500\text{m}^2$ ($\sim 100\text{m} \times \sim 85\text{m}$) civarında belirlenmiş en küçük bölge tipini temsil etmektedir.



Şekil 3.7. Örnek geçerli bir birim bölge gösterimi

Kullanıcılardan gelebilecek talepler göz önünde bulundurulduğunda daha az çabayla daha geniş bölgeler belirleyebilmek amacıyla Dar, Orta ve Geniş bölge tipleri de tasarıma eklenmiştir. Sırasıyla Dar, Orta ve Geniş bölgeler, Birim bölgenin on, yüz ve bin katı büyüklüğündedir. Bu şekilde kullanıcı daha az çabayla geçerli şifre üretebileceği alanları belirleyebilecektir.

Bölgeler tiplerine göre, enlem ve boylam koordinat verilerinin virgülden sonraki, Birim bölge için üç basamağı, Dar bölge için iki basamağı, Orta bölge için bir basamağı, göz önüne alınarak TKŞ üretimine sokulur. Geniş bölge içinse virgülden sonraki basamaklar göz ardı edilerek TKŞ üretimi gerçekleştirilecektir. Yani, KB (39,940999 / 32,823000), GB (39,940000 / 32,823000), GD (39,940000 / 32,823999), KD (39,940999 / 32,823999) bölgesini kapsayan bir Birim bölge sadece (39,940000 / 32,823000) noktasıyla temsil edilmektedir. Örneğin, kullanıcı konum koordinatları (39,940365 / 32,823147) olsun. Kullanıcı da bu noktayı kapsayan, bir Birim bölge tanımlasın. İstemci yazılımı GPS alıcısından okuduğu bu değeri

(39,940000 / 32,823000) değerine dönüştürecek ve doğrulama sunucusu da ilgili kullanıcı için geçerli tüm bölgeleri deneyerek doğrulama işlemini gerçekleştirecektir.

3.6. Tasarımın Grafıksel Kullanıcı Arayüzleri

Kayıt evresini tamamlamış bir kullanıcı için gerçekleştirilen bir kimlik doğrulama örneđi ile birlikte tasarımda yer alan istemci ve doğrulama sunucusu yazılımlarına ait kullanıcı arayüzleri tanıtılacaktır. Kayıt evresini tamamlamış ve ilk İstemci TKŞ değeriyle birlikte kendini sisteme doğrulamış olan kullanıcı, sunucu ekranları üzerinden kendine ait geçerli bölgeleri de sisteme kaydetmiştir. Bu şekilde istediđi takdirde konumsal doğrulama seçeneđini aktif hale getirerek doğrulamada konum verisinin de kullanılmasını sağlayabilme imkânına sahiptir.

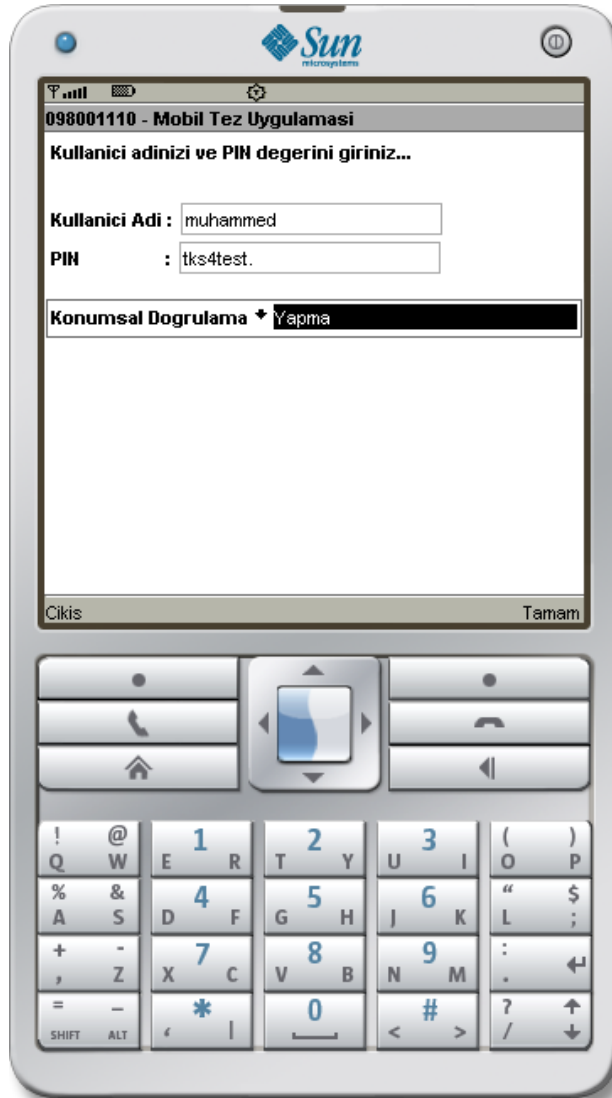
3.6.1. İstemci TKŞ üretim süreci

Geçerli kullanıcı, hizmet aldığı sisteme Giriş yapmak istediđinde ilk olarak cep telefonu üzerinde yüklü olan istemci yazılımını başlatması gerekmektedir. Şekil 3.8’ de verildiđi gibi kullanıcı bir açılış ekranı ile karşılanır.



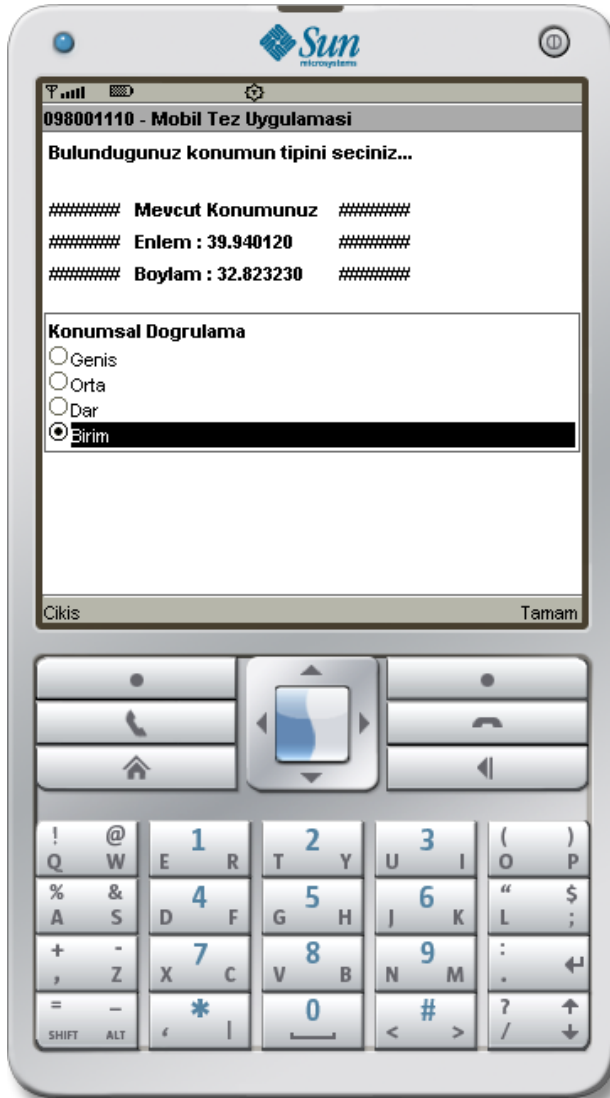
Şekil 3.8. İstemci yazılımı açılış ekranı

Açılış sayfasında yer alan menüde İptal ve Devam seçenekleri mevcuttur. Kullanıcı eğer TKŞ üretmekten vazgeçerse İptal seçeneği ile uygulamaya son verebilmektedir. Devam seçeneği ile TKŞ üretim süreci başlamış olur. Bir sonraki sayfada kullanıcıdan TKŞ için gerekli parametreler arasında yer alan KullanıcıAdı ve PIN değerleri ile birlikte kullanıcıdan konumsal doğrulama yapmak isteyip istemediği bilgileri talep edilir. Şekil 3.9’ da gösterildiği üzere KullanıcıAdı ve PIN değerlerini giren kullanıcı bir seçmeli menü kutusu yardımıyla konumsal doğrulama yapmak isteyip istemediğini yazılıma bildirebilmektedir.



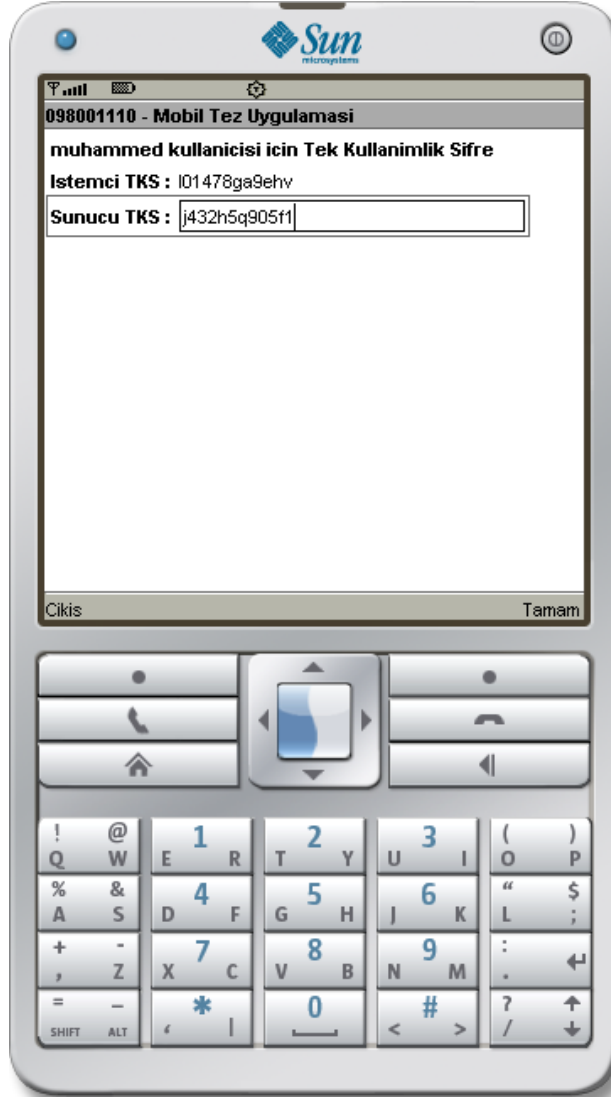
Şekil 3.9. İstemci yazılımı parametre giriş ekranı

Eğer kullanıcı konumsal doğrulama yapmayı seçerse, istemci yazılımı, kullanıcının o anki mevcut konumunun enlem ve boylam değerlerini gösterdiği ekran ile birlikte kullanıcıdan bulunduğu konumun tipini seçmesini talep eder. Şekil 3.10’ da görüldüğü üzere kullanıcı bulunduğu konumu daha önce doğrulama sunucu sistemine tanıtırken belirttiği konum tipini seçer.



Şekil 3.10. İstemci yazılımı konum tipi seçim ekranı

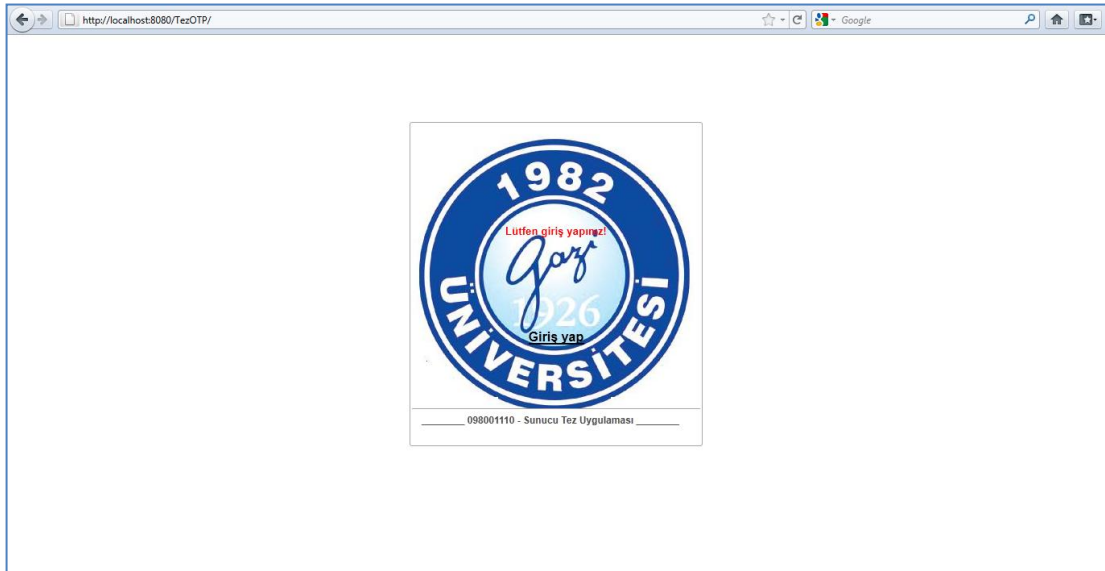
Konum tipini işaretleyip Tamam seçeneğine tıklayan veya parametreleri girdiği bir önceki ekranda konumsal doğrulama yapma seçeneği ile Tamam seçeneğini tıklayan kullanıcı, İstemci TKŞ değerinin görüntülediği ekrana yönlendirilir. Şekil 3.11’ de gösterildiği üzere bu ekranda ayrıca Sunucu TKŞ değeri de istemci yazılımı tarafından talep edilmektedir.



Şekil 3.11. İstemci TKŞ değeri gösterimi ve sunucu TKŞ giriş talebi

3.6.2. Sunucu TKŞ üretim süreci

Kullanıcı bu safhada geçici olarak istemci yazılımı ile olan işini tamamlamıştır. Hizmet aldığı sunucuya giriş yapmak amacıyla herhangi bir web tarayıcı üzerinden doğrulama sunucusuna bir istek gönderir. Bu istek Şekil 3.12’ de görülen doğrulama sunucusu açılış sayfası ile cevaplanır. Bu sayfa Giriş sayfasına yönlendirilmiş bir link bağlantıya sahiptir. Giriş yapmak istediğini belirten kullanıcı bu link vasıtasıyla Giriş sayfasına yönlendirilir.



Şekil 3.12. Doğrulama sunucusu açılış sayfası

Giriş sayfası olabildiğince yalın bir yapıdadır ve sadece kullanıcıdan KullanıcıAdı ve İstemci TKŞ değeri talep edilir. Şekil 3.13’ te gösterildiği üzere, bu iki değeri ilgili alanlara giren kullanıcı Giriş Yap butonunu kullanarak isteği sunucuya iletir. Sunucu gelen isteği değerlendirmeye ilk önce geçerli kullanıcılar arasında bu isme sahip olan bir kullanıcı olup olmadığını tarayarak başlar. KullanıcıAdı geçerli bir kullanıcıda bulunursa ilgili kullanıcının verileri kullanılarak istemci yazılımının yaptığı gibi bir geçerli şifre üretilir ve İstemci TKŞ değeri içinde aranır. Şayet kullanıcı hesabında konumsal doğrulama aktif ise kullanıcıya ait her bir konum için ayrı ayrı geçerli şifreler üretilir ve İstemci TKŞ değeri içinde aranır.

The screenshot shows a web browser window with the address bar displaying 'http://localhost:8080/TezOTP/'. The main content area contains a login panel titled 'Giriş Paneli'. Inside this panel, there is a sub-section titled 'Giriş'. It contains two input fields: 'Kullanıcı Adı : *' with the value 'muhammed' and 'İstemci TKŞ : *' with the value '101478ga9ehv'. Below these fields is a blue button labeled 'Giriş Yap' with a checkmark icon.

Şekil 3.13. Doğrulama sunucusu giriş sayfası

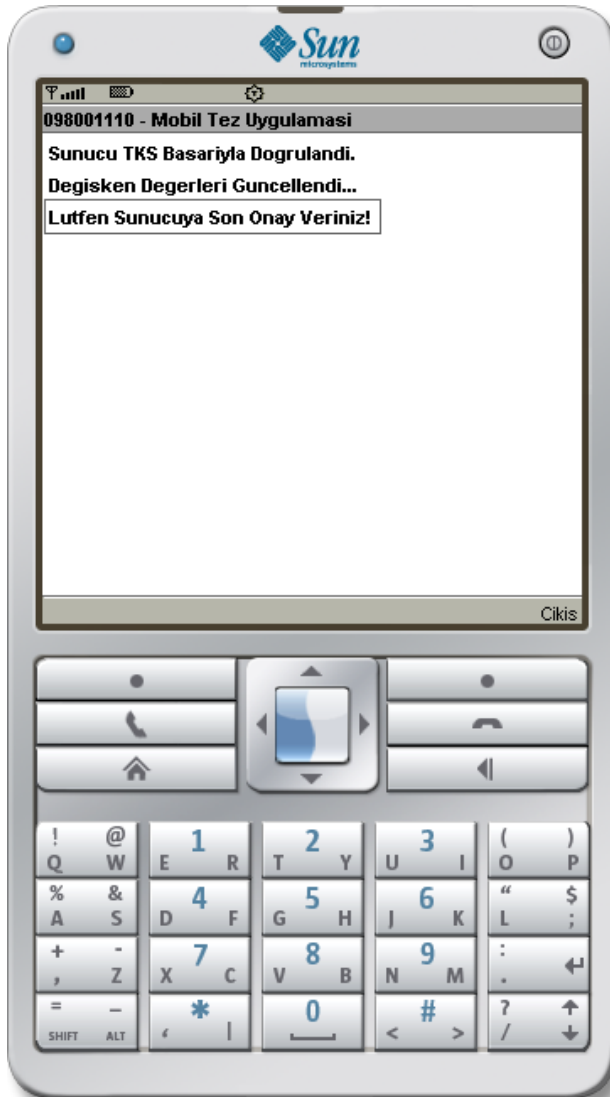
Geçerli şifre veya şifrelerden herhangi biri, İstemci TKŞ içinde yer alıyorsa, kullanıcı girişi kabul edilir. Aksi takdirde bir uyarı mesajı ile birlikte giriş isteği reddedilecektir. Girişi kabul gören kullanıcı Şekil 3.14’ te gösterildiği üzere Sunucu TKŞ değerini içeren bir sayfaya yönlendirilir. Bu sayfada, Sunucu TKŞ değerini istemci yazılımına girmesini isteyen bir uyarı ile birlikte Sunucu TKŞ değeri gösterilmektedir.

The screenshot shows a web browser window with the address bar displaying 'http://localhost:8080/TezOTP/'. The main content area features a large image of a building at sunset. Overlaid on the image is a box titled 'Sunucu Tek Kullanımlık Şifre' containing the token 'j432h5q905f1'. Below the token are two buttons: 'Son Onay' and 'İptal'. At the bottom of the page, there is a text prompt: 'Lütfen bu değeri cep telefonunuza giriniz...'. In the top right corner, there is a notification bubble that says 'Başarılı Giriş', 'Muhammed Özsoy', and 'Hoşgeldiniz...'.

Şekil 3.14. Sunucu TKŞ gösterim sayfası

3.6.3. Son onay süreci

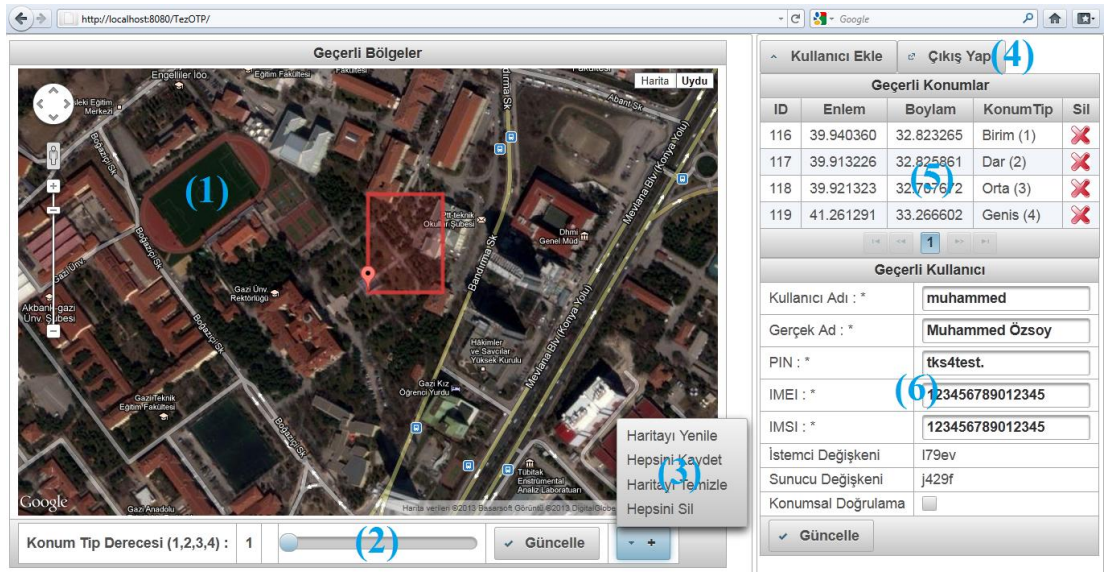
Sayfadan Sunucu TKŞ değerini okuyan kullanıcı hali hazırda açık olan istemci yazılımına Şekil 3.11’ de görüldüğü üzere bu değeri girer. Girilen değer benzer bir sınamadan geçirilerek karşı tarafın gerçek sistem olup olmadığı tespit edilir. Sunucu TKŞ sınaması başarılı ise Şekil 3.15’ te görüldüğü üzere, istemci yazılımı tarafından olumlu bir cevap ekranı kullanıcıya gösterilir. Olumlu sonucu gören kullanıcı son onay için Şekil 3.14’ te gösterilen Son Onay butonunu kullanarak doğrulama sürecini tamamlar.



Şekil 3.15. İstemci yazılımı sunucu TKŞ doğrulama sonuç ekranı

3.6.4. Geçerli bölgeleri ve kişisel bilgileri güncelleme sayfası

Doğrulama sürecini başarıyla tamamlayan kullanıcılar istedikleri takdirde, kişisel bilgilerini ve konumsal doğrulama için gerekli geçerli bölgeleri güncelleyebilecektir. Bu işlemleri, doğrulama sunucusunun sağlamış olduğu Şekil 3.16’ da gösterilen ekran üzerinden gerçekleştirebileceklerdir.



Şekil 3.16. Geçerli bölgeleri ve kişisel bilgileri güncelleme sayfası

Şekil üzerinde (1) olarak işaretlenmiş bölümde yer alan harita, kullanıcının geçerli bölgelerini görebilmesini ve yeni geçerli bölge ekleyebilmesini sağlamaktadır. Etkileşimli bu harita arayüzü sayesinde kullanıcılar kolaylıkla geçerli bölgelerini görebilmekte ve yeni bölgeler tanımlayabilmektedir. Şekilde (2) olarak işaretlenmiş bölümde yer alan kaydırma çubuğu aracılığıyla eklenecek olan yeni geçerli bölgelerin tipleri seçilebilecektir. Bölge tipleri için 1 Birim bölgeyi, 2 Dar bölgeyi, 3 Orta bölgeyi ve 4 ise Geniş bölgeyi temsil etmektedir. Şekilde (3) olarak işaretlenmiş bölümde yer alan menüde, harita üzerinde gerçekleştirilebilecek dört adet işlem tanımlanmıştır. Bunlar sırasıyla, “Haritayı Yenile” adıyla haritayı temizledikten sonra ilgili kullanıcı için kayıtlı olan tüm bölgeleri harita üzerine yansıtmaya, “Hepsini Kaydet” adıyla o an için harita üzerine işaretlenmiş tüm bölgeleri kalıcı olarak kaydetmeye, “Haritayı Temizle” adıyla harita üzerindeki tüm çizimleri silme, “Hepsini

Sil” adıyla kullanıcıya ait tüm geçerli bölgeleri kalıcı olarak silme işlemlerinden oluşmaktadır. Şekilde (4) olarak işaretlenmiş bölümde yer alan “Çıkış Yap” adlı butonla kullanıcı mevcut oturumuna son verebilmektedir. Sistemden sorumlu yönetici kullanıcılar için gözükür durumda olan “Kullanıcı Ekle” butonu ile Şekil 3.17’ de gösterildiği gibi sisteme yeni kullanıcı kayıtları yapılabilen ve sistemdeki tüm kullanıcılar listelenebilmektedir. Şekilde (5) olarak işaretlenmiş bölümde yer alan veri tablosunda, ilgili kullanıcıya ait o an için geçerli tüm bölgelerin bir listesi sunulmaktadır. Bu liste ile kullanıcı geçerli bölgelerini görebilmekte, istediği bir bölgeyi seçerek haritada merkez konuma getirebilmekte ve isteği herhangi bir konumu kolayca silebilmektedir. Şekilde (6) olarak işaretlenmiş bölümde yer alan kullanıcı kişisel bilgileri arasında KullanıcıAdı, PIN, IMEI ve IMSI numaraları yer almaktadır. Kullanıcı istediği takdirde bu değerleri güncelleyebilir. Bu değerleri güncellediği andan itibaren istemci yazılımına bu yeni değerleri girmesi gerekmektedir. Kullanıcının cep telefonunu değiştirmesi gerektiği durumda, ilk olarak sisteme kendini tanıtmalı, ardından istemci yazılımını taşıdığı yeni telefonuna ait IMEI ve IMSI numaralarını sistemde güncellemesi gerekmektedir. Ayrıca kullanıcı, bu bölümde yer alan konumsal doğrulama tik seçimini işaretleyerek, bir sonraki giriş işlemini konumsal doğrulama ile birlikte yapabilmektedir.

Kullanıcı Kayıt

Kullanıcı Adı : *

Kullanıcı Gerçek Adı : *

PIN : *

IMEI : *

IMSI : *

Konumsal Doğrulama : ☐

ID	Kullanıcı Adı	Kullanıcı Gerçek Adı	PIN	IMEI	IMSI	Konumsal Doğrulama	Sil
1	muhammed	Muhammed Özsoy	tk4test.	123456789012345	123456789012345	Hayır	☒
6	mustafa	Mustafa Burunkaya	12asd357	444444444444444	111111111111111	Hayır	☒
7	ayhan	Ayhan Erdem	789852	777777777777777	555555555555555	Hayır	☒
8	huseyin	Huseyin Polat	ab12cd.	333333333333333	999999999999999	Hayır	☒

Şekil 3.17. Doğrulama sunucusu yeni kullanıcı ekleme sayfası

Sistem yöneticileri için geliştirilen kullanıcı ekleme ve listeleme sayfası, doğrulama sunucusu için geliştirilen son sayfadır. Şekilde (1) olarak işaretlenmiş bölümde yer alan panel üzerinden yeni kullanıcı kaydı yapılabilmektedir. Şekilde (2) olarak işaretlenmiş bölümde yer alan veri tablosu sistem üzerinde kayıtlı olan geçerli kullanıcı listesini vermektedir. Bu liste üzerinde bulunan silme işlemi ile istenilen kullanıcı sistem üzerinden kalıcı olarak silinebilmektedir. Şekilde (3) olarak işaretlenmiş yerdeki “Geri” buton ile kullanıcı bir önceki sayfaya yönlendirilir.

Tanıtilan bu sayfalar, hizmet sağlayıcısının sadece kullanıcı doğrulama işlevini yerine getirecek şekilde tasarlanmıştır. Bu yazılımı geliştirmekteki temel hedef, gerçekleştirilen kimlik doğrulama tasarımının gerçek bir örnek üzerinde test edilebilmesidir.

3.7. Kimlik Doğrulama Sürecinde Gerçekleşen İşlem Çıktıları

Bu bölümde örnek bir kimlik doğrulama süreci boyunca arka planda gerçekleştirilen işlemlere ait çıktıları yer verilmiştir. İşlemler, konumsal kimlik doğrulamanın aktif ve pasif olduğu durumlar için gerçekleştirilmiştir. Geçerli bir kullanıcı sisteme kendini doğrulatmak amacıyla cep telefonuna kurulu durumda olan istemci yazılımını başlattığında yazılım ilk olarak hafızasında kayıt olan mevcut istemci ve sunucu değişken değerlerini okur. Parametre olarak kullanıcı tarafından girilen KullanıcıAdı ve PIN değerleri ile birlikte İstemci TKŞ hesaplama süreci başlar. Bu aşamada gerçekleştirilen işlem adımlarına ait çıktılar Çizelge 3.5’ te listelenmiştir.

Çizelge 3.5. İstemci TKŞ hesaplama işlemleri çıktıları

İşlem	Açıklama	İşlem Çıktısı
Topl.	Şifre Metni	muhammedtks4test.123456789012345123456789012345b12l6s6e7a
SHA-1	Hash Fonk.	31660c5b8afa251937dc460fece943567644f8c3
XOR	XOR Fonk.	(31660c...dc $\oplus$ 460fec...c3) = 7769e0b2c9ac535dcf1f
XOR	XOR Fonk.	(7769e0b2c9 $\oplus$ ac535dcf1f) = db3abd7dd6
Hx2Ds	Dönüştürme	d(db3abd7dd6) = 0148gah (geçerli şifre)
Rast	Rastgele	l79ev(yeni istemci değişkeni)
Sonuç	İstemci TKŞ	l01478ga9ehv

İstemci TKŞ değerini üreten yazılım bunu cep telefonu ekranında gösterir ve Sunucu TKŞ değerini beklemeye başlar. Giriş sayfasına, KullanıcıAdı ile birlikte İstemci TKŞ değerinin girilmesinin ardından doğrulama sunucusu üzerinde gerçekleştirilen işlemlere ait çıktılar Çizelge 3.6’ da ve Çizelge 3.7’ de verilmiştir. İstemci TKŞ’ nin doğrulanması amacıyla üretilen geçerli şifre hesaplaması istemci yazılımı ile aynı olduğu için çizelgede tekrar edilmemiştir.

Çizelge 3.6. İstemci TKŞ doğrulama işlemleri çıktıları

İşlem	Açıklama	İşlem Çıktısı
Parametre	İstemci TKŞ	l01478ga9ehv
Geç. Şif. Üret	Geçerli Şifre	0148gah
Karşılaştı	İ. TKŞ Doğ.	l01478ga9ehv (doğrulama başarılı)
İ. Değ. Al	İ. Değişkeni	l79ev (yeni istemci değişkeni)

İstemci TKŞ değeri ile ürettiği geçerli şifreyi karşılaştıran doğrulama sunucusu hem doğrulama işlemini gerçekleştirmekte hem de yeni istemci değişkeninin değerini elde etmektedir. Geçerli şifrenin her bir karakterini İstemci TKŞ içinde eşleştiren sunucu yazılımı kullanıcı girişini kabul eder ve Sunucu TKŞ değerini üretir.

Çizelge 3.7. Sunucu TKŞ hesaplama işlemleri çıktıları

İşlem	Açıklama	İşlem Çıktısı
Gç. Şif.	Geçerli Şifre	0148gah
Sonuç	İ. TKŞ Doğ.	l01478ga9ehv (doğrulama başarılı)
İ. Değ.	İ. Değişkeni	l79ev
Topl.	Şifre Metni	muhammedtks4test.123456789012345123456789012345l79evs6e7a
SHA-1	Hash Fonk.	b5feb9eab32b9214365e6f35a69b87cad4b3521b
XOR	XOR Fonk.	(b5feb9...5e $\oplus$ 6f35a6...1b) = dacb1f7134e146a76445
XOR	XOR Fonk.	(dacb1f7134 $\oplus$ e146a76445) = 3b8db81571
Hx2Ds	Dönüştürme	d(3b8db81571) = 3h5q051 (geçerli şifre)
Rast	Rastgele	j429f (yeni sunucu değişkeni)
Sonuç	Sunucu TKŞ	j432h5q905f1

Son onay sayfasında gösterilen Sunucu TKŞ değeri kullanıcı tarafından istemci yazılımına girildiğinde gerçekleştirilen işlemlere ait çıktılar Çizelge 3.8’ de verilmiştir. Sunucu TKŞ doğrulama amacıyla üretilen geçerli şifre hesaplaması doğrulama sunucu yazılımı ile aynı olduğu için çizelgede tekrar edilmemiştir.

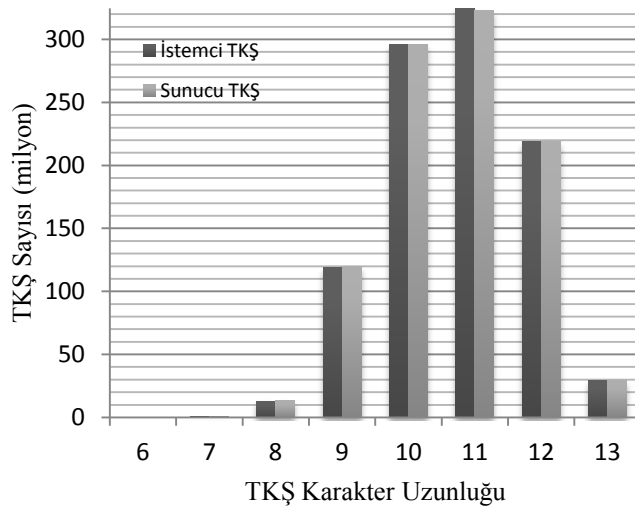
Çizelge 3.8. Sunucu TKŞ doğrulama işlemleri çıktıları

İşlem	Açıklama	İşlem Çıktısı
Parametre	Sunucu TKŞ	j432h5q905f1
Geç. Şif. Üret	Geçerli Şifre	3h5q051
Karşılaştır	S. TKŞ Doğ.	j432h5q905f1 (doğrulama başarılı)
S. Değ. Al	S. Değişkeni	j429f (yeni sunucu değişkeni)

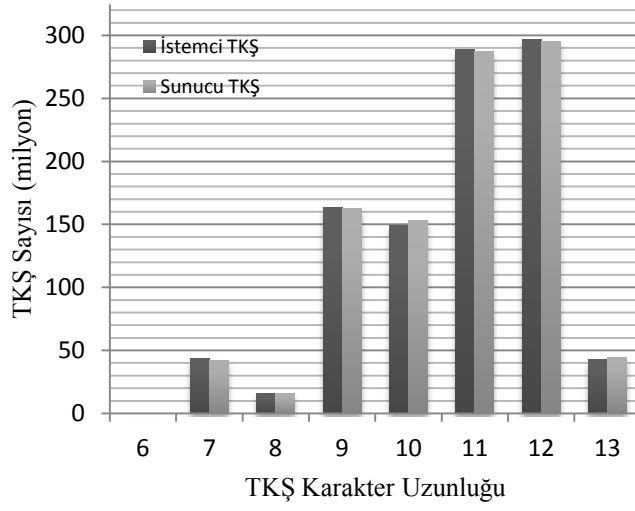
Sunucu TKŞ değerini doğrulayan istemci yazılımı hem istemci hem de sunucu değişken değerlerini günceller ve aynı işlemin sunucu tarafında da yapılması için cep telefonu ekranında bir uyarı mesajı görüntüler.

4. ÖNERİLEN TASARIMIN GÜVENİLİRLİK VE ETKİNLİK TESTLERİ

Çalışmanın temel hedefleri arasında yer alan güvenilirliğin sağlanabilmesi için, algoritma tasarımında rastlantısallık yöntemi kullanılmıştır. Şifre üretiminde rastlantısallıktan faydalandığı gibi üretilen TKŞ'lerin karakter sayılarının da rastlantısal olarak değişmesi sağlanmıştır. Şifrelerin karakter uzunluklarının değişimini gözlemlemek amacıyla Şekil 3.4' deki kimlik doğrulama döngüsü farklı zaman dilimlerini kapsayacak şekilde birer milyar kez işletilerek, iki ayrı örneklem kümesi oluşturulmuştur. Karakter uzunluklarına göre üretilen şifre sayılarını içeren bu kümeler Şekil 4.1 ve Şekil 4.2' de grafiksel olarak gösterilmiştir.

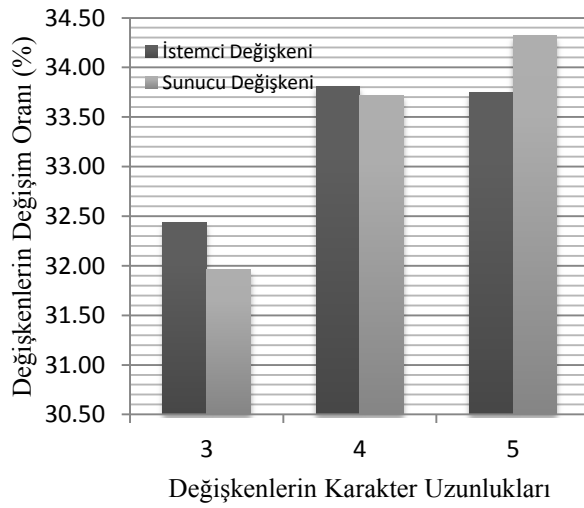


Şekil 4.1. Birinci örneklem kümesi için karakter uzunluklarına göre TKŞ sayıları

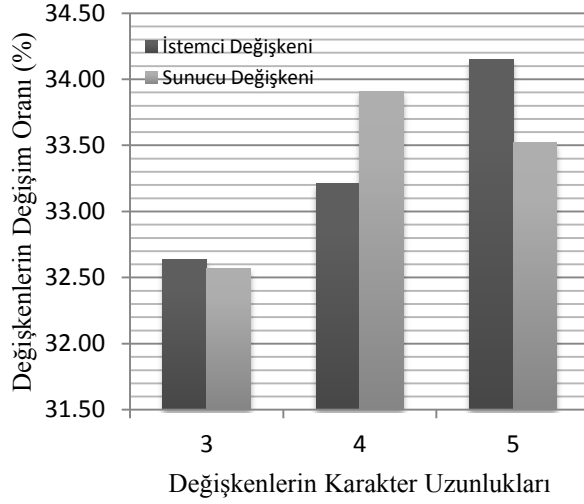


Şekil 4.2. İkinci örneklem kümesi için karakter uzunluklarına göre TKŞ sayıları

Şekil 4.3 ve Şekil 4.4’ teki grafiklerde ise ilgili örneklem kümesini oluşturan TKŞ değerleri için kullanılan istemci ve sunucu değişkenlerinin test süreci boyunca karakter sayılarına göre değişim oranları verilmiştir.



Şekil 4.3. Birinci örneklem kümesi için istemci ve sunucu değişkenlerinin karakter sayılarına göre değişim oranı grafiği



Şekil 4.4. İkinci örneklem kümesi için istemci ve sunucu değişkenlerinin karakter sayılarına göre değişim oranı grafiği

Şekil 4.1 ve Şekil 4.2’ de yer alan grafikler göz önüne alındığında, test süreçleri boyunca üretilen TKŞ’ lerin karakter sayılarına göre farklı dağılımlar gösterdiği görülmektedir. Bu duruma sebep olarak, algoritmanın en güçlü özelliğinden biri olan rastlantısallık gösterilebilir. Benzer olarak, Şekil 4.3 ve Şekil 4.4’ te de karakter sayısı, izin verilen aralıkta, rastlantısal olarak değişen ve üretilen TKŞ’ nin karakter sayısını etkileyen, istemci ve sunucu değişkenlerinin test süreçleri boyunca farklı dağılımlar gösterdiği görülmektedir. Bu grafiklerden anlaşılabileceği üzere, sıradaki TKŞ’ nin karakter sayısının ne olacağını tahmin etmek imkânsıza yakındır.

Kimlik doğrulama işlemi, tasarım gereği doğrulama sunucusu kullanıcıyı, kullanıcı da doğrulama sunucusunu doğrulamak suretiyle karşılıklı olarak yapılmaktadır. Hem cep telefonu hem de sunucu uygulaması ürettikleri her şifre içine bir sonraki şifre üretiminde kullanacakları, istemci ve sunucu değişkenleri olarak adlandırılan rastlantısal kodlar yerleştirilmektedir. Bu kodlar geçerli şifre içine sıralamada değişikliğe uğramadan geliş güzel eklenmektedir. Örneğin Çizelge 4.1’ de test ortamında gerçekleştirilen doğrulamaya ait İstemci TKŞ ve geçerli şifre karşılaştırması verilmiştir.

Çizelge 4.1. İstemci TKŞ ile geçerli şifre eşleştirme ve istemci değişkenini elde etme

Açıklama	Karşılaştırma İşlem Çıktısı
İstemci TKŞ	1 0 1 4 7 8 g a 9 e h v
Geçerli Şifre	0 1 4 8 g a h
Yeni İstemci Değişkeni	1 7 9 e v

Sunucu üretmiş olduğu geçerli şifrenin, sırasıyla her bir karakterini kullanıcının girmiş olduğu İstemci TKŞ karakteri ile karşılaştırmaktadır. Şayet geçerli şifrenin tüm karakterleri İstemci TKŞ karakterleri ile eşleşirse kullanıcıyı doğrulamakta ve eşleşmeyen diğer karakterleri bir sonraki şifre üretiminde kullanmak üzere kaydetmektedir. Kullanıcının girişi kabul edildikten sonra aynı aşamalar bu kez sunucu doğrulaması yapılmak üzere tersten işletilir. Sunucu doğrulama yaparken elde ettiği en son istemci değişkenini ve sahip olduğu sunucu değişkenini kullanarak üretmiş olduğu Sunucu TKŞ, cep telefonu yazılımına kullanıcı tarafından girilir. Cep telefonu yazılımı girilen bu Sunucu TKŞ ile üretmiş olduğu geçerli şifreyi Çizelge 4.2’ de görüldüğü gibi karşılaştırarak doğrulama yapar. Sunucu TKŞ, geçerli şifreyi kapsıyorsa, geri kalan kısım bir sonraki şifre üretiminde kullanılmak üzere sunucu değişkeni olarak kaydedilir.

Çizelge 4.2. Sunucu TKŞ ile geçerli şifre eşleştirme ve sunucu değişkenini elde etme

Açıklama	Karşılaştırma İşlem Çıktısı
Sunucu TKŞ	j 4 3 2 h 5 q 9 0 5 f 1
Geçerli Şifre	3 h 5 q 0 5 1
Yeni Sunucu Değişkeni	j 4 2 9 f

Kötü niyetli bir kişinin eline geçen TKŞ’ lerden bir sonraki şifre üretimde kullanılacak olan istemci ve sunucu değişkenlerinin elde edilmesi, bu değerlerin TKŞ içerisine geliş güzel yerleştirilmesi sebebiyle imkânsıza yakındır. Yukarıdaki örneği ele alacak olursak, cep telefonu yazılımı tarafından üretilen TKŞ içerisinde yer alan istemci değişkeninin elde edilmesi olasılığı Çizelge 4.3’ te listelenen parametreler kullanılarak, güvenilirlik sınama formülü olan Eş. 4.1’ deki gibi hesaplanabilir.

$$O_{id}(n,r) = O_{idt} * [n - (r - 1)]^r \quad (4.1)$$

$$O_{idt} = s(ISKK) = 3$$

Çizelge 4.3. Güvenilirlik sınaması parametreleri ve açıklamaları

Parametreler	Açıklama
O_{id}	İstemci değişkeninin elde edilmesi olasılığı,
$ISKK = \{3, 4, 5\}$	İstemci değişkeninin karakter uzunluğu kümesi,
O_{idt}	İstemci değişkeninin karakter uzunluğunun tahmin edilme olasılığı,
n	İstemci TKŞ karakter uzunluğu,
r	İstemci değişkeni değerinin karakter uzunluğu,

Eş. 4.1' de yer alan parametreler ayarlanarak hesaplama yapılacak olursa;

$$O_{id}(12, 5) = 3 * [12 - (5 - 1)]^5$$

$$O_{id}(12, 5) = 98304$$

Benzer olarak sunucu yazılımı tarafından üretilen Sunucu TKŞ içinde yer alan sunucu değişkeninin elde edilmesi olasılığı da hesaplanabilir.

$$O_{sd}(12, 5) = 98304$$

İki değişkeninde elde edilme olasılığı genel çarpma kuralına göre;

$$O(n,r) = n * r$$

$$O(98304, 98304) = 9.663.676.416$$

Bu hesaplamalar ışığı altında yukarıdaki örnek için elde edilen tek kullanımlık şifrelerden hem istemci hem de sunucu değişkeni değerlerinin tahmin yoluyla elde edilme olasılığı;

$$O(n) = 1 / n$$

$$O(n) = 1 / 9.663.676.416$$

$$O(n) = 1.034803 \times 10^{-10}$$

Görüldüğü üzere tek kullanımlık şifrelerden bir sonraki geçerli şifreyi üretmek için kullanılacak olan değerlerden ikisi olan istemci ve sunucu değişkenlerini elde etmek yaklaşık on milyarda bir ihtimalindedir. Bu algoritmanın gücünü kanıtlamakta ve güvenilirliğini artırmaktadır.

Gerçekleştirilen tasarımın sağladığı faydalara ve diğer doğrulama yöntemlerine göre üstünlüklerine değinilirse, ilk olarak, bu tasarım açık bir algoritmaya sahiptir. Algoritmanın üçüncü kişiler tarafından biliniyor olması üretilen şifrelerin bu kişiler tarafından elde edilebileceği anlamına gelmemektedir. Bunun sebebi, algoritma tasarımında rastlantısallık yönteminin kullanılmış olmasıdır.

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 [7, 8]. Eş zamanlılık gerektiren bir mekanizmaya ihtiyaç duyulmaması sebebiyle, gerçekleştirilen tasarımda bu tip problemler görülmez. Eş zamanlılığın bozulması veya başka bir sebeple, SMS gibi herhangi bir iletişim kanalı üzerinden kimlik doğrulaması yapan yöntemlerde ise gidip gelen veri paketlerinin çalınması, buna bağlı olarak üretilen şifrelerin elde edilmesi gibi problemler yaşanabilmektedir [33]. Örneğin SMS üzerinden haberleşme yapan yöntemlerin güvenliği tercih edilen GSM operatörünün sisteminin güvenliği kadardır. Bağlantı gerektiren bir mekanizmaya ihtiyaç duyulmaması sebebiyle gerçekleştirilen tasarımda bu tip problemler yaşanmaz.

Tek kullanımlık şifrelerin üretildiği donanımsal bir cihaz kullanılarak yapılan doğrulama yöntemlerinde ise zaman ve sayaç tabanlı TKŞ algoritmalarında olduğu gibi eş zamanlılık problemi, bir cihaz kullanıldığı için her iki tarafa da getirilen ek yüklerden dolayı bu çalışma ile sunulan yöntem daha avantajlıdır. Çünkü kullanılan cihazın sistem tarafında tanıtımı, sistem ile eş zamanlanması, kullanıcıya ulaştırılması, bozulduğunda teknik destek sağlanması gibi birçok olumsuz yönü vardır. İstemci tarafında ise, sürekli yanında taşıma, düşürme, çaldırma, kaybetme ve ek ücret ödeme gibi birçok olumsuz yönü mevcuttur. Gerçekleştirilen tasarımda ise

istemci tarafı, bugün vazgeçilmez bir ihtiyaç haline dönüşen cep telefonlarında çalışacak olan bir yazılımdan ibarettir. Hiçbir ek masraf olmadan indirilip kurulabilecek olan yazılım hem istemci telefonuna hem de doğrulama sunucusuna çok kolay adapte edilebilir bir özelliğe sahiptir. Bir kez kurulduktan sonra kendi yaşam döngüsünü oluşturan yazılımlar, sorun çıkarmadan kimlik doğrulama işlemini yürütebileceklerdir.

Kullanıcı hareketine bağlı olarak doğrulama ve yetkilendirme yapan mekanizmalarda, zamana göre kullanıcı konumunda gerçekleşen değişimler temel alınmaktadır [29, 33]. Bu yöntemlerde de benzer şekilde zaman bilgisinde taraflar arasında yaşanan eş zamanlılık problemleri ve konum ölçümünde ki hassasiyet kayıpları, bu yöntemlerde yaşanabilecek problemler arasındadır. Bu çalışmayla birlikte gerçekleştirilen tasarımda yer alan geçerli bölge kavramıyla birlikte, kullanıcı konumunun belirlenmesinde yeterli miktarda tolerans payı bırakılmıştır.

Gerçekleştirilen tasarımın, mevcut tüm sistemlere kolay ve maliyetsiz bir şekilde kurulup kullanılabilir. 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. Çizelge 4.4’ te TKŞ kullanmayan geleneksel kimlik doğrulama yöntemi ile bu çalışmayla sunulan yöntem arasında yapılan karşılaştırmalara değinilmiştir.

Çizelge 4.4. Bu çalışma ile sunulan yöntem ile geleneksel kimlik doğrulama yönteminin karşılaştırılması

	Geleneksel yöntem	Bu çalışmada sunulan 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

5. SONUÇ

Bu çalışma ile rastlantısal değişkenlere ve tercihe göre kullanıcı konumuna bağlı olarak üretilen tek kullanımlık şifreler ile kullanıcı doğrulaması yapabilen yeni bir mekanizma geliştirilmiştir. Geliştirilen mekanizmanın etkinliğini sınamak amacıyla örnek bir kimlik doğrulama ile yazılımlar test edilmiştir. Geliştirilen yöntemde, kullanıcı mobil cihazı ve doğrulama sunucusu üzerinde çalışabilecek iki ayrı yazılım Java platformu üzerinde geliştirilmiştir. Java ME kütüphaneleri kullanılarak kodlanan mobil Midlet yazılım projesi, Sun Wireless Toolkit (SWT) aracıyla test edilmiştir [22]. Dinamik web projesi olarak geliştirilen sunucu yazılım projesi ise JBoss Uygulama Sunucusu (JBoss AS 7) üzerinde çalıştırılmıştır [24]. Her iki yazılımı da birlikte çalıştırarak yapılan testler sonucunda kimlik doğrulama sürecinin başarıyla gerçekleştirildiği gözlemlenmiştir. Yapılan testlerde hem değişkenlerin hem de üretilen TKŞ değerlerinin karakter uzunluklarının rastlantısal olarak değişim gösterdiği ve buna bağlı olarak tahmin edilebilme risklerinin son derece az olduğu ortaya çıkmıştır.

Gerçekleştirilen mekanizma sahip olduğu özellikler sebebiyle güçlü bir kimlik doğrulama yöntemi olarak nitelenebilir. Maliyet açısından, standart kullanıcı adı/şifre tasarımı gibi ücretsiz, güvenlik açısından diğer TKŞ yöntemleri gibi güçlüdür. Bu sebeple, tasarım kullanıcı kimlik doğrulama amacıyla, internet üzerinden hizmet sunan ticari yazılımlar, hükümet uygulamaları veya ücretsiz sosyal medya hizmetleri gibi sistemler tarafından rahatlıkla kullanılabilir.

Tek kullanımlık şifreler, herhangi bir iletişim kanalına veya eş zamanlı çalışma gerektiren bir mekanizmaya ihtiyaç duyulmadan üretilmiştir. Tek kullanımlık şifrelerin sağladığı faydalar sayesinde kimlik doğrulama sistemlerinin güvenilirliği artırılmıştır.

KAYNAKLAR

1. Getting, I. A., “The global positioning system”, **IEEE Spectrum**, pp. 36–47 (1993).
2. Guha, R. K., Furqan, Z., Muhammad, S., “Discovering Man-in-the-Middle Attacks in Authentication Protocols”, **IEEE, Military Communications Conference, MILCOM 2007**, 1(7) : 29-31 (2007).
3. Jøsang, A., AlFayyadh, B., Grandison, T., AlZomai, M., McNamara, J., “Security Usability Principles for Vulnerability Analysis and Risk Assessment”, **Computer Security Applications Conference**, pp. 269-278 (2007).
4. Kim, H. C., Lee, H. W., Lee, K. S., Jun, M. S., “A Design of One-Time Password Mechanism using Public Key Infrastructure”, **Fourth International Conference on Networked Computing and Advanced Information Management**, 1(1) : 18-24 (2008).
5. Eldefrawy, M. H., Alghathbar, K., Khan, M. K., “OTP-Based Two-Factor Authentication Using Mobile Phones”, **Eighth International Conference on Information Technology: New Generations**, pp. 327-331 (2011).
6. Aloul, F., Zahidi, S., El-Hajj, W., “Multi Factor Authentication Using Mobile Phones”, **IEEE/ACS International Conference on Computer Systems and Application**, pp. 641-644 (2009).
7. Lin, I. C., Chang, C. C., A countable and time-bound password-based user authentication scheme for the applications of electronic commerce. **Information Sciences**, 179:1269–1277 (2009).
8. Liao, S., Zhang, Q., Chen, C., Dai, Y., A “Unidirectional One-Time Password Authentication Scheme without Counter Desynchronization”, **ISECS International Colloquium on Computing, Communication, Control, and Management**. 4(1):361-364 (2009).
9. Lee, Y. S., Lim, H. T., Lee, H. J., “A Study on Efficient OTP Generation using Stream Cipher with Random Digit”, **Advanced Communication Technology (ICACT)**. 2(1):1670-1675 (2010).
10. Internet : Wikipedia “Security Token”
http://en.wikipedia.org/wiki/Security_token (2013).
11. Cleeff, A., Pieters, W., Wieringa, R., “Benefits of Location-Based Access Control: A Literature Study”, **IEEE Computer Society**, pp. 739-746 (2010).

12. İnternet : Wikipedia “Access Control”
http://en.wikipedia.org/wiki/Access_control (2013).
13. Chengqiang, X., Zhenli, Z., “An Integrated One-Time-Password and Access Control Authentication Scheme”, **Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conference**, pp. 252-254 (2010).
14. Lamport, L., “Password authentication with insecure communication”, **Communications of The ACM**, 24(11) : 770-772 (1981).
15. Bellare, M., Canetti, R., Krawczyk, H., “Keying Hash Functions for Message Authentication”, **Springer-Verlag Berlin Heidelberg**, pp. 1-15 (1996).
16. Liao, I., Lee, C., Hwang, M., “A password authentication scheme over insecure Networks”, **Journal of Computer and System Sciences**, 72(4) : 727-740 (2006).
17. Do van, Thanh, Jorstad, I., Jenvik, T., Do van, Thuan, “Strong authentication with mobile phone as security token”, Mobile Adhoc and Sensor Systems, **MASS '09. IEEE 6th International Conference on** , pp.777-782 (2009).
18. Raddum, H., Nestas, L. H., Hole, L. H., “Security Analysis of Mobile Phones Used as OTP Generators”, **WISTP'10 Proceedings of the 4th IFIP WG 11.2 international conference on Information Security Theory and Practices: security and Privacy of Pervasive Systems and Smart Device**, pp. 324–331 (2010).
19. Liao, K. C., Lee, W. H., Sung, M. H., Lin, T. C., “A One-Time Password Scheme with QR-Code Based on Mobile Phone”, **Fifth International Joint Conference on INC, IMS and IDC**, pp.2069-2071 (2009).
20. İnternet: Tüketici Finansman “İnternet Bankacılığı’nda Tek Kullanımlık Şifre Dönemi” <http://www.tuketicifinansman.net/2009/12/internet-tek-kullanimlik-sifre-otp.html#ixzz1MjBVCGGe> (2013)
21. İnternet : Wikipedia “Strong Authentication” http://en.wikipedia.org/wiki/Strong_authentication (2013).
22. Kim, H. C., Lee, H. W., Lee, K. S., Jun, M. S., A Design of One-Time Password Mechanism using Public Key Infrastructure, **Fourth International Conference on Networked Computing and Advanced Information Management**; 1(1) : 18-24 (2008).
23. Cho, J. S., Yeo, S. S., Kim, S. S., “Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value”, **Computer Communications**, 34:391-397 (2011).

24. Anind, K. D., "Understanding and using context", **Personal and Ubiquitous Computing**, 5 (1) : 4-7 (2001).
25. Becker, G. T., Lo, S. C., Lorenzo, D. S. D., Enge, P. K., Paar, C., "Secure Location Verification - A Security Analysis of GPS Signal Authentication", **In DBSec**, pp. 366-373 (2010).
26. Sandhu, R., Coyne, E., Feinstein, H., Youman, C., "Role-based access control models", **IEEE Computer Society**, 29(2) : 38-47 (1996).
27. Bertolissi, C. , Fernandez, M., "Time and Location Based Services with Access Control. New Technologies", **Mobility and Security**, pp.1-6 (2008).
28. Damiani, M. L., Bertino, E., Catania, B., Perlasca, P., "GEO-RBAC: A spatially Aware RBAC", **ACM Transactions on Information and System Security (TISSEC)**, 10(1) (2007).
29. Damiani, M. L., Bertino, E., Silvestri, C., "An Approach to Supporting Continuity of Usage in Location-based Access Control", **12th IEEE International Workshop on Future Trends of Distributed Computing Systems**, pp. 199-205 (2008).
30. Berbecaru, D., "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 (2011).
31. Liao, H. C., Chao, Y. H., "A New Data Encryption Algorithm Based on the Location of Mobile Users", **Information Technology Journal**, 7(1) : 63-69 (2008).
32. Scott, L., Denning, D., "Geo-encryption: using GPS to enhance data security", **GPS World**, pp. 40-49 (2003).
33. Hsieh, W. B., Leu, J. S., "Design of a Time and Location Based One-Time Password Authentication Scheme", **Wireless Communications and Mobile Computing Conference (IWCMC)**, pp. 201-206 (2011).
34. Durresi, A., Durresi, M., Paruchuri, V., Barolli, L., "Secure Spatial Authentication using Cell Phones, Availability, Reliability and Security", **The Second International Conference**, pp. 543-549 (2007).
35. Diffie, W., Hellman, M., "New directions in cryptography", **IEEE Transactions on Information Theory**, 22(6) : 644-654 (1976).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı : ÖZSOY, Muhammed
Uyruğu : T.C.
Doğum Tarihi ve yeri : 01.07.1986 Kastamonu
Medeni hali : Bekâr
Telefon : 0 (312) 203 82 45
e-posta : muhammedozsoy@hotmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek Lisans	Gazi Üniversitesi / Elek. Bil. Eğit ABD	-
Lisans	Selçuk Üniversitesi / Bilgisayar Müh.	2008
Lise	Kast. Abdurrahman Paşa Süper Lisesi	2004

İş Deneyimi

Yıl	Yer	Görev
2010-	Türkiye Elektrik İletim A. Ş.	Bilgisayar Müh.

Yabancı Dil

İngilizce

Hobiler

Bilgisayar teknolojileri, Yüzme, Amatör senaristlik