MOBİL TELEFONLARIN MİKRO-ÖDEME ARACI OLARAK KULLANILMASI

Erbuğ Çelebi*, Hasan Amca**
*Uluslararası Kıbrıs Üniversitesi, Bilgisayar Mühendisliği Bölümü, ecelebi@ciu.edu.tr
**Doğu Akdeniz Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü, hasan.amca@emu.edu.tr

ABSTRACT
Today, using different technologies for electronic-payment in retail market carries some issues in the mean of security and usability. The use of portable communication devices became particularly attractive candidates when versatility, security and simplicity features of payment technologies are considered.

In this paper, we investigate the use of mobile communication devices as versatile, secure and simple micro-payment tool, which satisfy the related financial, technological, computational and managerial requirements. The versatility and security of the method comes from the use of mobile telephone with a Variable Transaction Number in each transaction. Experimental results show that, the systematic requirements for the implementation of this technology are minimal and the costs involved are very much reasonable.

Key words: Payment, secure payment, industrial devices, mobile phone application.

1. GİRİŞ
Visa, Master-Card, Card Plus, American Express gibi kart tabanlı elektronik ödeme (e-ödeme) yöntemlerinin ödeme araçları olarak kullanılması, çalıntı, kayıp ve hasarlı olabilmeleri ihtimallerinden dolayı her yıl büyük ölçüde maddi zararlara yol açmaktadır [1]. Bu yöntemleri daha güvenli hale getirmek için geliştirilen, ödeme sırasında POS cihazlarına girilecek ve elektronik imza gibi düşünülebilecek kişisel kimlik numarası (PIN) da bazı güvenlik problemleri taşımaktadır. Cep telefonları (CT), bu tür elektronik ödeme araçlarının yerini tutacak basit, kullanımı kolay ve çok yönlü bir araç olarak kullanılabilir.

CT'ları Kısa Mesaj Servisi (SMS), Kızıl ötesi (IrDa), BlueTooth, RFID gibi araçlar yardımıyla elektronik ödemelerde kullanılma imkanlarına sahiptirler [3, 16]. Bu yöntemlerin tümü yapılan ödemeyi CT görüşmeleri için gelen faturaya ekleyebilme özelliklerine de sahiptirler [4].

SMS yöntemi, özel olarak belirlenmiş bir telefon numarasına gönderilen kısa mesaj ile güvenli bir alış-veriş yapılmasını sağlar. Bu yöntem ile müşterilerin yaptıkları alışveriş tutarları, CT faturalarına yansıtılabilir. CT servis sağlayıcısı alt yapısı ile çalışan SMS yöntemi yığın işleme yöntemi ile çalıştığından, alışveriş tutarını ödemek (onaylamak) için gönderilen SMS'in ne kadar gecikme ile banka tarafından onaylanacağı ve işlemin tamamlanacağı kesin değildir [5].

IrDa teknolojisi yeterince iyi tanımlı olmasına rağmen iletişim (CT ile ödeme cihazı arasında bağlantı kurulması) süresinin uzun olması e-ödeme aracı olarak kullanılmasını zorlaştırmaktadır. Ödeme süresini kısaltan fakat güvenlik seviyesini düşüren yöntemler, ödeme cihazına tüketicinin onaylamadığı ödemeleri de tükteci telefon faturasına aktarabilmesi şansını tanımaktadır [2, 6]. BlueTooth yöntemi de oldukça uzun ayarlama süresi gerektirmektedir. Ayrıca, BlueTooth cihazı alışveriş sırasında kapsama alanındaki birden fazla cihazı da arayacak ve ödeme süresinin uzamasına sebep olabilmektedir [7].

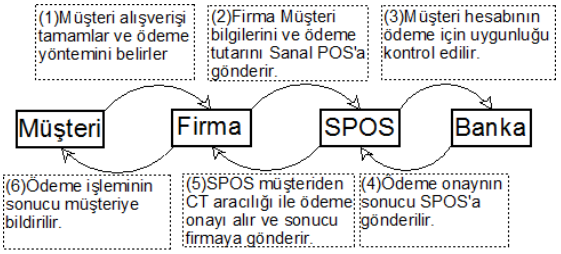
Bu makalede önerdiğimiz yöntem, ödemeyi onaylayan aracı firmanın ürettiği her işlem için ayrı ve güvenli bir işlem numarası temeline dayanmaktadır. Üretilen bu numara, CT'na GPRS aracılığı ile gönderildikten sonra CT'de çubuklu kod'a dönüştürülür. CT'de oluşan bu çubuklu kod ödeme noktasındaki çubuklu kod okuyucusu tarafından okunabilecek şekildedir. Ödeminin bu şekilde yapılması yukarıda sayılan gecikme ve güvenlik sorunlarını da aşacaktır.

Önerdiğimiz bu ödeme yöntemi cep telefonlarının kredi kartlarından daha yaygın kullanıldığı ortamlarda kullanılabilme şansına sahiptir. Gelişmemiş ve gelişmekte olan ülkelerde CT'lerin kullanımı kredi kartı kullanımından daha yaygındır. Bu ülkelerde, mobil ödemenin yaygınlaşması için CT'ler kredi kartı yerine kullanılabilir.

Bu makale şu şekilde organize edilmiştir: Bölüm 1'de mobil ödeme tanıtılmış, bölüm 2'de çevirim içi mobil ödeme için gerekli adımlar, bölüm 3'te Değişken İşlem Numaralı Çubuklu Kod (DİNÇ) yöntemi ile sistem yapısı ve güvenlik konuları anlatılmıştır. Deneysel sonuçlar ve test sonuçları bölüm 4'te, sonuç ise son bölümde anlatılmıştır.

2. ÇEVİRİM İÇİ ÖDEME İÇİN GEREKLİ ADIMLAR
Çevirim içi ödeme, diğer adıyla elektronik ödeme, alınan hizmetlerin veya ürünlerin banknot kullanımadan ve ödeme sırasında banka tarafından onay alınarak yapılan ödemedir. Birden fazla olan

elektronik ödeme yöntemleri güvenli, hızlı, kullanımı kolay ve sahteciliğe imkan tanımayan bir yapıda olmalıdır. Bu gereksinimleri karşılamak için, 2 temel adım gereklidir:



Şekil 1: e-ödeme aşamaları

2.1 Onay

Onay adımında müşterinin yapmak istediği miktardaki harcamanın hesabından karşılanabileceği ve ödemeyi yapmak isteyenin hesap sahibi olduğu doğrulanır. Bu işlem şekil 1 de gösterilmiştir.

2.2 Parasal işlemler

SPOS (Sanal POS) adımında, müşteri hesabındaki ilgili tutar işlemin onaylanması durumunda, hizmet veya ürün alımı yapılan firma hesabına aktarılır ve bu işlemin tamamlandığı bilgisi gönderilir. Bu işlem bazen PayPal [14] gibi aracı firmalar ile de yapılabilir.

Bir sonraki bölümde, CT ler kullanılarak yapılan elektronik ödemenin altyapısı ve pratik uyarlaması anlatılmıştır. Yukarda da bahsettiğimiz onay ve parasal işlem adımları da belirtilmiştir.

3. DEĞİŞKEN İŞLEM NUMARASI İLE ÇİZGİSEL KOD (DİNÇ) YÖNTEMİ

Kredi kartları alışverişlerde kullanılırken, kredi kartı numarası müşteriyi temsil eden bir kimlik numarası gibi kullanılır. Ancak bu numara her alışverişte (işlemde) hiç değiştirilmeden kullanıldığından, bazı güvenlik sorunları ortaya çıkmaktadır. Kredi kartı numaraları hatırlanması ve kopyalanması kolay olduğundan kötü niyetli kişiler tarafından kullanılması riskini de taşırlar. Bu riski azaltmak için son zamanlarda zorunlu tutulan PIN numarası sorgusu da, müşterilerin PIN numaralarını girerken veya sözlü olarak kasiyere söylerken başkaları tarafından kopyalanabileceğinden yeterince güvenli olamamaktadır. Bunun sebebi her hesap sahibinin sadece bir kredi kartı hesap numarası ve bir PIN numarası olmasından kaynaklanmaktadır. Sıkça raslanan kredi kartı bilgilerini elde etme yöntemleri (yan kesicilik, veritabanı hırsızlığı v.s.) de [13] te anlatılmıştır.

Kötü niyetli kullanım ie birlikte kayıp ve hasar problemleri de her yıl ciddi bir maddi zarara yol açmaktadır [2]. Kredi kartlarında yaşanan bu tür sorunlar maddi zararlara sebep vermeleri yanında, müşterilerin de güvenlik endişelerini artırmaktadır. Bu sebeple kredi kartlarından daha başarılı ve kullanışlı bir yöntem bu sorunları ortadan kaldıracak ve müşterilerin ödemelerini herhangi bir endişe duymadan yapmalarını sağlayacaktır.

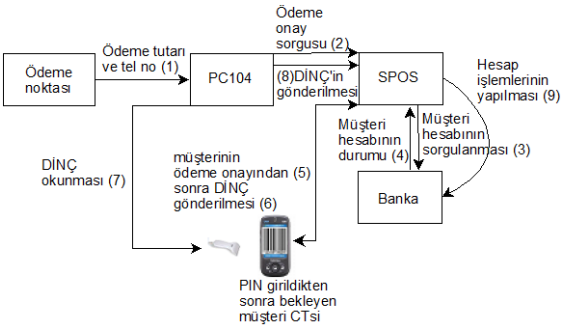
Bu çalışmada güvenli bir ödeme aracına alternatif olarak önerdiğimiz DİNÇ yöntemi yapısal olarak basit, kullanımı kolay, uygulanabilir, açık mimari, kısa işlem süresi ve diğer sistemlere kolaylıkla entegre edilebilir bir yapıdadır. DİNÇ yöntemi mevcut telekominikasyon altyapısını kullanabilen, CT'ler ile çalışabilecek yukarıda anlatılan güvenlik sorunlarını çözebilecek bir yapıya sahibtir. DİNÇ yönteminin detayları bir sonraki bölümde verilmiştir.

3.1 Yapısal basitlik ve uygulanabilirlik

Önerdiğimiz yöntemin yapısal olarak basit ve uygulanabilir olması; DİNÇ yöntemini varolan bir ödeme sistemine dahil etmek için gerekli yazılım ve donanımın yapısından kaynaklanmaktadır. Ayrıca DİNÇ yöntemi ile yapılan ödeme, iletişim ağını minimum düzeyde kullanarak, işlemleri hızlı gerçekleştirmesi gerekmektedir. Böylece düşük hızda ve çok yoğun ağ ortamlarında da çalışabilecektir. Şekil 2'de bu işlemler daha detaylı anlatılmıştır. DİNÇ sistemi temel olarak kredi kartı sistemi ile benzer kullanıma sahiptir. Ancak, müşteriler, kredi kartı yerine CT ekranlarındaki çizgisel kodları, satış noktasındaki görevli kontrolündeki çizgisel kod okuyucusuna göstererek ödemelerini tamamlarlar. Ödeme noktasondaki kredi kartı POS cihazı yerinde ise, network bağlantısına sahip gömülü bir sistem (PC104) ile çizgisel kod okuyucu yer alır. Şekil 2'de gösterilen PC104 ve üzerinde Linux gibi az kaynak gerektiren bir işletim sistemi ile çalışan bir yazılım, ödeme noktası için gerekli cihaz ihtiyaçlarını karşılayacaktır.

3.2 Katmanlı protokol yapı

DİNÇ sisteminin sunucu tarafındaki uygulama katmanı, CT'den gelen değişken işlem numarasını GPRS aracılığı ile alıp gerekli işlemleri yapar. Şekil 2'de gösterilen 2, 3, 4, 5, 6, 8 ve 9 adımları DİNÇ'in uygulama katmanını anlatmaktadır.



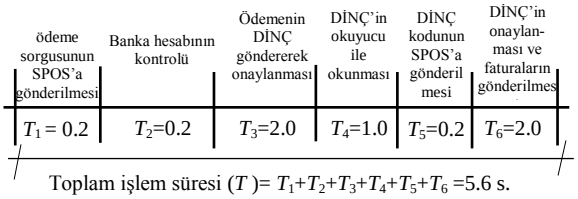
Şekil 2: DİNÇ Sisteminin yapısı

Alışveriş yapıldıktan sonra, firma yazar-kasasındaki tutarı DİNÇ yöntemi ile ödemek isteyen bir müşteri için gerçekleştirilecek işlemler şöyledir: Ödeme, CT arkasındaki sabit çubuklu kodu ödeme noktasındaki okuyuca göstermekle başlar. CT arkasındaki bu sabit çubuklu kod, ödemenin yapılacağı CT numarasını belirtecektir. Bu işlemden sonra, sanal POS (SPOS) cihazından CT ye gelecek olan değişeken numaralı barkod beklenir. CT sahibi ödeme onayı vermesi için PIN girdikten sonra CT'ye gelen çubuklu kodu çubuklu kod okutucusuna gösterir ve ödeme işlemi onayı tamamlanır (7). Ödeme onayından sonra, SPOS'a gönderilen değişken işlem numarası sunucu sisteminde teyit edilir (8) ve işlem tamamlanır.

Sisteme ek bir güvenlik eklemek için, CT'ye çubuklu kod gönderilmeden önce, kullanıcıya PIN sorulur (5. adımdan önce). PIN doğru girilmesi durumunda, ödeme onayı için gerekli değişken işlem numarası SPOS tarafından CT'ye gönderilir ve CT'de çubuklu kodlara dönüştürülür. DİNÇ yöntemi ile yapılan ödemeler, benzin istasyonu, satış makineleri, otobüsler, araba park yerleri ve sinema gibi yerler için uygun bir sistemdir.

3.3 İşlemler ve bekleme süresi.

İşlemlerin bekleme süresi elektronik ödeme sistemlerinin kabul edilebilirlikleri için önemli bir parametredir. Ödeme sırasında ortaya çıkacak uzun bekleme süreleri, sistemin devamlılığını olumsuz yönde etkileyecektir. Daha önce yapılan çalışmalar, bu bekleme süresinin 1 saniyeden az olması gerektiğini göstermektedir [12]. DİNÇ yöntemi ile yapılan ödemelerdeki bekleme süresinin, Bluetooth, IrDa, RFID gibi yöntemlerden daha kısa ve geleneksel kredi kartı işlemleri bekleme süresine benzer bir bekleme süresinin olması öngörülmektedir. Önerdiğimiz sistemdeki bekleme süresi, CT arkasındaki çubukulu kodun okunup, SPOS'a gönderilmesi, SPOS'tan CT'ye çubuklu kod gönderilmesi, CT ekranındaki çubuklu kodun VPOS'a gönderilmesi ve SPOS'un gelen bilgiyi teyit edip gerekli banka transferlerinin yapılması işlemleri bekleme süresini etkilemektedir. SPOS tarafından oluşturulan değişken işlem numarası rasgele seçilen 10 basamaklı bir sayıdır. Rasgele seçilen bu sayı SPOS veritabanına yazılır ve CT'ye rakam olarak gönderilir. CT'ye gelen bu rakam CT üzerindeki Java Midlet uygulaması ile çubuklu koda dönüştürülür. Bu aşamada, CT'ye doğrudan çubuklu kod gönderilmesi bir resim dosyası gönderilmesi gerektirdiği için GPRS üzerinden gelecek bu veri uzun bekleme süresi (ve yüksek maliyet) oluşmasına sebep olacatı. SPOS tarafından gönderilecek bir rakam, bu rakama karşılık gelen resim dosyasından çok daha kısa (veri uzunluğu olarak) olacağından bekleme süresini oldukça azaltacaktır. DİNÇ sisteminde değişken işlem numarasının oluşturulup CT'ye gönderilmesi ve ödeme onaylandıktan sonra bu numaranın tekrar SPOS'a gönderilmesi (GPRS üzerinden iletişim) bekleme süresini en fazla etkileyen adımlardır. Buradaki bekleme süreleri ise iletişim ağlarındaki yoğunluğa bağlıdır. Yaptığımız çalışmalar doğrultusunda, her bir adımdaki beklem süreleri Şekil 3'te belirtilmiştir.



Toplam işlem süresi (T)= $T_1+T_2+T_3+T_4+T_5+T_6$ =5.6 s.

Şekil 3: Sistem için gerekli süreler

DİNÇ sisteminde, bekleme süresini oluşturan temel parametreler; bağlantı süresi, veri iletim süresi, işlem süresi, güvenlik doğrulama süresi ve bağlantının kapatılması süresidir. Sonuç olarak DİNÇ sistemi aşağıdaki adımlardan oluşmaktadır ve bu adımların her biri bekleme süresini etkilemektedir. Şekil 3'teki her bir T süresinin açıklaması şu şekilde yapılabilir:

T_1: Müşteri bilgileri ile ödeme tutarının, ödeme kontrolu için SPOS'a gönderilmesi

T_2: Müşteri hesabının ilgili ödeme için uygun olup olmadığı kontrolü

T_3: SPOS'un CT'ye ödem onayı için değişken işlem numarası göndermesi

T_4: Değişken işlem numarasının okunması

T_5:Değişken işlem numarasının teyit edilmesi için SPOS'a gönderilmesi

T_6: Değişken işlem numarasının onaylanması, banka işlemlerinin yapılması, ödeme bilgisinin hem müşteriye, hem de ilgili firmaya gönderilmesi.

Yukarıda sözü geçen müşteri hesabı, herhangi bir banka tarafından belirlenen bir kredi-kartı hesabı olup, sanal POS yazılımları tarafından da erişilen bir hesaptır.

3.4 Sistemin kullanırlığı

DİNÇ sistemini kullanmak, mağzadan satın alınan bir ürünün çubuklu kod okuyucusuna okutmak kadar basit bir işlemdir. Bu sistemi kullanacak kullanıcıların temel telefon kullanma bilgilerinden başka bir bilgiye ihtiyaçları yoktur. Bu sistemi kullanmak için gerekli olan tek işlem, ilgili servis sağlayıcısına kayıt olmaktır. Kredi kartı kullanımının yaygın olmadığı fakat CT kullanım oranının çok yaygın olduğu ülkelerde bu sistemin kullanılması daha uygundur.

3.5 Diğer servis sağlayıcıları ile çalışabilme

Önerdiğimiz elektronik ödeme sisteminin kullanılabilmesi için, yukarıda da bahsettiğimiz gibi aracı bir servis sağlayıcısına (banka) ihtiyaç duyulmaktadır. Bu sistemi kullanacak kullanıcılar, kredi-kartı numaraları ile sisteme kayıt olurlar.

Ödeme işlemi sırasında DİNÇ sistemi SPOS sistemi ile bağlı olduğu banka aracılığı ile müşterilerin kredi-kartları hesapları üzerinden gerekli işlemleri yapar. Burada önemli olan, seçilen bankanın ve müşteri hesaplarının bulunduğu bankanın sistem için önemli olmadığı ve dolayısı ile sistemden bağımsız olmasıdır. Ayrıca müşterilere gönderilecek değişken işlem numarası da herhangi bir GPRS altyapısı üzerinden müşteri CT'na ulaşabileceğinden; sistem müşterilerinin abonesi oldukları mobil operatöründen de bağımsızdır.
Sistemin banka ve mobil operatör gibi servis sağlayıcılarından bağımsız olması, sistemin daha yaygın bir şekilde kullanılmasını sağlayacaktır.

3.6 Güvenlik

Değişken işlem numarası ile CT kullanıcılarının bir alışveriş için kullandıkları işlem numarasını bir sonraki alışverişlerinde kullanmaları engellenmektedir. Güvenliğini sağlamak için, sistem CT'ye değişken işlem numarası göndermeden önce PIN veya şifre soracaktır. Böylece, günümüzde kullanılan, kredi-kartları için kasiyer yanındaki POS cihazına girilen PIN numarası CT'na girerek ödeme işlemi devam edecektir. Bu sistemi kullanacak kullanıcıların tanımlanması için CT üstüne yapıştırılmış çubuklu kodlar veya alternatif olarak, RFID kullanılabilir.

Kredi-kartı temelli ödemelerde ödemenin yapıldığını gösteren belgeyi saklama zorunluluğu da vardır. Ancak, elektronik ortamın getirdiği avantajlarla, bu tür belgeleri saklamaya gerek yoktur. Yapılan ödemelere CT üzerindeki yazılımlar ile ulaşmak ve tüm işlem hareketlerini takip etmek mümkündür.

4. DENEYSEL ÇALIŞMALAR VE TEST SONUÇLARI

DİNÇ sistemi üç ana modülden oluşmaktadır. Bunlar sırasıyla; kullanıcıların kullanacakları satış noktasındaki POS cihazı, tüm işlemlerin gerçekleştirilip gerekli kayıtların tutulacağı bir uygulma sunucusu ve CT dir.

4.1 POS Cihazı

DİNÇ sisteminin POS cihazı modülü tek kartlı bilgisayar (PC104) ile tasarlandı. Tek kartlı bilgisayarlar (TKB) özellikle endüstriyel amaçlı uygulamalar için kullanılan, işlemci, hafıza, çevre üniteleri, ekran kontrolü v.b. modüllerinin küçük bir kart üzerinde (3.5"x3.5") toplandığı bilgisayarlardır. Cihaz için gerekli işletim sisteminin ve diğer yazılımların saklanacağı disk için DiskOnModule (DOM) denilen 44 pinli Flash diskler kullanıldı. DOM diskleri herhangi bir hareketli veya mekanik aksam içermediklerinden ve dolayısıyle arızalanma ihtimalleri klasik harddisklerden daha düşük olduğundan, DİNÇ sisteminin POS cihazında kullanılmak üzere tercih edildi. Sistemin çalışması için bir Linux dağıtımı olan Ubuntu kullanıldı.

Sonuç olarak ortaya çıkan sistem şu özelliklere sahip oldu: 133MHz işlemci, 64MB hafıza, 2×USB port, PCI arayüz, parallel port, 2×RS232 port, AGP uyumlu VGA arayüz, 44-pin IDE flash disk, klavye, VGA arayüzü ve +5V güç kaynağı. Sistemde ihtiyaç duyulan ekran görüntüleri (ödeme tutarı, ödeme onayı v.b.) çok az olduğundan maliyeti artıran bir VGA ekran yerine 4 satırlı Hitachi HD44780 tabanlı (20×4 karakter) bir LCD kullanıldı. Bu LCD'yi kontrol için ise C++ tabanlı LCD4Linux kütüphanesi kullanıldı.
Yukarı da bahsedildiği gibi bu cihaz ödeme noktasındaki kredi kartları için kullanılan POS cihazı yerine kullanılmak üzere tasarlandı. Bu cihaz ile merkezde bulunan uygulama sunucusu (sanal POS) arasındaki bilgi alışverişi için LibCurl kütüphanesi kullanıldı.

4.2 Uygulama Sunucusu

Uygulama sunucusu, ödeme noktasından gelen ödeme sorguları için müşteri hesaplarının uygun olup olmadığının saptanması, müşteri bilgilerinin saklanması/düzenlenmesi, müşteri CT'na gönderilecek değişken işlem numaralarının oluşturulması ve gönderilmesi, sistemin kontrolü için gerekli raporların oluşturulmasını sağlar. Yaptığımız çalışmalarda bu fonksiyonları gerçekleştirmek için C#.Net ile geliştirdiğimiz web servisleri kullandık.

4.3 CT yazılımı

CT üzerinde yapılacak tüm işlemler için GPRS altyapısı ile uygulama sunucusuna ulaşabilecek, Java Midlet teknolojisi ile bir yazılım geliştirdik. Geliştirdiğimiz bu uygulama CT üzerinde çalıştırıldığında kullanıcıya bir PIN numarası sorar. Müşteri tarafından girilen bu PIN numarası ile kullanıcının sisteme güvenli bir şekilde erişmesi sağlanır. Müşteri sisteme girdikten sonra, kendisi için bekleyen bir ödeme sorgusu varsa CT üzerindeki yazılım ile kullanıcıya bildirilir. Bu kontrolü yaparken uygulama sunucusu üzerindeki web-servisleri kullanılır. Uygulama sunucu, müşteri için bekleyen bir ödeme için onay verilmesi durumunda, müşteri CT'na değişken işlem numarası gönderir. CT'na gelen değişken işlem numarası, aynı uygulama ile çubuklu kod'a çevrilir. Kullanıcının CT ekranındaki çubuklu kodu ödeme noktasındaki okuyucuya göstermesiyle işlem devam eder. Ödeme noktasından okunan kodlar, uygulama sunucusunda tekrar onaylanır ve ödeme tamamlanır.

5. SONUÇ

Bütün dünyada kullanılan kredi kartları bazı güvenlik sorunlarını ve kullanım zorluklarını da beraberinde getirmektedir. Yukarıdaki bölümlerde de bahsedildiği gibi belirtilen sorunlardan

kurtulmak için farklı ödeme çözümleri gerekmektedir. Ödeme yöntemi olarak cep telefonu kullanımı; ileri güvenlik seçenekleri, farklı sistemlerle (banka, mobil operatör) müşterek çalışabilmesi, kullanım kolaylığı, yüksek kullanım oranı ve sağladığı teknik kolaylıklardan dolayı uygun olduğu düşünülmektedir.

Alternatif bir ödeme yöntemi olarak önerdiğimiz cep telefonu tabanlı DİNÇ sistemi güvenli, verimli ve hızlı bir sistem olduğu gözlemlenmiştir. Sistemin çalışması için gerekli ve CT üzerinden girilen PIN numarası ile yapılan kimlik doğrulaması sistemin güvenirliğini sağlanmaktadır. Önerdiğimiz sistem modüler olduğundan, her modül farklı yöntemler ile geliştirilebilir ve sistem daha farklı çalıştırılabilir.

Yaptığımız bu çalışmada, mobil iletişim araçlarının çok yönlü, güvenilir ve basit bir mikro-ödeme aracı olarak kullanılması üzerine araştırmalar ve geliştirmeler yaptık. Önerdiğimiz sistemin çok yönlü ve güvenilir olması her hareketin (alışverişin) üretilen Değişken İşlem Numarası üzerine kurulmasıyla oluşturulmuştur. Yaptığımız çalışmalar, böyle bir sistemin mikro-ödemeler (gazete, büfe, park-yeri v.b.) için uygun olduğunu ayrıca, geliştirilmesi için gerekli altyapı maliyetinin de kabul edilebilir seviyede olduğunu göstermiştir.

KAYNAKLAR

[1] Eliminating Some Credit Card Risk for E-Business, http://ecommerce.Internet.com/solutions/ec101/article/0,1467,6321_569741,00.html.

[2] Internet Usage Statistics – The Big Picture, http://www.internetworldstats.com/

[3] Pi Huang And A.C. Boucouvalas, Future Personal "E-Payment: Irfm", *IEEE Wireless Communications*, pp. 60-66, Feb. 2006.

[4] S. Schwiderski-Grosche and H. Knospe, "Secure Mobile Commerce", *Electronics & Communication Engineering Journal*, pp. 228-238, October, 2003.

[5] S. F. Mjpllsnes and C. Rong, "On-line e-wallet system with decentralized credential keepers," *Mobile Network Applications,* vol. *8* , pp. 87-99, 2003.

[6] IrDA, Infrared Financial Messaging Point and Pay Profile (IrFM), ver. 1.0, Dec. 2003.

[7] Bluetooth Core Specification, ver. 1.2+EDR, *Bluetooth SIG*, Nov. 2003.

[8] Weiping Z.H.U, Dong WANG and Huanye SHENG, "Mobile RFID Technology for Improving M-Commerce". *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'05)*, Shanghai, China, March 2005

[9] Raj BRIDGELALL, "Enabling Mobile Commerce Through Pervasive Communications with Ubiquitous RF Tags", *Wireless Communications and Networking*, Volume 3, pp: 2041–2046, March 2003.

[10] William Stallings, "*Data and Computer Communications, Seventh Edition*", Prentice-Hall, 2004.

[11] C.D. Knutson And J.M. Brown, "Irda Principles And Protocols:" *The IrDA Library*, Vol.1, MCL Press, 2004.

[12] H.R. Damon, R.J. Brown, and L. Faulkner, White Paper, "Creating an End-To-End Digital Payment System," *IrDA Press*, Oct. 1999.

[13] Yingjiu Li and Xinwen Zhang, "A Security-Enhanced One-Time Payment Scheme for Credit Card", Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications, RIDE-WS-ECEG'2004, Boston, USA , March, 2004.

[14] PayPal "Online Payment Processing", https://www.paypal.com/cgi-bin /webscr?cmd=_wp-pro-overview-outside.

[15] Sami IREN, Paul D. AMER and Phillip T. CONRAD, "The Transport Layer: Tutorial and Survey", *ACM Computing Surveys*, Vol. 31, No. 4, December 1999.

[16] Hasan Amca And Raygan Kansoy, "A Mobile Telephone Based, Secure Micro-Payment Technology Using The Existing ICT Infrastructure"**,** Chinacom 2007: International Conference On Communications and Networking In China, 22-24 Aug. 2007, Shanghai, China.