T.C.
KAHRAMANMARAŞ SÜTÇÜ İMAM ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
ELEKTRİK-ELEKRONİK MÜHENDİSLİĞİ ANABİLİM DALI

3.NESİL GEZGİN TELEFONLAR ÜZERİNDE MULTİMEDYA DESTEKLİ GÜVENLİK ARTIRIM TEKNİKLERİNİN ARAŞTIRILMASI

M. ERDAL DAYAK

YÜKSEK LİSANS TEZİ

KAHRAMANMARAŞ
ŞUBAT - 2007

T.C.
KAHRAMANMARAŞ SÜTÇÜ İMAM ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
ELEKTRİK-ELEKTRONİK ANABİLİM DALI

3.NESİL GEZGİN TELEFONLAR ÜZERİNDE MULTİMEDYA DESTEKLİ GÜVENLİK ARTIRIM TEKNİKLERİNİN ARAŞTIRILMASI

M. ERDAL DAYAK

YÜKSEK LİSANS TEZİ

Kod No:

Bu tez 06/02/2007 Tarihinde Aşağıdaki Jüri Üyeleri Tarafından Oy Birliği ile Kabul Edilmiştir.

Yrd.Doç.Dr Abdulhamit SUBAŞI DANIŞMAN	**Prof. Dr. M.Kemal KIYMIK ÜYE**	**Yrd. Doç. Dr. Metin ARTIKLAR ÜYE**

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof. Dr. Özden GÖRÜCÜ
Enstitü Müdürü

Proje No:

İÇİNDEKİLER

ÖZET

Gelişen teknoloji ve İnternet'in yaygın olarak kullanımıyla birlikte pek çok rahatlığın yanında başta güvenlik olmak üzere pek çok problem ortaya çıkmıştır. Bu güvenlik problemlerin en başında da karşıda muhatap olduğunuz kişinin gerçek/doğru kişi olup-olmadığıdır.

Multimedya destekli güvenlik yöntemleri her geçen gün günlük hayatımıza girmeye başladı (Kurum girişlerinde, özel yerlere girişlerde). Ancak gezgin telefonlar üzerinde ise güvenlik yöntemi olarak hâlâ sadece şifreler kullanılmaktadır. Kullanımı her geçen gün artan multimedyalı telefonlar sayesinde sunucu tabanlı görsel ve/veya işitsel bilgiler yöntemler kullanarak güvenliğin arttırılacağı öngörülmektedir.

Bu çalışmada gezgin cihazlar ile bunların bağlantı kurdukları sunucular arasında işitsel güvenlik yöntemleri kullanılarak iletişimin daha güveli hale getirilmesi araştırılmış ve bununla ilgili bir uygulama geliştirmeye çalışılmıştır.

Anahtar Kelimeler: multimedya, gezgin cihazlar, güvenlik, ses tanıma.

ABSTRACT

Though the evolving technology and the widespread usage of Internet made the daily works easier for us, it brought some problems to deal with, such as security. A primary issue is to assure the identity of the users connected to a server with a mobile device.

Multimedia-based security applications are being more popular day by day (Entering a company building, exclusive places etc). But only passwords are used as a security method on mobile device based authentication. It is foreseen that by the multimedia supported mobile phones those usage is spreading continuously, the security will be increased by server based visual and auditory methods.

In this work, it is investigated to make a more secure communication of a client and server by using auditory security methods and we worked to develop a relevant security application.

Keywords: Multimedia, mobile device, security, speech recognition.

ÖNSÖZ

Multimedya tabanlı gezgin cihazların her geçen gün hızlanmaları buna bağlı olarak da bunlardan beklenen işlerinde her geçen gün artmasına sebep olmuştur. Gezgin cihazlara yüklenen görevlerin bir kısmı da (banka işlemleri, kurumsal işlemler gibi) beraberinde güvenlik problemlerini ortaya koymuştur. Ancak şu aşamada güvenlik problemleri sadece şifre veya kullanıcıya sorulan kişisel sorular yöntemiyle yapılmaktadır.

Gezgin cihazların her geçen gün hem hızlanması hem de multimedya desteklerinin artmasından dolayı sunucu tabanlı görsel/işitsel güvenlik yöntemleri kullanılarak güvenliliğin arttırılabilineceği öngörülmüş ve çalışmalar bu doğrultuda yapılmıştır.

Hazırlanmış olan bu çalışmalarım sırasında değerli yardımlarını esirgemeyen danışman hocam Yrd.Doç.Dr. Abdülhamit SUBAŞI'na teşekkürlerimi sunarım.

Bu alanda yapmış olduğum çalışmalar sırasında ve pek çok çalışmalarımda değerli yardımlarını esirgemeyen değerli arkadaşlarım Mustafa KARABULUT'a teşekkürlerimi iletirim.

Şubar, 2007
KAHRAMANMARAŞ **MEHMET ERDAL DAYAK**

ÇİZELGELER DİZİNİ

ŞEKİLLER DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

1G : First Generation
2G : Second Generation
3D : Three Dimension
3G : Third Generation
4G : Fourth Generation
AMPS : Advanced Mobile Phone Service
AMS : Application Management Software
ANSI : American National Standards Institute
AUC : Authentication Center
API : Application Programming Interface
AWT : Absract Windows Toolkit
BSC : Base Station Controller
CDC : Connected Device Configuration
CDPD : Cellular Digital Packet Data
CLDC : Connected Limited Device Configuration
CPU : Central Processing Unit
D-AMPS : Dijital-Advanced Mobile Phone Service
DCS : Digital Cellular System
DECT : European Digital Enhanced Cordless Telecommunications
DES : Data Encryption Standard
DVD : Digital Video Disk
ECB : Electronic Code Book
EDGE : Enhanced Data Rate for GSM Evolution
GPRS : General Packet Radio Service
GSM : Global System for Mobile Communications
GUI : Graphical User Interface
HSCSD : High Speed Circuit Switched Data
HTTP : Hypertext Transfer Protocol
HTTPS : Hypertext Transfer Protocol Secure
IDE : Interface Developement Environment
IMAP : Internet Mail Application Protocol
IrDA : Infrared Data Association
ITU : International Telecommunication Union
J2EE : Java 2 Enterprise Edition
J2ME : Java 2 Micro Edition
J2SE : Java 2 Standart Edition
JAD : Java Application Descriptor
JAM : Java Application Manager
JAR : Java Archive File
JDBC : Java Database Connectivity
JSP : Java Server Pages
JVM : Java Virtual Machine
KB : Kilo Byte
Kbit/s : Kilobit/saniye
Kbps : Kilo bit per second

KVM : Kilobyte Virtual Machine
MB : Mega Byte
Mbit/s : Megabit/saniye
Mbps : Mega bit per second
Mhz : Mega hertz
MIDP : Mobile Information Device Profile
MMAPI : Mobil Media API
MMC : Multi Media Card
NAM : Number Assigment Module
NMT : Nordic Mobile Telephone
NFC : Near Field Communication
OS : Operating System
PC : Personal Computer
PDA : Personal Digital Assistant
PIM : Personal Information Management
POP3 : Post Office Protocol 3
PPP : Point to Point Procotol
QVGA : Quarter Video Graphic Array
RAM : Random Acces Memory
RMS : Record Management System
ROM : Read Only Memory
SD : Secure Digital
SDK : Software Development Kit
SHA : Secure Hash Algorithm
SIM : Subscriber Identity Module
SMS : Short Message Service
SSL : Secure Sockets Layer
TACS : Total Access Communication System
TAPI : Telephony Applications Programming Interface
TCP/IP : Transmission Control Procotol / Internet Procotol
TIA : Telecommunication Industry Association
TLS : Transport Layer Security
UIQ : User Interface for Symbian OS
VGA : Video Graphic Array
VHE : Virtual Home Environment
VM : Virtual Machine
VoIP : Voice over IP
WAP : Wireless Application Procotol
WML : Wireless Markup Lenguage
XML : eXtensible Markup Language

1. GİRİŞ

1.1. 1G Birinci Nesil Telefon Teknolojisi

1G (veya 1-G) telefon teknolojilerinin ilk nesillerinin kısaltmasıdır. Bunlar 1980 yıllarında ortaya çıkan 2G sayısal telefonlar çıkıncaya kadar kullanılan analog tabanlı telefon teknolojileridir. 1G ve 2G mobil telefon sistemleri arasındaki en temel fark 1G şebekelerinin analog, 2G şebekelerinin ise sayısal radyo sinyalleri kullanmasıdır. Bununla birlikte 1G ve 2G şebekelerinin her ikisinde de cep telefonları baz istasyonları ile sayısal olarak haberleşmektedir. Tek fark baz istasyonlarının şebekenin geriye kalanı ile haberleşme için kullandığı teknolojidir. Fakat sadece 2G de ses tamamen sayısal olarak kodlanmaktadır.

1.1.1. NMT - Nordic Mobile Telephone

NMT (Nordic Mobile Telephone) Nordic Haberleşme Firması tarafından 1970'de ortaya atılan, mobil telefon ağlarına olan yoğun ihtiyaç ve talep sonucunda 1981'de hizmet vermeye başlayan bir mobil telefon sistemidir: Bu hizmeti ilk kullananlar Finlandiya'dan ARP (150 MHz) ve İsveç, Norveç ve Danimarka da hizmet veren MTD (450 MHz) şebekeleridir. NMT temeli anologdur (1G) ve iki türü bulunur: NMT-450 ve NMT-900. buradaki 450 ve 900 frekans bantlarını belirtmektedir. NMT-900 1986 çıkartılmıştır, çünkü kendisinden önce çıkan NMT-450 ağına göre daha fazla kanal taşıyabilir.

NMT'nin teknik prensipleri 1973 itibariyle hazırdı ve baz istasyonları için gerekli protokolleri 1977 yılında hazırlandı. NMT protokolleri bedava ve açık olarak yayınlanması sonucu pek çok firmanın NMT donanımı üretmesine izin verilerek maliyetlerinin aşağı çekilmesi sağlanmıştır. NMT'nin başarısı Nokia ve Ericsson'a ilham kaynağı olmuştur. Başlangıçtaki NMT telefonları tipik taşınabilir telefonlardı: kolayca taşınabiliyordu fakat daha çok arabada kullanıma uygun tasarlanmıştı. Sonradan çıkan modeller (Benefon gibi) 100 mm gibi küçük ve 100 gram gelecek kadar hafifti.

1.1.2. AMPS - Advanced Mobile Phone System

AMPS birinci nesil hücresel teknolojidir. AMPS FDMA teknolojisini kullanır. FDMA teknolojisinde yapılan her konuşma farklı kanallar kullanılarak bölünür. Bu yönüyle eski 0G IMTS hizmetine benzemektedir. Fakat, AMPS eski teknolojilerden üstündür. Çünkü cihazdaki arama yönetimi, güç yönetimi ve frekans yönetimi gibi çoğu işler bilgisayarlaştırılmıştır. AMPS "Hücre" teriminin babasıdır, çünkü sistemde küçük "hücre"ler kullanılmıştır. Bu hücreler AMPS'i başarılı yapandır, çünkü bu sistem frekansların tekrar tekrar kullanılmasını sağlamıştır, böylece sistemin farklı parçalarındaki insanlar birbirlerinin kullanımı engellemeden aynı frekansı kullanabilmişlerdir. Bu bir analog standart olduğundan dolayı gürültülere açıktı ve başkalarının dinlemesine karşı bir önlemi de yoktu. 1990 yılında, "kopyalama" sanayinin milyon dolarlar harcadığı bir salgındı. Kötü niyetli bir saldırgan özel bir donanımı ile cihazın NAM (Number Assignment Module) modülüne müdahale edebiliyordu. NAM mobil cihazdan şebekeye faturalandırma için gönderilen bir veri paketidir. Daha sonra sistem kendisindeki müşteri/cari dosyasına göre konuşmaya, diğer özelliklere izin verip/vermeyeceğini karar verir. Eğer NAM durdurulursa, başka bir telefona kopyalanabilir. Bu problem gittikçe

büyüdüğünden dolayı bir süre sonra aramalarda PIN kullanımı devreye girdi. Yine de sayısal teknolojilerle kopyalama mümkün olmasına rağmen kablosuz iletişim maliyetlerinin düşmesinden dolayı bu tür olaylar nerdeyse tamamen sonlandı. Daha sonra GSM ve CDMA gibi daha yeni teknolojiler AMPS'nin yerini almıştır.

1.1.3. CDPD - Cellular Digital Packet Data

Cellular Digital Packet Data (CDPD) normal olarak AMPS mobil telefonlarında kullanılmayan 800 ve 900 MHz bantlarını veri transferi için kullanır. İletişim 19.2 kbit/s hızına kadar çıkabilir.

1990 yılının başlarında geliştirilen CDPD geleceğin teknolojisi olarak görülmekteydi. Fakat o zamanda olan daha ucuz ve daha yavaş DataTac ve MobiTex sistemleriyle yarışmakta zorlanmıştır ve GPRS gibi daha yeni, daha hızlı sistemler baskın olana kadar da hala tam olarak yaygınlaşamamıştı.

CDPD kullanıcılarına sunduğu seçenekler oldukça kısıtlıydı. AT&T Wireless firması PocketNet adı altında bu teknolojiyi ilk kez Amerika'da pazara sundu. Pazardaki ilk kablosuz internet hizmetini sunmuşlardır. Cingular Wireless firması Wireless Internet adı altında pazara giren ikinci firma olmuştur. PocketNet kendisinden sonra gelen 2G hizmetleriyle kıyaslandığında genel olarak başarısız kabul edilmektedir. AT&T Wireless firması önceleri pazara üç tane telefon sunmasına rağmen daha sonra bu işten vazgeçmiştir.

1.1.4. DataTAC

DataTAC Motorola tarafından geliştirilen ve ilk kez Amerika'da ARDIS şebekesi tarafından kullanılan kablosuz ağ teknolojisidir. DataTAC 1990 yılı ortalarında Telecom Avustralya tarafından MobileData olarak pazarlanmıştır. Bu standart MobilTex gibi noktadan noktaya kablosuz veri iletişimi için açık standarttır ve özel uygulamalarda kullanılmıştır. Newton Messaging Card ilk DataTac cihazlarından birisidir, DataTac şebekesini kullanmak için bir PCMCIA karta bağlanan çift yönlü bir sayfalayıcıdır. Orijinal BlackBerry cihazlarından RIM 850 ve 857 de DataTac şebekesini kullanmışlardır.

Kuzey Amerika'da 800MHz bandını kullanan DataTac uygulanmıştır. DataTAC Telecom Avustralya tarafından da aynı bantta kullanılmıştır.

1.2. 2G İkinci Nesil Telefon Teknolojisi

2G ikinci nesil mobil telefon teknolojisidir. 1G teknolojisine benzer olarak hücresel bir ağ sistemi kullanır. Bu hizmet Türkiye'de Turkcell, Telsim ve Avea tarafından sağlanır.

2G ile 1G arasındaki en büyük fark analog veri yerine sayısal veri kullanılmaya başlanmış olmasıdır. Bu teknolojide ISDN'e benzer bir yapı kullanılmıştır:

Tüm cihazlar, bağlantı ve durum verilerini aynı kanal üzerinden yollarlar.

Bağlantı kurulduğunda, veri (veya ses) akışı bir kanal üzerinden yapılır. Her kullanıcı veri paketleri alıp verdiği sürece kanalı elinde tutar, paylaşmaz.

Avantajları

2G'nin sağlamış olduğu en büyük yenilik olan sayısal teknoloji, birçok yeniliği de beraberinde getirmiştir:

Daha yüksek ses kalitesi
Daha büyük kapasite
Sesi ve verileri şifreleme imkânı
Kısa veri iletimi (kısa mesaj, hücre bilgisi, v.b.)

Gelişmeler

İlk olarak 850-900Mhz bandını kullanmak üzere tasarlanan GSM, kullanıcı sayısının artmasıyla birlikte 1800-1900Mhz bandına taşınmıştır. Bazı şebekeler bu yeni banttan yayına DCS adı vermektedirler, ülkemizde ise genelde GSM1800 denir.

İnternet'in yaygınlaşması sonucu GSM'in sunduğu 9.6 kbps veri taşıma kapasitesi yetersiz olmaya başlamıştır. Buna cevap olarak:

HSCSD standardı çıkartılmıştır. Bu standart sayesinde, bir cihaz birçok kanalı aynı anda kullanarak 43.2 kbps'ye kadar veri iletişimi yapabilmektedir.

Öte yandan, HSCSD de benzer olarak GSM gibi veri iletilmediği zamanlarda bile hattı meşgul ettiği için şebekelere sorun çıkartmıştır. Bu karşılık olarak bandın sadece veri iletilirken kullanıldığı GPRS standardı çıkartılmıştır. GPRS'in veri yollama şeklinden yararlanan BasKonuş gibi özellikler de kullanıcı bütçesine katkısı dolayısıyla ilgi görmüştür.

Son olarak, GPRS'in hızını artırmak için GSM modülasyon tipi değiştirilerek EDGE teknolojisi oluşturulmuştur.

EDGE ile pratikte 380 kbps hızında veri transferi mümkündür.

Sorunlar

2G standardı çıktığı zaman çok bant genişliği ve az işlemci vardı, dolayısıyla hattı kullanmazken bile meşgul eden bir teknoloji oluşturuldu. Bununla birlikte, bu seçimden dolayı birçok durumda karşımıza çıkan "şebeke meşgul" mesajının önüne geçmek operatörler için gitgide daha çok zorlanmaktadır.

Buna da cevap olarak verilerin yollanmadığı zamanlarda, aynı Ethernet teknolojisinde olduğu gibi iki cihazın aynı anda veri yollayınca bunu fark edebildiği bir teknoloji olan 3G çıkartılmıştır. Özellikle Avrupa'da yaygınlaşmaya başlayan bu teknoloji, daha da yüksek bir bant kullanmasından dolayı (2100 Mhz) kapsama alanı sorunları yaşamaktadır.

1800Mhz GSM standardı ile ortaya çıkan ve 3G teknolojisinde de daha da belirgin olan kapsama alanı sorununu çözmek için 4G teknolojisi planlanmaktadır.

1.1.5. GSM - Global System for Mobile Communications

GSM sistemi, Avrupa'daki sivil el ve araç telefonu kullanıcılarını tek sistem altında toplamak amacıyla 1982 yılında CEPT (European Conference of Postal and Telecommunications Administrations) tarafından geliştirilmesine karar verilen hücresel ve sayısal bir sistemdir.

Yaklaşık 10 yılda ve milyarlarca dolarlık harcamayla oluşturulabilen GSM, 1987 yılında, 30 Avrupa ülkesi tarafından standart olarak kabul edilmiştir. İlk GSM standartları 1990 yılında yayınlanmıştır. Bir Avrupa standardı olarak başlamasına rağmen GSM kısa sürede dünyaca benimsenerek bir dünya standardı haline gelmiştir. A.B.D.'de bu standartların kullanılabilmesi için ANSI (American National Standards Institute-Amerikan Ulusal Standartlar Enstitüsü) devreye girmiş ve GSM standartları A.B.D.'de de yayınlanarak uygulamalarına başlanmıştır (Arslan, 2000).

Günümüzde kullanılan biçimi ile GSM sisteminin abonelerine sunduğu servis ve avantajlar şöyle özetlenebilir (Candan, 2002):

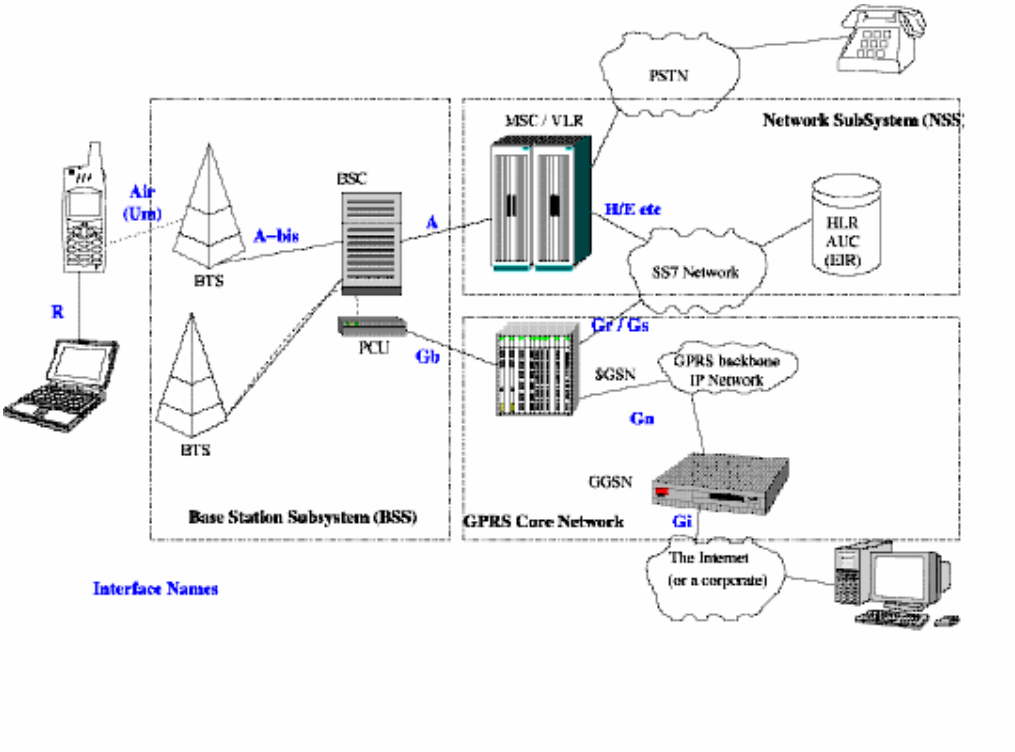
- Herhangi bir GSM şebekesinin abonesi, artık çoğumuz tarafından kullanılan küçük boyutlara sahip cep telefonuyla GSM sistemine dâhil olan ve kapsama alanı içinde bulunan bütün ülkelerde her yeri arayıp telefon görüşmesi yapabilmekte, nerede olursa olsun aranabilmektedir.
- Kullandığı telefonun kendisine ait olması gerekmemektedir, çünkü abonelik bilgilerini içeren SIM (Subscriber Identity Module- Abone Tanıtım Modülü) kartını yanında taşıması kiralayabileceği ya da ödünç alabileceği herhangi bir GSM el telefonunu kullanması için yeterli olacaktır.
- Ayrıca abone kendisine ait telefonu belirli çağrılara (örneğin daha pahalı olan uluslararası çağrılara) kapatabilmekte, erişilemediği ya da meşgul olduğu durumlarda çağrı yönlendirme özelliği kazandırılabilmektedir. Üstelik bütün bunları GSM sistemine özgü güvenlik önlemlerinin sağladığı gizlilik içinde gerçekleştirebilmektedir.

1990 yılında, GSM'in 1800 MHz'de çalışan bir türü olarak tanımlanabilecek olan DCS (Digital Cellular System - Sayısal Hücresel Sistem) 1800 sisteminin standartlarının belirlenmesine de başlanmış ve bu standartların tamamlanmasıyla 2x75 MHz'lik band genişliğinin kullanılmasının sonucu olarak belirgin bir kapasite artışı sağlanmıştır (Candan, 2002).

GSM, sayısal olması ve kullandığı radyo erişim teknikleri açısından birçok yenilikler getirmesine karşılık erişilen son nokta olmayıp, daha gelişmiş ve küresel sistemlere geçişi sağlayacak bir aşama olarak kabul edilmektedir. İkinci nesil GSM sistemlerindeki gelişmeleri, her biri daha hızlı veri iletimine imkan sağlayan HSCSD (High Speed Circuit Switched Data-Yüksek Hızda Devre Anahtarlamalı Veri), GPRS (General Packet Radio Service-Genel Paket Radyo Hizmeti) ve EDGE (Enhanced Data Rate for GSM Evolution -GSM Evrimi için Geliştirilmiş Veri Hızı) sistemleri izlemektedir (Çizelge 1.1).

Çizelge 1.1. Mobil Hizmetlerin Karşılaştırmalı Tablosu (Selian, 2001).

		Teknoloji	Bandgenişliği (Kbit/s)	Özellikler
1. Nesil (1G) Gezgin Sistemler	AMPS, NMT	Gelişmiş Gezgin Telefon Sistemi-(Advanced Mobile Phone System) Nordic Mobil Telefon-(Nordic Mobile Telephony)	9.6	• Analog ses hizmeti • Veri kapasitesi yok
2./2.5. Nesil (2G/2.5G) Gezgin Sistemler	GSM	Küresel Gezgin İletişim Sistemleri (Global System for Mobile Communication)	9.6 →14.4	• Sayısal ses hizmeti • Gelişmiş mesaj gönderme hizmeti • Evrensel dolaşım • Devre anahtarlamalı veri
	HSCSD	Yüksek Hızda Devre Anahtarlamalı Veri (High-Speed Circuit Switched) Data)	9.6 →57.6	• Gelişmiş GSM • Daha hızlı veri hızı
	GPRS	Genel Paket Radyo Hizmeti (General Packet Radio Service)	9.6 →115	• Gelişmiş GSM • Her zaman bağlantı imkânı • Paket anahtarlamalı veri
	EDGE	GSM Evrimi için Geliştirilmiş Veri Hızı (Enhanced Data Rate for GSM Evolution)	64 →384	• Gelişmiş GSM • GPRS'den daha hızlı
3.Nesil (3G) Gezgin Sistemler	IMT-2000, UMTS	Uluslararası Gezgin İletişim 2000 (International Mobile Telecommunications 2000), Evrensel Gezgin İletişim Sistemi (Universal Mobile Telecommunications System)	64 →2048	• Her zaman bağlantı imkânı • Küresel dolaşım • IP-olanağı



Şekil 1.1. Bir GSM Ağının Yapısı

GPRS - General Packet Radio Services

Telekomünikasyon endüstrisinde yıllar önce devre anahtarlamalı iletim modelinden paket tabanlı iletim servislerine geçişin en büyük temsilcisi olan GPRS aynı zamanda kullanıcılara gezgin çoklu ortam ile tanıştıracak olan üçüncü nesil gezgin internet sistemlerinin öncüsüdür. Devre anahtarlamalı (Circuit Switched-CS) bağlantı tarzında bağlantının kurulduğu bir noktadan diğerine sabit bir trafik kanalı tanımlanır. Konuşma veya veri bu kanal üzerinden akar. Paket anahtarlamalı (Packet Switched-PS) bağlantı tarzında ise devre anahtarlamalının aksine her bağlantı için adanmış bir hat tanımlanmaz. İletilmesi gereken veri paketlere ayrılır ve her bir paket kendisini ve gitmesi gereken yeri tanımlayan bilgiyi içerir. Bu paketler temel olarak yönlendiricilerin (routers) yardımıyla gidecekleri yere ulaşır. İnternet, paket anahtarlamalı bağlantı tarzının kullanıldığı en tanınmış örnektir. Aslında ortada gerçek zamanlı tanımlanmış bir hat yoktur ama kullanıcı kendisi için devre anahtarlama benzeri bir bağlantı yapıldığı yanılgısına kapılır. Bu kavram "sanal bağlantı" diye adlandırılır.

Paket anahtarlamalı iletim teknolojisi, gezgin veriler için birçok yeni uygulamayı ortaya koymuştur. Başlangıçta, paket anahtarlamalı teknolojinin doğasından kaynaklanan avantajlar doğrultusunda gelişen uygulamaların dışında yeni, makine-makine ve makine-insan arası iletişim olanakları da söz konusudur. Örneğin GPRS donanımlı kola veya sigara otomatları, tekrar doldurulmaları veya tamir edilmeleri gerektiğini merkezlerine bildirebileceklerdir (Şen, 2001).

Dünya üzerindeki tüm GSM operatörleri, bugünün teknolojik imkânlarından 12 kat daha hızlı bir şekilde, 115 Kbps ile gezgin kullanıcılara bağlantı kurma imkânı verebilecek GPRS'e yönelmişlerdir. GPRS yalnız gezgin olarak İnternet'e erişimi sağlamakla kalmayıp, bu erişimi sabit hatların kapasitelerinin çok daha üzerindeki veri iletim hızlarıyla sağlayıp 3G doğrultusundaki gelişim çizgisinin de hayati bir basamağı olmuştur (Buckingham, 1999).

GSM şebekesi üzerinde tek bir trafik kanalının yalnız bir kullanıcıya tahsis edilmesi, şebekenin en meşgul olduğu saatlerde trafiğin de yüklü olmasına neden olur. Fakat GPRS'in tek trafik kanalını birden fazla abonenin kullanımına olanak veren paket anahtarlamalı yapısı, şebeke kapasitesinin artmasına imkân vermekte, GSM standardının kullandığı devre anahtarlamalı yapıya göre avantaj sağlamaktadır. Bu, trafiğin yüklü olduğu saatlerde normal devre anahtarlamalı trafik bloke olurken, kısa GPRS paketlerinin aktarımının mümkün olacağını göstermektedir.

Yüksek hızda bir GPRS bağlantısının kurulma süresi sadece 1–2 saniye almakta ve yalnız bir kez yapılması yeterli olmaktır. Bu aşamada, son kullanıcı herhangi bir şebeke kaynağını kullanmadan sürekli hatta kalabilmekte ve kapasiteye ihtiyaç duyulduğunda erişim gecikmeleri ise yalnız birkaç yüz milisaniye almaktadır. GPRS ile her zaman bağlantı halinde kalmak, ucuz ve çok hızlı bir gezgin erişim imkânına kavuşmak mümkün olacaktır. Maliyetler açısından bakılacak olursa, GPRS'in bir paket teknolojisi olması hem operatörler hem de kullanıcılar için daha verimlidir (Candan, 2002).

GPRS teknolojisi fiyatlandırmayı bağlantı süresiyle değil, gönderilen ve alınan veri miktarı üzerinden hesaplamaktadır. Böylece abone yalnızca alıp gönderdiği veri miktarı

kadar ödeme yapmaktadır. GPRS ayrıca 9.6 Kbps olan veri iletim hızlarını 115 Kbps gibi çok yüksek seviyelere çıkartabilmektedir. Paket veri servislerinin kullanımı ile aboneler her zaman ucuz ve hızlı bağlantı halinde olmaktadır (Anonim, 2001b).

GPRS, diğer tüm teknik üstünlüklerini yanında sahip olduğu iki önemli karakteristik özellik ile de dikkate değerdir. GPRS;

- Kablosuz iletişim ağlarının, bireylerin ve kurumsal kullanıcıların hizmetine sunulacak olan çeşitli türlerde ve çok sayıda Gezgin İnternet uygulamasını destekleyecek şekilde ilerleme göstermesi,

- Kullanıcıların gezgin iletişim deneyimlerini gezgin çoklu ortam ve görüntü akışı (video streaming) gibi canlı öğelerle süsleyecek olan 3G'ye uzanan yolda bir dönüm noktası olmasıdır (Anonim, 2001c).

GPRS'in en önemli özelliği, var olan GSM şebekelerine hızlı ve basit bir şekilde bütünleşmesi sağlanabilmesidir. Şu anki gezgin şebekenin temelini oluşturan GSM yapısı bozulmayacak, GPRS veri iletimi uygulamalarında görev almak üzere mevcut şebekedeki yerini alacaktır. Böylece GPRS teknolojisi kurulan şebekelerde, konuşma amaçlı görüşmelerde yine GSM kaynakları dâhilindeki devre anahtarlamalı yapı, veri iletimi esnasında ise daha yüksek veri iletim hızları sunan paket anahtarlamalı yapı kullanılacaktır. GPRS'in altyapıda kurulmasıyla birlikte 3G gelişimi yolunda bir diğer önemli adım olan EDGE teknolojisini destekleyecek altyapı da hazırlanmış olacaktır (Gihribi ve Logrippo, 2000).

GPRS özellikli son kullanıcı cihazlarının maliyetleri pazarın da büyümesiyle hızla düşecek ve birkaç yıl içerisinde gezgin internet erişimi ciddi boyutlarda gerek maliyet gerekse veri iletim hızları yönünden sabit hatlarla rekabet eder hale gelecektir (Anonim, 2001d).

1.1.6. HSCSD (High-Speed Circuit-Switched Data)

1998 yılında, veri iletim hızını arttırmak amacıyla devre anahtarlamalı veri kapasitesine sahip mevcut 2G GSM şebekelerinin gelişmiş bir uygulaması HSCSD yapısı oluşturuldu. HSCSD kullanımı ile 57.6 Kbps hızına kadar veri iletimi gerçekleştirmek mümkündür. Bu sayede, GSM terminal cihazları ile video konferans, çoklu ortam uygulamaları gibi gelişmiş hizmetleri almak mümkün olacaktır.

HSCSD'nin kurulumunun kolay ve maliyetinin düşük olmasının nedeni, sadece baz istasyonlarının yazılımlarının yenilenmesinin yeterli olmasının yanı sıra yeni bir donanıma gerek olmamasıdır. Bununla birlikte, veri trafiğinin artması ile birlikte ses kapasitesi azalmaktadır. Böylece veri kullanıcılarının, kanal kullanımı için ses kullanıcıları ile yarışmaları gerekecektir. Bu nedenle, HSCSD'nin çoğunlukla kapasitenin boş olduğu ya da yeni şebekelerde kullanılabileceği düşünülmektedir (Sung ve ark., 2001).

1.1.7. EDGE (EGPRS) - Enhanced Data Rates for GSM Evolution

3G sistemlerine doğru giden yolda en son adımı oluşturan EDGE, UMTS (Universal Mobile Telecommunications System - Evrensel Gezgin İletişim Sistemi) lisansı alması zor olan veya alamamış gezgin şebeke operatörlerinin yararlanması amacıyla

geliştirilmiştir. EDGE, GSM operatörlerine, UMTS şebekeleri üzerinde sunulan servislere yakın hızlarda hizmet sunma olanağı vermektedir.

Aynı zamanda EDGE, daha sonra UMTS kullanımında gerekli olacak modülasyon değişikliklerini şimdiden yaparak, GSM'den UMTS'e geçiş sürecinde de yardımcı olacaktır.

Şebeke operatörleri tarafından EDGE, kurulumu basitçe gerçekleşecek şekilde tasarlanmıştır. Sadece bir EDGE verici biriminin her hücreye eklenmesi gereklidir. Birçok üreticinin de tahmin ettiği, BSC (Base Station Controller - Baz İstasyonu Kontrol birimi)'lerde ve baz istasyonlarında çok az yazılım yenilenmesinin gerekli olacağıdır. Yeni EDGE vericileri, standart GSM trafiğini taşıyabilecekleri gibi gerekli durumlarda vericiler otomatik olarak EDGE kipine anahtarlanacaklardır.

Mevcut GSM terminalleri yeni modülasyon tekniğini desteklemediğinden, EDGE şebekesinin fonksiyonlarından yararlanabilmek için değiştirilmeleri gerekmektedir. Bazı EDGE uyumlu terminal cihazlarında sadece veri alma konumunda yüksek hızlı veri hızlarını destekleyecek şekilde tasarlanmıştır (yüksek hızda veri alınabilmekte fakat gönderilememektedir). Diğer terminal türlerinde ise hem veri gönderme hem de veri alma durumunda EDGE erişimi sağlanacaktır (yüksek hızda veri alınabilmekte ve gönderilebilmektedir). Gelecekte kullanılacak cihaz türlerinde hem alıcı hem de verici kısımlarında büyük oranda terminal modifikasyonuna gerek duyulacaktır (Anonim, 2001b).

EDGE kullanımına başlanması, teknolojisinin büyük oranda GSM temelli olması nedeniyle operatörlere yatırım açısından çok büyük külfet getirmemektedir. EDGE çekirdek şebeke ve hücre kaplama açısından mevcut GSM mimarisi ile uyumludur. EDGE teknolojisinde 384 Kbps veri hızına ulaşılmıştır (Aksu, 2004).

Analistler, 3G'nin pazara yerleşmesi ile birlikte küresel rekabet ortamındaki taşların yerinden oynayacağını belirtmektedir. 1995'ten beri uzanan internet dalgasının değişime ayak uydurmakta güçlük çeken pek çok şirketi sarsması ve yeni fırsatların önünü açması gibi, kablosuz Web'de yenilikçi ve rekabetçi bir pazarın gelişmesine öncülük edecektir. Sesli iletişimden elde edilen gelirlerin düşmesi, Telekom operatörlerini daha yüksek kazanç sağlamayı umdukları veri servisleri üzerine yoğunlaşmaya itmektedir (Aksu, 2004).

Avrupa'da son zamanlarda birçok şirket, yüksek hızlı üçüncü nesil kablosuz hizmetleri taşıyacak 3G iletişim platformlarının haklarını alabilmek için yüz milyar dolardan fazla para harcadılar. İşin şaşırtıcı yönü 3G'nin getireceği yeni iş fırsatlarının sadece telekom operatörlerinin ya da taşıyıcıların değil başka kategorilerdeki oyuncuların da iştahını kabartacak olmasıdır (Aksu, 2004).

1.3. 3G Üçüncü Nesil Telefon Teknolojisi

3G gezgin iletişim teknolojisine yönelik standartlar, ITU (International Telecommunication Union - Uluslararası Telekomünikasyon Birliği) tarafından geliştirilmekte olup, topluca IMT–2000 olarak adlandırılmaktadır. "IMT", "Uluslararası Gezgin İletişim"i (International Mobile Telecommunication); "2000" ise hem bu alanda

geliştirilmiş ilk deneme sistemleri için belirlenmiş tarihi, hem de bu standartlardaki sistemlerin çalışacağı öngörülen 2000Mhz civarındaki frekans bölgesini temsil etmektedir (Yanık, 2001).

3G hizmeti ile ilgili gelişmeler standardizasyon, altyapı çalışmaları, şebeke denemeleri, anlaşmaların yapılması, terminal cihazlarının piyasaya çıkarılması, uygulamaya yönelik gelişmeler v.b. konuları içermektedir. Bu evreler Çizelge 1.2'de gösterilmektedir.

Çizelge 1.2. Üçüncü Nesil (3G) Gelişim Süreci (Candan, 2002).

Tarih	Kilometre taşı
1999 süresince	3G telsiz ara yüz standartları belirlendi ve ilk 3G canlı altyapı ve terminal tanıtımı yapıldı.
2000	Şebeke yapısı, terminal gereksinimleri ve standartlarla ilgili çalışmalara devam edildi.
Mayıs 2000	ITU Radyokomünikasyon Topluluğunda IMT–2000 Tavsiyelerinin resmi onayı yapıldı.
2000	Avrupa ve Asya'da hükümetler tarafından 3G lisansları verildi.
2001	3G hizmetleri ile ilgili denemelere başlandı.
2001	Japonya'da NTT DoCoMo tarafından 3G servisleri hizmete sunuldu.
2001 Yazı	Avrupa'da 3G hizmetlerinin ilk denemesi yapıldı.
2002 başı	İlk 3G uyumlu terminaller piyasaya sürüldü.
2002 süresince	Operatörler ticari olarak 3G hizmeti sunmaya başladı.
2002/3	Yeni 3G uygulamalarının hizmete sunulması, şebeke kapasitesinin artması, daha fazla uyumlu terminal cihazının piyasaya sürülmesi
2010	3G'nin ticari açıdan önemli bir seviyeye ulaşacağı öngörülmektedir.

3G teknolojisinin getirileri:

1. Hızlı erişim,
2. Paket anahtarlama ve isteğe bağlı hız,
3. VHE (Virtual Home Environment - Sanal Ev Ortamı),

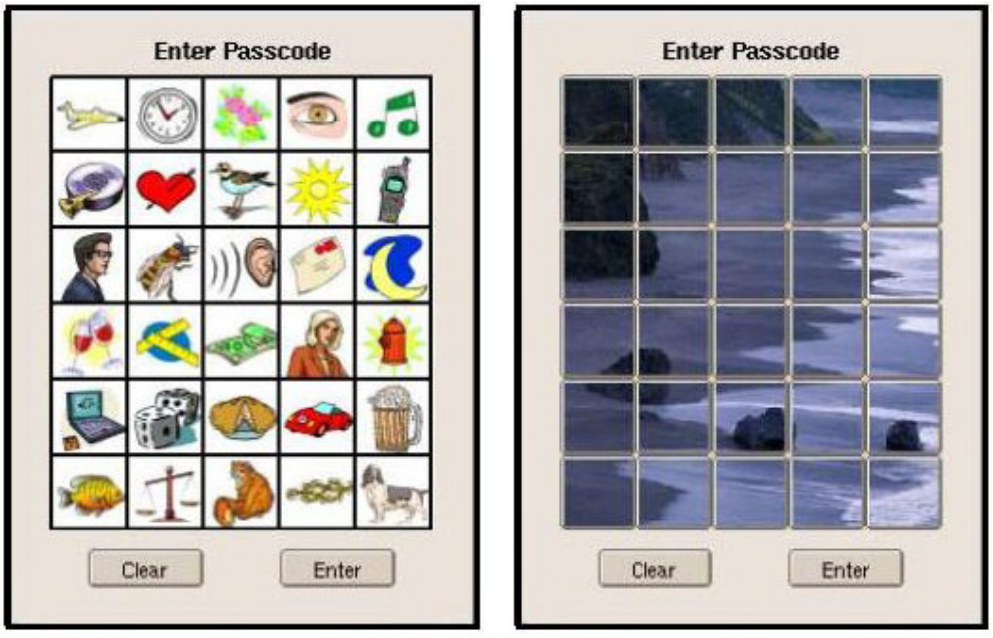
3G teknolojisi ile kullanıcıya hareket halinde iken sesin yanı sıra veri, resim, grafik ve benzeri bilgilerin 2 Mbit/s hızına varan yüksek hızlarda, başka bir deyişle "geniş bantta" iletilebileceği daha önceki bölümlerde açıklanmıştır. Halihazırda kullanılmakta olan veya çok yakın bir gelecekte kullanılması planlanan GSM standartlarındaki sistemler ise, ancak 9.6 ile 384 Kbit/s arasındaki hızlarda bilgi aktarımına izin vermektedir (Yanık, 2001).

2.ÖNCEKİ ÇALIŞMALAR

Daha önce güvenli girişlerin olduğu yerler için geliştirilmiş yüz tarama, retina tarama ve/veya ses tanıma çalışmaları oldukça mevcuttur. Ve bu uygulamalar %97 varan doğrulukla çalışabilmektedir. Ancak bu uygulamaların cep telefonu üzerinden yapılması gibi bir çalışma eksikliği göze çarpmaktadır.

Pantelis ve Konstantinos (2004), Akıllı telefon tabanlı tele-radyoloji sistemi adını verdikleri çalışmalarında mobil cihazlar kullanarak bir hastanın filmlerini uzaktan görüntüleme ve işleme yapılmasını sağlayan bir uygulamayı geliştirmiş ve incelemişlerdir. Uygulama güvenliği için var olan GSM güvenliğine ve hedef sunucuya bağlanma sırasındaki kimlik doğrulama sitemlerine güvenmişlerdir. Ancak bu çalışmada özel bir iletişim güvenliği konusu açıkta kalmıştır.

Jansen (2004), Resim Seçme yolu ile Mobil kullanıcılarda Kimlik Doğrulama (Authenticating Mobile Device Users Through Image Selection) adlı çalışmalarında; kimlik doğrulamanın sürekli bir problem olduğundan bahsetmişlerdir. Özellikle uygulama alanı olarak mobil cihazlardan PDA'yı seçmişlerdir. Çünkü PDA geniş kullanıcı etkileşim seçenekleri, renkli ve geniş ekranı ve kullanım kolaylığı gibi özellikleriyle ön plana çıkmış bir cihazdır. Ve bu cihazlar askeri ve kamu ajanslarında, hastanelerde ve banka gibi kritik yerlerde kullanıldıklarından üzerlerinde taşıdıkları önemli bilgiler yanı sıra bu cihazlarla uzaktan bağlantı yapıldığından güvenlik ön plana çıkmaktadır. Kimlik doğrulama yetkisiz kişilerin eline geçen bir mobil cihaz için ilk karşılaşacağı güvenliktir. Güvenlik için basit PIN ve parolalar kullanmak ve bunların sürekli güncellenmesini istemek zorluklar çıkartmaktadır. Jansen'ın yaptığı bu çalışmada kullanıcıların resim seçme ile kimlik doğrulaması yapması sağlanmıştır. Bu işlemin temelindeki fikir; insanların resimleri anlamsız metinlerden daha kolay hatırda tutabilmesi ve hatırlamasıdır.



Şekil 2.1. Resim Tabanlı Güvenlik Doğrulaması

Perrig ve Song (2000), Hash Visualization adını verdikleri çalışmalarında şuan ki güvenlik sistemlerinde temel problemin insan faktörünü yeterince hesaba katmamalarından dolayı şifre unutmalarını engelleyerek hem daha güçlü şifreler kullanmalarını ve bunları kolay hatırlayabilmek için yapısal resimlerden faydalanmışlardır. Kullanıcının bir sisteme giriş yapacağı zaman kendisine sunulan resimlerden uygun bir resim serisi girmesi istenerek kimlik doğrulanması yapması istenmektedir.

Yuliang Zheng (2004), GSM de Güvenlik Artırımları (Enhancing Security in GSM) adlı çalışmasında var olan GSM güvenlik sistemlerindeki zayıflıklardan bahsedip daha iyi bir güvenlik sistemi önermişlerdir. Bu önerilen sistem; doğrulama merkezi (AUC – Authentication Center) ile mobil istasyonu (MS – Mobile Station) arasında her bir arama için oturum anahtarı dağıtım protokolü sağlamaktadır. Bu protokol sayesinde hem mobil istasyon hem de şebeke tarafında karşılıklı doğrulama sağlamaktadır. Var olan sistemler için kullanılan A5 şifreleme algoritmasından daha güçlü bir algoritma önerilmiştir. Ve böylece GSM PLMN (Public Land Mobile Network – Genel Mobil Kapsama Alanı) üzerinde açıkça IMSI (International Mobile Subscriber Identity – Uluslar Arası Mobil Abone Kimliği) taşınmasına son vermiştir.

Özçelik (2006), Bluetooth Üzerinde Güvenli Veri İletimi adlı çalışmasında; Bluetooth iletişim ortamının kablosuz olması ve ortamın tüm kullanıcılara açık olması sistemde güvenlik açıkları meydana geldiğini belirtmektedir. Bu nedenden ötürü kablosuz ağ ortamı olan bluetooth'a özgü güvenlik protokol ve yöntemleri geliştirilmektedir. Yapmış olduğu çalışmada bluetooth teknolojisi sisteminin yapısı açıklanmış, kullandığı güvenlik yöntemlerini incelenmesi, sistemin güvenlik açıkları tespit edilmeye çalışılmıştır. Sistemi daha güvenli hale getirmek için güvenlik mekanizmalarının nasıl geliştirilmesi gereği üzerinde durulmuş ve yeni yöntem uygulanmıştır. Bu çalışmada DES algoritması kullanılarak anahtar tabanlı şifreleme bluetooth üzerinde uygulanmıştır.

3. MATERYAL VE METOD

Bu bölümde çalışmayı gerçeklerken kullanılacak metot ve materyalle ilgili bilgilere yer verilecektir.

3.1. MATERYAL

Mobil güvenlik ile ilgili bir çalışma hem istemci (mobil cihazlar) hem de sunucu tarafı programlama, donanım fizibilitesi anlamında çalışma gerektirir.

İstemci tarafında uygulama geliştirme ortamları, uygulamanın taşınabilirliği, olabildiğince tüm cihazlara uygulanabilirliği, güvenlik kavramı, güvenlikle ilgili sorunlar ve çözümleri, uygulamaların yaygınlığı gibi çok çeşitli parametreler ortaya çıkar.

Sunucu tarafında ise dikkate alınması gereken noktalar aynı anda çok sayıda mobil cihaza destek verebilecek donanım konfigürasyonu, sunucu tarafı yazılımların çeşitli türdeki mobil cihazlara destek verebilmesi, sunucu güvenliği gibi farklı yönlerin dikkate alınmasını gerekli kılar.

Mobil cihaz uygulamaları için Java yazılımı, mobil cihazların çoğunu test edebilmek için ilgili cihazların emülatörleri uygun çalışma ortamını sağlar.

Sunucu tarafı uygulama güçlü bir masaüstü bilgisayar, asp. net veya jsp gibi sunucu teknolojileri etrafında şekillenir.

3.1.1. Mobil Cihazlar Ve Mobil Cihazların Kullandığı Referans Teknolojiler

Cep telefonları ve PDA tabanlı cihazlar genel olarak mobil cihazlar olarak tanımlamaktayız. Notebook veya dizüstü sistemeler taşınabilir olmalarına rağmen farklı bir teknoloji çerçevesine işaret ettiklerinden dolayı bu bölümde incelenmeyeceklerdir. Cep telefonları fiziksel görünümlerinin yanında yeni teknolojilerle zenginleşirlerken, PDA (Personal Digital Asistant-Kişisel Dijital Asistan) tabanlı cihazların yeteneklerini de bünyelerinde barındırarak melez cihazlar olarak ortaya çıktılar. Klasik cep telefonları sınırlı bir işletim sistemine sahip iken, akıllı telefon (smartphone) adı verilen cihaz teknolojisi bu cihazlar için üretilmiş ve kapsamlı işlevleri barındıran işletim sistemlerini beraberinde getirmiştir. Bu tür cihazlar, mp3 dinlemekten, ebook adı verilen kitapları okumaya dek çok geniş bir platformdaki ihtiyaçları bir arada sunmak şeklinde ciddi çoklu ortam ihtiyaçlarına tek bir cihazla cevap vermektedir.

Cihazlar genişleyen hafızaları, artan mikroişlemci güçleri, çözünürlüğü artan güçlü ekranları ve gittikçe azalan ağırlıklarıyla çok ciddi bir tüketici grubunun ihtiyaçlarına cevap verecek bir yapıya kavuşmuşlardır. Üstelik çok sayıda farklı firmanın piyasaya sunmuş olduğu alternatif ürünler çeşitliliği arttırarak bu tarz çokluortam cihazların yaygınlaşmasını hızlandırmıştır.

Mobil cihazlar çok sayıda işlevi üstlenmeye hazırlanırlarken tüm bu teknolojilerin ve cihazın giriş çıkış birimlerinin yönetimi için sofistike işletim sistemleri gerekmiştir.

Cep telefonu (günümüzde cep telefonlarıyla tümleşik bir hale gelmiş PDA türü cihazları ayrı bir sınıfta incelemek yerine artık cep telefonlarıyla tümleşik olarak düşüneceğiz) teknolojileri birinci nesil, ikinci nesil ve üçüncü nesil vb. cihazlar şeklinde sınıflandırılan teknolojileri göre sınıflandırılmışlardır. Cep telefonlarının hızlı gelişim sürecini aşağıdaki şekille özetlemek mümkündür.

Şekil 3.1. Gezgin Telefonların Gelişim Süreci (Helin, 2002)

Cep telefonlarının gelişim sürecinin hızı dikkate alındığında artık birinci ikinci nesil cep telefonlarından burada bahsedilme gereği duyulmamaktadır. Ancak basit bir ifade ile önceleri iletişim ekseninde piyasaya-tüketime sunulan cep telefonları ikinci-üçüncü nesilde eğlence ve diğer kişisel kullanım teknolojileri ile yüklenmiş olarak ortaya çıkarlar. Günümüz açısından yaygınlık düzeyi ve günümüz standardı dikkate alındığında üçüncü nesil cep telefonlarını incelersek, bu cep telefonlarında WAP, Bluetooth, IrDA (Infrared Data Association) gibi iletişim teknolojilerinin artık bir standart haline geldiğini gözleriz. Bu iletişim teknolojileri çokluortam teknolojileri (gelişkin kamera ve audio-video yetenekleri) ile zenginleşerek, kullanıcılarına neredeyse bir dizüstü bilgisayar sisteminin konforunu sunmaya adaydırlar.

Üçüncü nesil cep telefonları eski teknolojilere göre kullanıcısına daha fazla yeni ve kullanılabilir teknolojinin yanında daha fazla cihaz hâkimiyeti sunar. Kullanım kolaylığının artması (arayüz yazılımlarında ve donanımdaki iyileştirmeler) cep telefonlarının kulanım alanlarını ve bu tür cihazlar için üretilen ek donanım-yazılım teknolojilerinin gelişim sürecini ciddi bir dinamizm sürecine sokmuştur.

Çoklu ortam özelliğine sahip ilk cep telefonları kendilerine halen piyasada ciddi şekilde kullanım alanı bulan ve ciddi birer standart-klasik olarak yer alan Nokia 6600, SonyEricsson P800/900, Motorola MPx Serisi telefonlar sayılabilir.

3G özelliklerine sahip bu telefonlardan bazıları aşağıdaki şekilde gösterilmiştir.

Şekil 3.2. Bazı 3G Cihazları (Anonim, 2004a).

3G cihazlarına ait teknolojiler yaygın şekilde kullanılırlarken iletişim teknolojileri kendini 4G'ye hazırlamaktadırlar. Bu teknolojilerin ve bu teknolojileri kullanan mobil cihazların birkaç sene içinde dünyanın hemen hemen her tarafında kullanılabilir hale geleceği öngörülmektedir.

3.1.1.1. Mobil İletişim Teknolojileri, Wap, Irda, Bluetooth

Mobil iletişim teknolojilerindeki, iletişim zenginliği ve çeşitliliği için yapılan araştırmalar meyvelerini WAP, Irda ve Bluetooth sürecindeki teknolojiler ile vermiştir.

WAP (Wireless Access Protocol) metin tabanlı bir iletişim protokolü olup yavaş ve yüksek iletişim hızlarına müsaade etmeyen bir protokoldür. Bu protokolü kullanan uygulamalarda bu eksende metinsel uygulamalar şeklindeydi. WAP teknolojilerinin en büyük handikapı tatmin edici bir iletişim hızı sağlayamazken bir de karmaşık ayarlamalar yapmayı gerektirmekteydi (Aksu, 2005). Muhtemelen, bu nedenlerden dolayı WAP

teknolojisi ile uğraşılarak onun yeterli hale getirilmesi yerine teknoloji başka bir şekilde yön değiştirerek yeni bir mecraya kavuşacaktır.

Mobil cihazlar arasında veri aktarımı-paylaşımı için geliştirilen teknolojilerden birisi olan kızılötesi iletişim kısa mesafe, düşük veri aktarım hızları ve iletişim kuran cihazların birbirini mutlaka görmesi gerekliliğinden dolayı çok kullanışlı bir teknoloji sayılmamaktadır. Bu teknoloji ile çok küçük boyutlardaki verilerin alış verişi mümkün olmakla birlikte kızıl ötesi iletişim birlikte günümüz telefonlarında yerini çok daha etkin olan Bluetooth kablosuz teknolojisine bırakmıştır.

Yeni bir iletişim teknolojisi olarak, Bluetooth, sabit ve taşınabilir cihazların, birbirlerine kablo ile bağlanmadan ve cihazların birbirlerini direkt olarak aynı düzlemde görmelerine gerek kalmadan haberleşmesini sağlayan bir evrensel standarttır. Ses ve veri iletişimini oldukça kolaylaştıran Bluetooth yetenekli cihazlar ortalama 10-100 metre mesafelerde radyo frekansları aracılığı ile haberleşebilirler.

3.1.1.2. Yeni Nesil Çoklu Ortam Mobil Cihazların Genel Özellikleri

Çoklu ortam ya da çokluortam mobil cihazlar, genel olarak işletim sistemleri, ekran büyüklükleri, destekledikleri medya formatı, destekleyebildikleri genişleme yuvaları ve bellkeleri gibi kriterler etrafında benzeşirler. Bu bölümde bahsi geçen kriterleri 3G cihazlarını baz alarak inceleyebiliriz:

Cep telefonlarında genel olarak ya bir Symbian türevi işletim sistemi ya da Microsoft Windows tabanlı bir işletim sistemi kullanılmaktadır. Yakın zamanlarda bu işletim sistemlerine Linux işletim sistemi türevleri de eklenmiştir. Symbian işletim sistemi kendini genel olarak kararlı ve çokluortam desteği üst düzey bir işletim sistemi olarak gösterir. Bu işletim sistemi piyasaya giren ve akılı telefon olarak bilinen çoğu çokluortam mobil cihazının standart sistemi olarak ortaya çıkmış ve bu nedenle de çok sayıda uygulama-yazılım desteği elde etmiştir.

Linux ve Microsoft'un cep telefonları veya mobil cihazlar için kullandığı işletim sistemi henüz gelişme aşamasında olmakla birlikte özellikle Microsoft bu alana ". NET Teknolojileri" üzerinden ciddi yatırım yapmakta ve piyasada ciddi yer tutacağı izlenimi vermektedir.

Çoklu ortam cihazlarındaki bir diğer ön plana çıkan özellik ekranın boyutu, çözünürlüğü ve renk derinliğidir. Cihaz boyutunu ve ağırlığını arttırmadan ekran boyutu ve kalitesi yüksek cihazlar ötekilere göre daha çok tutulmaktadır. Çokluortam uygulamaları ister istemez video-audio uygulamalarını, ebook tarzı kitap, dergi okuma beklentilerine cevap vermelidir. Bu nedenle yüksek çözünürlüklü, daha fazla renk desteğine ve parlak ekrana sahip modellere piyasadan ciddi talepler gelmiş ve bu istekler firmaları çokluortam destekli cep telefonları konusunda oldukça cesaretlendirmiştir.

Mobil telefonların uygulamaları çalıştırma performansı yine önemli bir seçim kriteri olarak ortaya çıkar. Bu tür cihazlarda, diğer tüm elektronik cihazlarda olduğu gibi performans kullanılan işlemci, hafıza gibi donanım yapısıyla yakından ilgilidir. Çünkü işletim sisteminin uygulamalara erişim-çalıştırma hızı bu faktörlerle çok yakından ilgilidir. İster istemez güncel ürünler bir zamanlar masaüstü sistemlerinde bile çok büyük kabul

edilen 64-128 MByte gibi hafızalar ve genişletilebilir (dahili-harici) yapılarla ortaya çıkmaktadırlar.

Çokluortam fonksiyonları arasında en gözde özellikler video-audio fonksiyonları olsa gerektir. Neredeyse Ipod ve benzeri ses dosyası çalan cihazların kalitesini, taşınabilir VCD-DVD player özelliklerini içinde barındıracak derecede sofistike ve kaliteli mobil cihazlar bu iki önemli özelliği tek bir cihazda birleştirerek piyasada yoğun bir talebin oluşmasına neden olmaktadırlar. Bu özeliklerin aktif kullanımı çok büyük boyutlardaki dosyaların yönetimi, organizasyonu ve saklama (genişletilebilir hafıza üniteleri) gibi isteklere cevap verilmesini gerekli kılmaktadır (Aksu, 2005).

Çokluortam telefonların destekledikleri genişletilebilir hafıza ve genişleme yuva standartları dikkate alındığında SD (Secure Digital) ve MMC (Multi Media Card) kart türleri bahsi geçen ihtiyaca cevap vermektedirler. Bu kartların veri depolama hızları artışın yanında 2-5 GByte boyutlarındaki hafızalar ile dikkati çekmektedirler.

Son olarak resim tabanlı güvenlik uygulamalarının da ilham kaynağı olan ve cep telefonlarına eklenen dijital kameralar, çok ciddi kaliteleriyle neredeyse orta ölçekli dijital kameralarla başa çıkacak derecede kaliteli bir mimariyle gelmektedirler. Hafıza kartlarının sakladığı veri miktarları göz önüne alındığında binlerce kaliteli resim ve saatlerce video kaydı yapabilen mobil çokluortam cihazları günümüzün birer gerçeği olarak ortada durmaktadırlar.

3.1.1.3. Çoklu Ortam Cihazlarında Kullanılan Yazılımlar

Çoklu ortam mobil cihazlardaki (hem cep telefonlarında hem de PDA'larda) gelişkin özelliklerin (film seyretme, mp3 yükleme, dinleme, birçok resim formatını görüntüleyebilme, mikro programlama dilleri ile yazılmış uygulamaları çalıştırma, görsel oyunları yükleme, oynama) yönetilebilmesi çalıştırılabilmesi, cihaz ile kullanıcı arasında bir arayüz gerektirir. Tüm bu işlemlerin gerçekleştirilmesi için daha önce kısaca bahsedilen işletim sistemlerine ihtiyaç duyulmaktadır. Mobil cihazlara yüklü işletim sistemlerinden en yaygın olarak kullanılanları Symbian OS, Windows CE/ Pocket PC, Palm OS, Pocket Linux işletim sistemleridirler (Aksu, 2005).

i)Symbian İşletim Sistemi: 32-Bitlik bir işletim sistemi olan Symbian, maliyeti düşük ve güç tüketimi az olan mobil cijazlar için tasarlanmış bir işletim sistemidir. Açık bir sistem olan Symbian, bu avantajı ile üzerinde en çok program-uygulama geliştirilen bir işletim sistemi konumundadır. Açık ortam yapısıyla 2G, 2.5G ve 3G mobil telefonlara ciddi şekilde gelişim desteği sunan bu sistemin en temel ön plandaki özellikleri şunlardır:

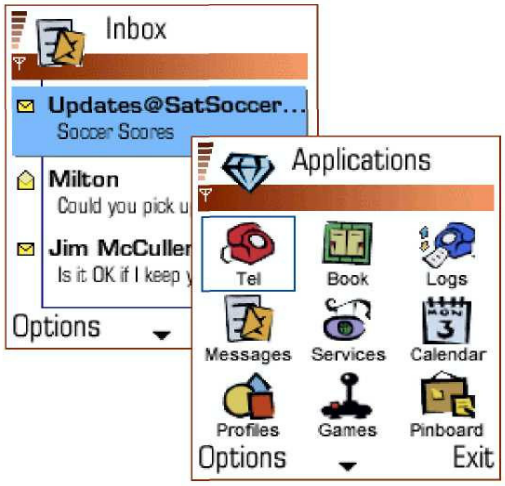
- Açık uygulama geliştirme ortamı
- Çok görevlilik (Multitasking)
- Esnek kullanıcı ara yüz tasarımı
- Tam nesne ve bileşen tabanı
- Sağlamlık
- Standartlar ve birlikte işlerliğe açık
- Çok kipli gezgin telefonlarla tümleşiktir

Mobil cihaz piyasasında Symbian OS lisansını kullanan bazı firmalar arasında belli başlı firmalar, Nokia, Siemens, Fujitsu, Samsung, Motorola, BenQ, Panasonic, LG gibi firmalar yer almaktadır.

Symbian işletim sistemi günümüzde kullandığı arayüzler anlamında geleneksel olarak iki türde GUI sunar. Symbian'ın kullanıcı arabirimi olarak sunduğu bu iki referans tasarım, UIQ (Dokunmatik Ekranlı Sony Ericsson cihazlarındaki tarz) ve Series 60 (Nokia ve benzeri firmaların telefonlarında kullandıkları arayüz) olarak bilinirler (Şekil 3.3).

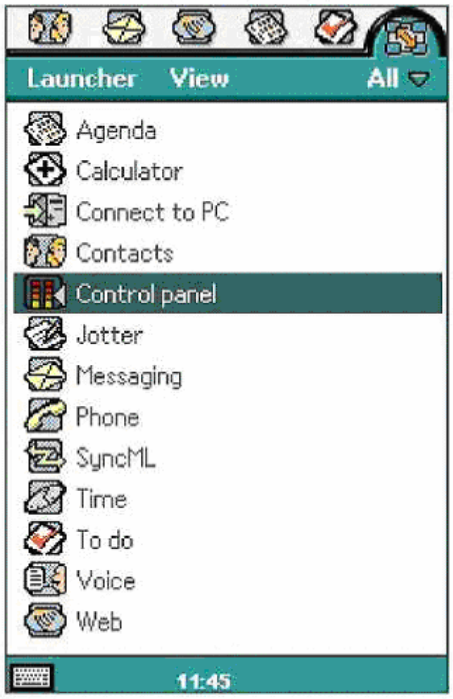
Series 60 arayüzlü Symbian'lar smartphone olarak bilinen akıllı telefonların gelişmiş yönetimsel ihtiyaçlarına cevap veren yazımlardır. İlk olarak Nokia tarafından kullanılan bu yazılım sonraki dönemlerde Siemens ve Panasonic gibi firmalar tarafından da kullanılmışlardır (Şekil 3.5).

Desteklenen donanım yapısı göz önüne alındığında Symbian işletim sistemi ARM tabanlı platformlarda çalıştırılmak üzere tasarlanmıştır. ARM yaygın olarak kullanılan gömülü RISC (Reduced Instruction Set Computer) işlemcisi ve mikro kontrol ailesindendir. ARM şirketi tarafından tasarlanıp üretilmiştir. ARM720T ve ARM9E Symbian işletim sistemi yüklü cihazlarda kullanılan tipik işlemci türleridir. Bu işlemcilerin her ikisi de güçlendirilmiş ön bellek, bellek kontrol ünitesi ve çevre birimlerini kontrol etmek için esnek bir veri yolu sunar. Çekirdekler, maliyet ve güce duyarlı uygulamalar için en iyi şekilde optimize edilmişlerdir (Aksu, 2005)



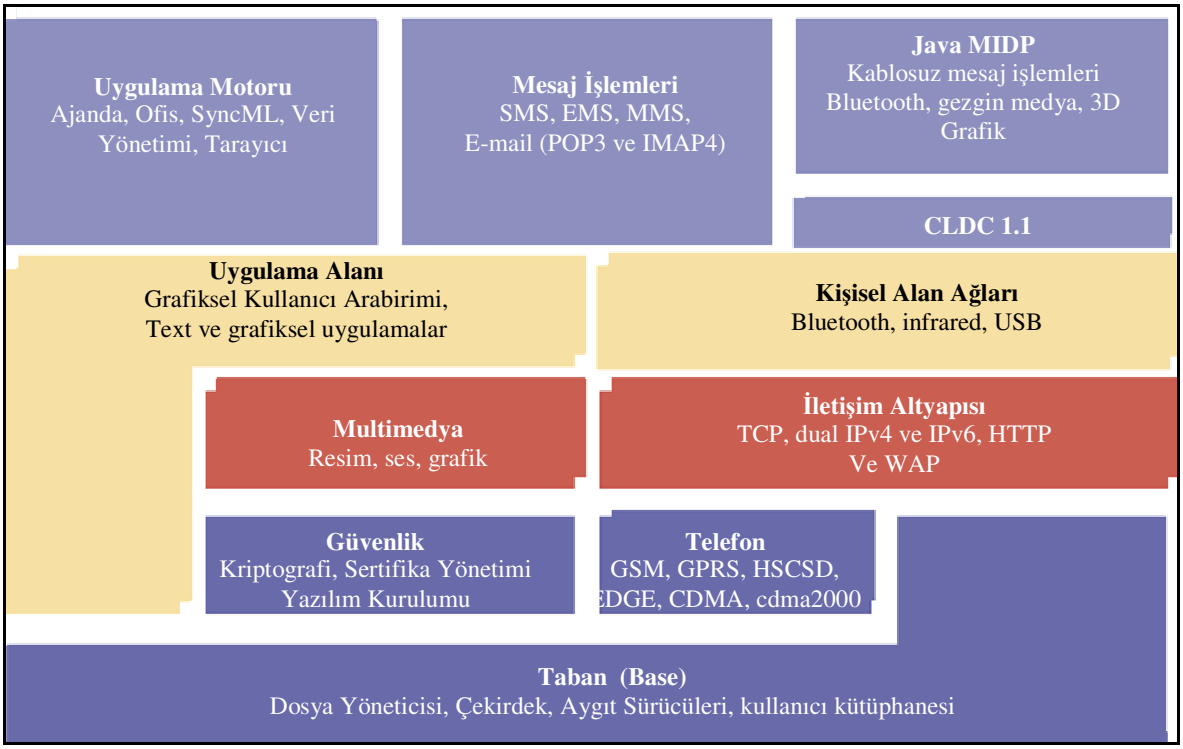
Şekil 3.3. Bir Symbian 60 Serisi Kullanıcı Arayüzü (Anonim, 2004a).

Sony-Ericsson'un kullanmış olduğu UIQ arayüzü ise interaktif geniş ekranlı, p800/p900/p910 serisi makinelerde tercih edilmiştir (Şekil 3.4).



Şekil 3.4. Sony P Serisi UIQ Arayüzü (Anonim, 2004a).

Genel yapısı ve donanımla etkileşimi dikkate alındığında Symbian OS teknolojisinin sunduğu servisler ve çerçeve mimari aşağıdaki şekil üzerinden incelenebilir.



Şekil 3.5. Symbian OS 8.0 Mimarisinin Blok Görünümü (Anonim, 2004a).

ii)Windows CE / Pocket PC İşletim Sistemi: Microsoft firmasının çokluortam mobil cihaz pazarına girmek için ortaya koyduğu ve Symbian işletim sistemine rakip olması için ürettiği bir işletim sistemidir. Symbian işletim sisteminin pazardaki hâkimiyetini kırmak ve bu alanda firmanın varlığını göstermek gayretiyle, tarz olarak Microsoft'un bildik masaüstü işletim sistemleri andıran bir stilde hazırlanmış, cep bilgisayarları/PDA'lar ile bir kısım cep telefonlarında kullanılmaya başlanan bir mobil işletim sistemidir.

Windows tabanlı mobil cihazlarda en önemli sorunlardan bir tanesi kısa batarya ömrüdür. İşletim sisteminde kullanılan API'ler güç yönetim fonksiyonunu desteklemediklerinden, Symbian'a kıyasla güç yönetimi anlamında çok kararlı bir işletim sistemi değildir.

Windows CE bataryayı ekonomik kullanmayışı, çoklu ortam isteğini karşılamakta yetersiz kalması ve kullanışsız ara yüzü nedeniyle ortaya çıkan sorunlarından dolayı bu temeli kullanan Pocket PC 2002 ve Pocket PC 2003 ve sonraki sürümler ardı ardına piyasaya sürülmüştür.

Aşağıdaki şekilde Microsoft'un Motorola MPx serisi cep telefonlarında kullandığı Pocket PC işletim sistemine ait ara yüz görünümü yer almaktadır.

Şekil 3.6. Microsoft Pocket PC Telefon Sürümü Kullanıcı Arayüzü (Aksu, 2005).

Microsoft'un Pocket PC 2002 ve Pocket PC 2003 sürümleri donanımsal açıdan incelendiğinde her iki sistemin de yalnızca ARM CPU'larını ve VGA (240X320) ekranları desteklediğini görürüz.

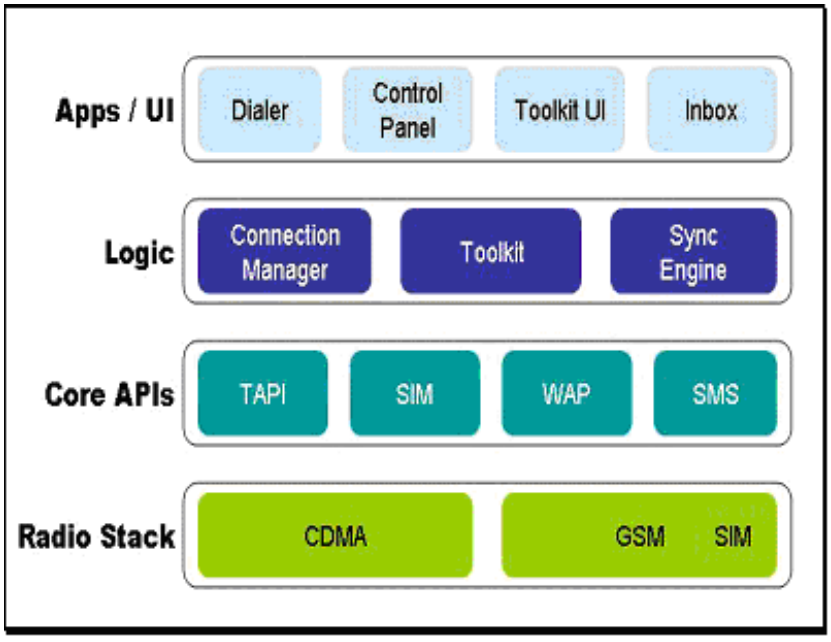
Microsoft'un cep telefonları için piyasaya sürdüğü Pocket PC versiyonları Windows Mobile serisi şeklinde isimlendirilmiştir. Bu isimlendirme beraberinde, kablosuz öğeleri destekleyen (Wi-Fi, Bluetooth) eklentileri, hızlı ve IE6.0 ile uyumlu Pocket Internet Explorer sürümünü ve Windows Media Player 9 serisini destekleyen çokluortam uygulamalarını da getirir.

Microsoft Smartphone işletim sistemi, Microsoft'un bir uçtan diğer uca kablosuz bilgisayar stratejisinin bileşenidir. Kullanıcılar için bir uçta veri diğer uçta kullanıcı servisleri olmak üzere geniş müşteri kitlesine ulaşmayı sağlar. MS Smartphone tek elle çalıştırılabilen kablosuz kompakt telefonda PDA'nın fonksiyonları ile telefon özelliklerini birleştirir. Fonksiyonlar: ses, SMS, sabit mesaj servisleri (Outlook, Exchange, IMAP ve POP3 servisleri) ve PIM uygulamalarını (takvim ve ajanda) içerir (Aksu, 2005).

Microsoft'un bu yeni işletim sistemi, Pocket PC tabanlı cihazlarda bulunan, E-mail, PIM araçları ve Pocket Web yazılımını içerir. Bu Web yazılımı HTML, WAP (WML) ve XML formatlarını destekler. Microsoft'un bu yeni işletim sistemi için uygulama geliştirmek isteyen yazılımcılar, uygun SDK (Software Development Kit-Yazılım Geliştirme Araçları)' larını ve gerekirse mevcut Windows tabanlı teknolojileri kullanabilirler.

Windows Mobile mimarisi Windows CE 3.0 mimarisi üzerine kurulduğu için, Win32 ve registry tabanlı özellik ve fonksiyonların pek çok çoğunun bir benzerini içerir. Microsoft Smartphone çekirdek mimarisi üzerinde yazılan uygulamalar bu bağlantılar hakkında her şeyi bilmeyi gerektirmeden, Windows CE tabanlı ve masaüstü cihazları için kablolu ortamda çalışması amacıyla pek çok uygulama geliştiricinin yazdığı uygulamalar onların Smartphone ile internet bağlantısını kurmak için değiştirilebilir (Finan, 2002).

Aşağıdaki Şekil'de Smartphone mimarisinin bileşenleri görülmektedir.



Şekil 3.7. Microsoft Smartphone Mimarisinin Bileşenleri (Finan, 2002).

iii) Palm OS: Daha çok PDA türü mobil cihazlarda kullanılan bu işletim sistemi daha çok kendi adıyla anılan Palm adlı cep bilgisayarlarında ve Sony tarafından üretilen cep bilgisayarlarında kullanıldı. Bu işletim sistemi, küçük, hızlı ve kullanımı kolay olarak tasarlandı. Bu işletim sistemini kullanan cihazlar pilleri şarj etmeden bir haftadan fazla kullanılabiliyorlardı.

Palm OS, 2MB'lık küçük bir hafıza ve 16 Mhz'lik bir işlemciyle çalışabilen hızlı bir işletim sistemiydi. Palm OS alışıla gelmiş dosya ve dizin yapısına ihtiyaç duymaz. Bunun yerine, veriler kolaylıkla erişilebilecek kayıtlarda ve veri tabanlarında saklanır. Multi-tasking (çok görevlilikten yoksun) olan bu sistem iki işi aynı zamanda yerine getiremez.

Önceleri ciddi bir Pazar payını elinde bulunduran Palm OS, zaman içinde bu hakimiyetini kaybetmiş, çokluortam destekli sistemler sunma çabasına rağmen yeni mobil cihazlarla rekabet etme gücünden yoksun görünmektedir (Andersson, 2001).

iv)Pocket Linux :Açık kaynak kodlu ve ücretsiz bir işletim sisteminin mobil cihazlarda kullanılması ve maliyetlerin düşürülmesi fikri, bu alanda masaüstü-dizüstü sistemlerde belli bir paya sahip olan Linux'u gündeme getirmiştir.

Linux tabanlı bir işletim sistemi hali hazırda çok yaygın olmamakla beraber yeni yeni cep telefonlarında ve bazı cep bilgisayarlarında kullanılma yoluna gidilmiştir. Sistemin başarısı, diğer rekabetçi sistemlere göre nasıl davranacağına bağlıdır.

Uygulamaların geliştirildiği üzerinde çalıştıkları ortam olan işletim sistemlerini genel hatlarıyla yukarıda inceledik. Bu noktada dikkate değer bir başka konu güvenlik anlamında incelemeye çalıştığımız değişik uygulama türlerinin hangi yazılımlar-uygulama geliştirme ortamlarının kullanılarak geliştirileceğidir.

Mobil cihazlar ve özelde cep telefonları işletim sistemlerinin çalışması ve farklı uygulamalar yüklenip yüklenmemelerine göre açık-kapalı platformlar olarak sınıflandırılırlar. Dışarıdan uygulama yüklenmesine izin veren sistemler açık, bu uygulamalara izin vermeyen sistemler kapalı sistemler olarak bilinirler.

Uygulamalar yazılırken, yazılım geliştiricilerin en önemli beklentileri multitasking (aynı anda çok görevi yapabilmek), enerjinin ekonomik kullanılması, iletişim ortamının kalitesi ve çok sayıda farklı cihaz yelpazesine uygun yazılımlar yazılabilmesi şeklindedir. Özellikle çok sayıda cihaz ile uyumlu uygulamaların yazılması, tek bir programın çok farklı firmaların ürettiği çok sayıda cihazın üzerinde çalışması bakımından çok önem taşır.

Bu ihtiyaçların Palm OS, Windows CE ve Symbian gibi farklı işletim sistemi ortamlarında aynı anda telefon modelinden bağımsız olarak çalışabilmesi (ya da değişikliklerin en azından ufak tefek modifikasyonlar seviyesinde kalması) en yaygın şekilde J2ME standardındaki API'lerle desteklenmektedir.

Bunun dışındaki uygulama yazma ve geliştirme ortamlarının bir özeti aşağıdaki tabloda gösterilmiştir (Mallick, 2003).

Çizelge 3.1. Mobil Cihazlar İçin Uygulama Geliştirme Araçları

İşletim Sistemi	Uygulama Geliştirme Aracı
Symbian OS	Symbian OS C++ Software Development Kit
	Symbian OS Java Software Development Kit
	AppForge MobileVB
Windows CE	Microsoft Visual Studio. NET with the .NET Compact Framework
	Microsoft Platform Builder
	AppForge MobileVB
Palm OS	Metrowerks CodeWarrior for Palm OS
	AppForge MobileVB
	PRC-Tools: GCC Development Tools
Java	JavaSoft J2ME Wireless Toolkit
	Netbeans Mobile Developement Kit
	Borland JBuilder 9-X
	Borland JBuilder MobileSet

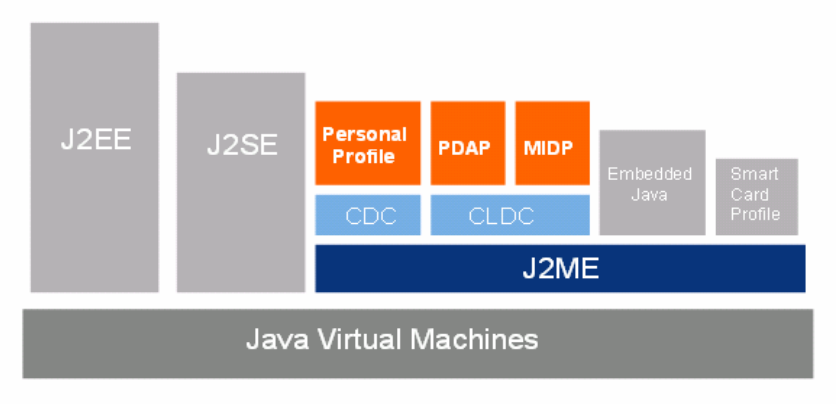
İzleyen bölümlerde bu çalışmanın yapıldığı geliştirme ortamı olarak Netbeans ve uygulama dili olarak Java dilinin bir alt kümesi olan "Mobil Java" incelenecektir. Burada java'dan ağırlıklı olarak bahsedilse de, C++'ın da mobil uygulama geliştirme dillerinden biri olduğu gözden kaçırılmamalıdır.

3.1.2. Uygulama Geliştirme Dili Olarak Java Dili Ve Mikro-Java Sürümü

SUN Microsystems firması tarafından geliştirilen Java dili normal masaüstü sistemlerde internet teknolojilerinin yaygınlaşmasıyla beraber çok güçlü bir standart haline gelmiştir. Bu yaygınlaşma ile birlikte Java'nın mikro cihazlara uyarlanması gündeme gelmiş ve ister istemez mobil cihazlar bu işi için en uygun kullanım alanı olmuştur. Cep bilgisayarı, cep telefonu ekseninde süregelen yoğun talep patlaması, paralel şekilde kullanıcı isteklerinin çeşitlenip artması, bu ihtiyaçlara cevap verecek bir uygulama geliştirme ortamının varlığını gerektirmiştir. Bu ihtiyaca -belki baştan planlanmış olmasa da- en güzel cevap, SUN firmasının Java'sı olmuştur.

Java dilinin üç farklı sürümü bulunmaktadır. Bu sürümler; Java 2 Standart Edition (**J2SE**), Java 2 Enterprise Edition (**J2EE**) ve Java 2 Micro Edition (**J2ME**) şeklindedir.

Bahsi geçen versiyonlar, değişik bilgisayar ve bilişim aygıtı barındıran ortamlar göz önüne alınarak tanımlanmışlardır. J2ME, elektronik ev araç gereçleri, gömülü aygıtlar üzerindeki kontrol ihtiyaçlarına cevap vermek amacıyla ortaya çıkmış ve tanımlanmıştır. Bu cihaz türleri, cep telefonları ve cep bilgisayarlarından, televizyonlara ve arabalara kadar birçok aygıttı içerebilir ve bu cihazların hemen hepsinde Java'nın J2ME sürümü yüklü gelebilmektedir (Özçelik, 2006).



Şekil 3.8. Java Platformu'nun Genel Yapısı (Özçelik, 2006).

J2ME cihazları genel olarak iki ana bölümde incelenirler:

i)Kişisel, Taşınabilir Cihazlar: Bunlar kesintili ağ bağlantısı olan, cep telefonu, çağrı cihazı, PDA ve cep bilgisayarı gibi aygıtlardır. Bu kategoriye giren cihazlar sınırlı yeteneklere sahip aygıtlardır ve bilgisayar tabanlı uygulama işlevleri son derece limitlidir.

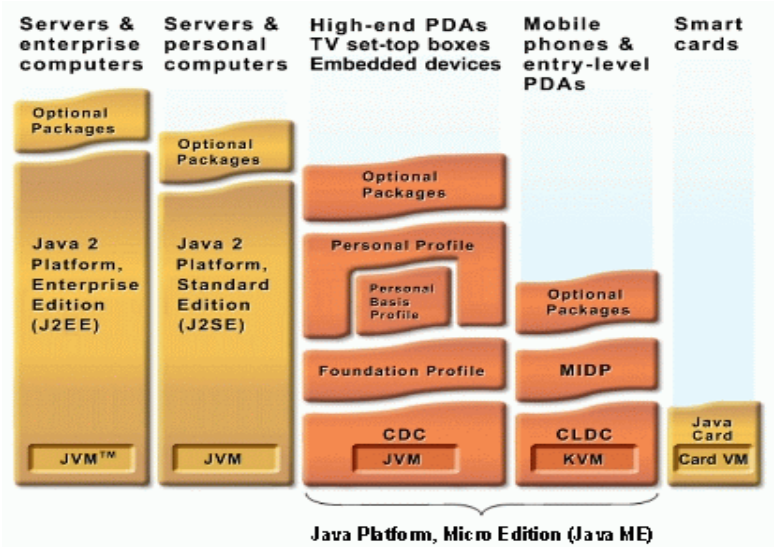
ii)Paylaşılmış Bağlantılı Cihazlar: Bunlar sabit, kesintisiz ağ aygıtlarıdır. Bunlara internet-tv'ler, internet-telefonları, arabalardaki eğlence ve seyir aygıtları örnek olarak sayılabilir. Bu kategoridekiler de yetenekli, daha gelişmiş bir ara yüze sahip aygıtlardır (Aksu, 2005).

Tüm bu bahsi geçen değişik yetenekteki ve farklı donanım yapısına sahip cihazların farklı ihtiyaçlarına cevap vermeye çalışmasından dolayı J2ME'de modüler bir yapıya gereksinim duymuştur. Bu modüler yapı ise çeşitli konfigürasyon (configuration)'lar ve profil (profile)'ler belirlenmiştir.

3.1.2.1. J2ME Konfigürasyonları Ve Profilleri

Bir J2ME konfigürasyonu bir grup cihaz için gerekli olan minimum Java platformunun tanımlamasını yapar. Burada "grup cihaz" kavramı benzer bellek ve işlemci

yapısına sahip aygıtları tanımlar. Daha açık şekilde izah etmek gerekirse; bir konfigürasyon, programcının sistem düzeyinde o aygıtın desteklediği bazı dil ve platform özelliklerini tanımlar. Bu yazılımcının belli bir konfigürasyona giren cihazlarda hangi Java kütüphanelerinin olduğunu bilmesi ve ona göre program yazmazı anlamına gelir. Özetlemek gerekirse bir konfigürasyon tanımında şu noktalar yer göze çarpar; İlgili Java programlama özellikleri , İlgili Java sanal makinesi özellikleri ve İlgili Java kütüphaneleri.



Şekil 3.9. Java Mikro Sürümü Genel Yapısı (SUN, Anonim 2006a)

Bir profil ise uygulama katmanında verilen servisleri tanımlar. Verilen servislerle ilgili bir sınırlama olmasa da, belli konulardaki profiller bir standart halindedir. Buna göre o profili destekleyen bütün cihazlarda belirli bir servis aynı şekilde bulunur. Profiller bir konfigürasyon üzerinde çalışırlar. Ayrıca bir profil bir başka profil üzerinde çalışabilir. Bir aygıt birden fazla profili destekleyebilir ancak sadece tek bir konfigürasyona sahip olur. Bu manada servis için örnek vermek gerekirse, en çok kullanılan SMS kısa mesaj servisi bir profil konusudur ve mobil cihazlar için çok yaygın bir profildir (Aksu, 2005).

3.1.2.2. Mobil Cihazlar İçin Tanımlanan Konfigürasyonlar

Bir konfigürasyon, ancak J2SE'deki bazı sınıfları içerebilir. Bir sınıf J2SE'de belli bir konfigürasyonda tanımlıysa mutlaka aynı şekilde tanımlı olmak zorundadır. Bu durumda bir mobil cihaz için konfigürasyon tanımlaması yapıldığında bu standart sınıfa eski metotları kullanmak zorunluluğu olmasa da yeni bir metot eklemek mümkün değildir.

J2ME genel olarak CLDC (Connected Limited Device Configuration-Sınırlı Bağlantılı Cihaz Konfigürasyonu) ve CDC (Connected Device Configuration) şeklinde iki konfigürasyon tanımlar. Şimdi bu konfigürasyonları kısaca inceleyelim.

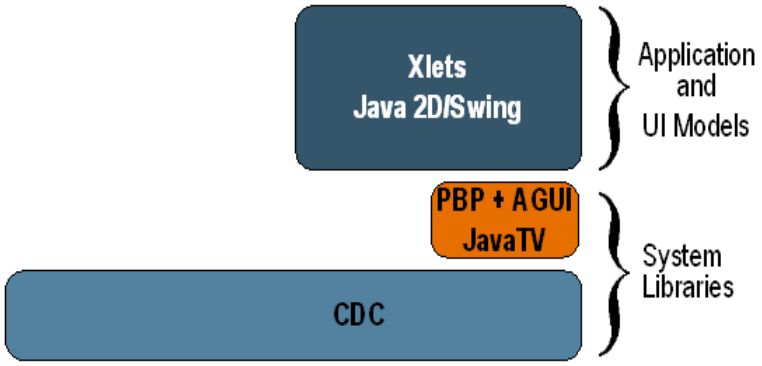
i)CDC: J2SE'de bulunan bir çok özelliği barındıran CDC için CVM (Compact Virtual Machine) kiti geliştirilmiştir.Bu kit standart JVM (Java Virtual Machine)'de olan

hemen hemen bütün özellikleri içermektedir. Bu iki kütüphane arazındaki tek fark referans olarak tasarlandıkları cihaz gruplarıdır. Çünkü CDC, JVM'nin aksine sınırlı kaynağa sahip cihazlar için tasarlanan bir konfigürasyondur.

CDC'de tanımlanmış java paketleri kısaca aşağıda listelenmiştir:

java.io
javax.microedition.io
java.text
java.security
java.security.cert
java.math
java.lang, java.lang.ref, java.lang.reflect
java.util, java.util.zip, java.util.jar
java.net

Bu konfigürasyonun tanımladığı profillerden ilki, Foundation Profile'dır. Bu profil J2SE'de bulunup, CDC'de bulunmayan nesnelerdeki (java.lang, java.util, java.net, java.io ve java.security) eksikleri eklemektedir. Bu profil CDC'yi bir programlama ortamı olarak devreye sokmuştur. Ancak bu ortamın en büyük handikapı, AWT (Absract Windows Toolkit) veya Swing gibi bir ara yüze sahip olmamasıdır. Bir programda ara yüz kullanmak için Personal Profile gibi bir profilin desteklenmesi gereklidir. Bu profil'le birlikte sistem Personal Java adıyla da anılıp, Java sisteminde J2ME'a bir geçiş yolu sağlamış olur. Bir nesnenin ağda başka bir aygıtta çalışan bir nesnenin herhangi bir metodunu doğrudan çağırmasını sağlayan RMI (Remote Method Invocation - Uzaktan Yöntem Çağırma) bir başka profil olarak göze çarpar.

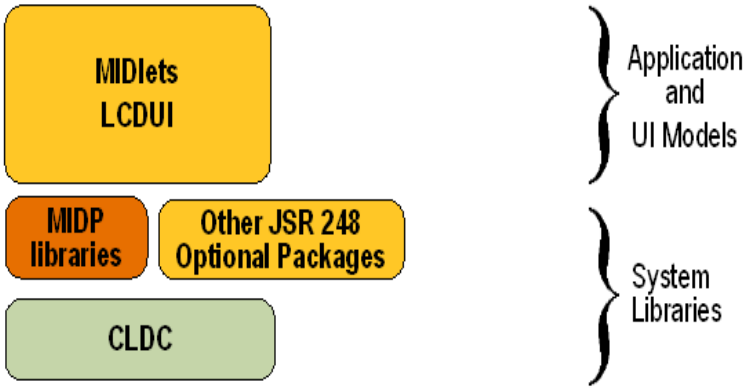


Şekil 3.10. CDC Cihaz Konfigürasyonu (Anonim, 2006a)

CDC konfigürasyonu 2 MB'tan fazla belleğe sahip gelişmiş cihazlar için tanımlanmışken, birazdan incelenecek olan CLDC 160 KB gibi düşük belleklere sahip az gelişmiş cihazlar için tanımlanmıştır. Ancak CDC tanımlamasının CLDC kütüphanelerini tümüyle kapsadığı gözden kaçırılmamalıdır. Bu anlamda CLDC'yi CDC'nin bir alt kümesi gibi görmek yanlış olmaz (Özçelik, 2006).

ii)CLDC : CDC'ye benzer şekilde Java'nın mikro sürümünde tanımlanmış ikinci konfigürasyonu CLDC olarak bilinir. Bu standart, bellek kapasitesi düşük, batarya gibi zayıf güç kaynaklarıyla beslenen, kablosuz cihazlar için tanımlanmıştır (Aksu, 2005).

Mobil cihazların pek çoğunda bazı donanım birimlerinin olmaması (kesirli sayıları destekleyen donanım birimleri gibi) bu standardın Float (kesirli) tipi Object Serialization özelliklerinden mahrum gelmesine neden olur.



Şekil 3.11. CLDC Cihaz Konfigürasyonu (Anonim, 2006a)

KVM (Kilobyte Virtual Machine) adı verilen bir sanal makine, CLDC'yi desteklemekte ve bu konfigürasyonda aşağıdaki paketler bulunmaktadır:

javax.microedition.io, java.io
java.lang
java.util

3.1.2.3. J2ME Profillerine Genel Bir Bakış

J2ME üzerine inşa edilmiş profiller arasında en yaygın olanı, CLDC konfigürasyonu üzerine kurulan Motorola, Nokia ve Sony-Ericsson gibi firmaların desteklediği MIDP (Mobile Information Device Profile) profilidir. MIDP 1.0 ve MIDP 2.0 şeklinde iki sürümü bulunan bu profil uygulamanın yaşam döngüsü, kullanıcı grafik arabirimleri, iletişim ağı ve kalıcı veri depolama ile ilgili kütüphanelerini içerir.

MIDP 1.0'ın sahip olduğu ve desteklediği paketlerin uzatılması ile ortaya MIDP 2.0 profili çıkmıştır. Sırasıyla bu iki grup profilin desteklediği paketler ve aralarındaki farklar aşağıda gösterilmiştir:

MIDP 1.0'ın desteklediği paketler:
java.io
java.lang,java.util
javax.microedition.io
javax.microedition.lcdui
javax.microedition.midlet
javax.microedition.rms

MIDP 2.0'ın MIDP 1.0'a ek olarak desteklediği paketler:

javax.microedition.lcdui.game
javax.microedition.media
javax.microedition.media.control
javax.microedition.pki

Bu gruptaki dağılıma dikkat edildiğinde MIDP 2.0'ın çokluortam teknolojilerini destekleyen sınıflarla zenginleştiği görülmektedir.

3.1.2.3.1. MIDP Profillerinin Programlanması Ve MIDlet'ler

Bir MIDlet, CLDC üzerinde MIDP profili için yazılan Java uygulaması olarak tanımlanır. Bir MIDP uygulaması geliştirilirken, MIDlet'lerin yaşam döngüsü, kullanıcı arabirimleri, komut işleme, konuşlandırma ve uygulama yönetimi gibi bazı temel bilgilere sahip olunmalıdır. İzleyen bölümde bu konudaki bilgilere kısaca yer verilecektir.

i)MIDlet Yaşam Döngüsü: Bir MIDlet'in kurulumu, başlaması, durdurulması ve kaldırılması ile ilgili işlemlerin yapıldığı ortam AMS (Application Management Software - Uygulama Yönetim Yazılımı) olarak bilinir. AMS aynı zamanda JAM (Java Application Manager - Java Uygulama Yöneticisi) olarak da bilinmektedir.

Genel olarak MIDlet'ler durağan, etkin ve ölü şeklinde üç durumdan birinde bulunabilirler. Bir MIDlet genel olarak oluşturulduğu ve başlatıldığı zaman durağan kiptedir. Eğer MIDlet yapılandırıcısında kural dışı bir durum oluşursa MIDlet ölü durumuna geçer. MIDlet'ler etkin durumdan durağan durumuna pauseApp() metodunu tamamladıktan sonra, etkin konumdan durağan duruma startApp() metodunu tamamladıktan sonra, ölü konumuna ise destroyApp() metodunun tamamlanmasından sonra geçerler. Sonuncu metod, bir MIDlet'in kullandığı kaynakları serbest bırakır ve sistemde gerekli temizleme işlemini yapar (Aksu, 2005).

Bir MIDlet yazılımcısı yazılımını etkin kipte çalıştırır ve gerektiği zaman diğer durumlar arasında geçişleri sağlar.

ii)MIDP Kullanıcı Arabirimi: Kullanıcı arabirimleri dikkate alındığında, iki ana kategori göze çarpar. Düşük düzey kullanıcı arabirimi Canvas isimli nesneye dayanırken, yüksek düzey kullanıcı arabirim nesneleri Alert, Form, List ve TextBox olarak sıralanabilir. Bu nesnelerin görünüş biçimleri profilin gerçekleştirildiği cihazların kullanıcı arabirimlerine göre değişebilir.

Canvas nesnesi ile kullanıcı arabirimine daha direkt kontrol sağlanır. Bu ekranda nelerin çizileceği ve klavye olayları hakkında daha geniş bir kontrol imkanı sağlar. Kullanıcı arabirimlerini kullanırken bilinmesi gereken en önemli nokta yazılan MIDlet'lerin değişik kapasiteli cihazlarda çalışabiliyor olmasıdır. Bu ise ekran genişliği, ekranın renkli veya siyah-beyaz oluşu gibi parametrelere göre bir takım kontroller yaptırılarak MIDlet'lerin değişik ortamlara uyum sağlayabilecek şekilde yazılmasına imkân tanır (Özçelik, 2006) .

iii)MIDlet Grubu ve Uygulama Tanımlayıcıları: Bir veya daha fazla MIDlet 'MIDlet Suite' denen JAR (Java Archive File) uzantılı dosyalara paketlenir ve her JAR

dosyasında, içeriğini tanımlayan bir JAD (Java Application Descriptor) uzantılı tanımlayıcı dosya vardır. Bu dosyalar Uygulama Yönetim Yazılımları tarafından kullanılırlar.

iv)RMS (Record Management System - Kayıt Yönetim Sistemi): MIDP, MIDlet'lerin cihazlarda kalıcı olarak veri depolamasını ve çağırabilmesini sağlar. Bu sistem, basit bir kayıt yönelimli veritabanıyla sağlanır. Bir MIDP veritabanındaki veri MIDlet'ten çıkış yapıldığında da varlığını sürdürür. RMS veri saklama ve erişimi için kullanılır. J2ME'de uygulamaya RMS desteğini sağlamak için '.rms ' uzantılı java paketinin kullanılması gerekmektedir.

3.1.2.4. MIDP Uygulamaları Geliştirme Araçları

Mobil cihazlar için (özellikle cep telefonları) bir MIDlet geliştirmek programcılara sunulan yetenekli ortamlar aracılığı ile oldukça kolaylaşmış, basitleşmiştir. Bu geliştirme yazılımlarının hemen hemen hepsinin ortak özelliği kullanıcıya bir görsel programlama ortamı sunmaları ve böylece programlama yükünü azaltmalarıdır.

Öte yandan bu yazılım geliştirme programlarının bir diğer önemli özelliği yazılan programı, hedef cihaza uygunluğu anlamında test etmeye izin veren emulatörlerle beraber gelmeleridir.

Bir emülatör, programın yazıldığı cihazın orijinali olmadan da yazılan programın çalışabilirliğini, ekran görünüşünü neredeyse cihazla birebir göstermeye imkan tanır. Eğer programın yazılacağı cihazın emülatörü geliştirme ortamıyla birlikte gelmemişse, firmalar tarafından kitler halinde yazılımcılara dönük olarak yazılmış emülatör firmanın web adresinden indirilerek kullanılabilmektedir. Çünkü geliştirme ortamları bu emülatörleri kullanabilecek şekilde tasarlanmış olduklarından, her yeni cihaz için sadece yeni bir emüülatörün web sitesinden indirilerek, yazılıma tanıtılması yeterlidir.

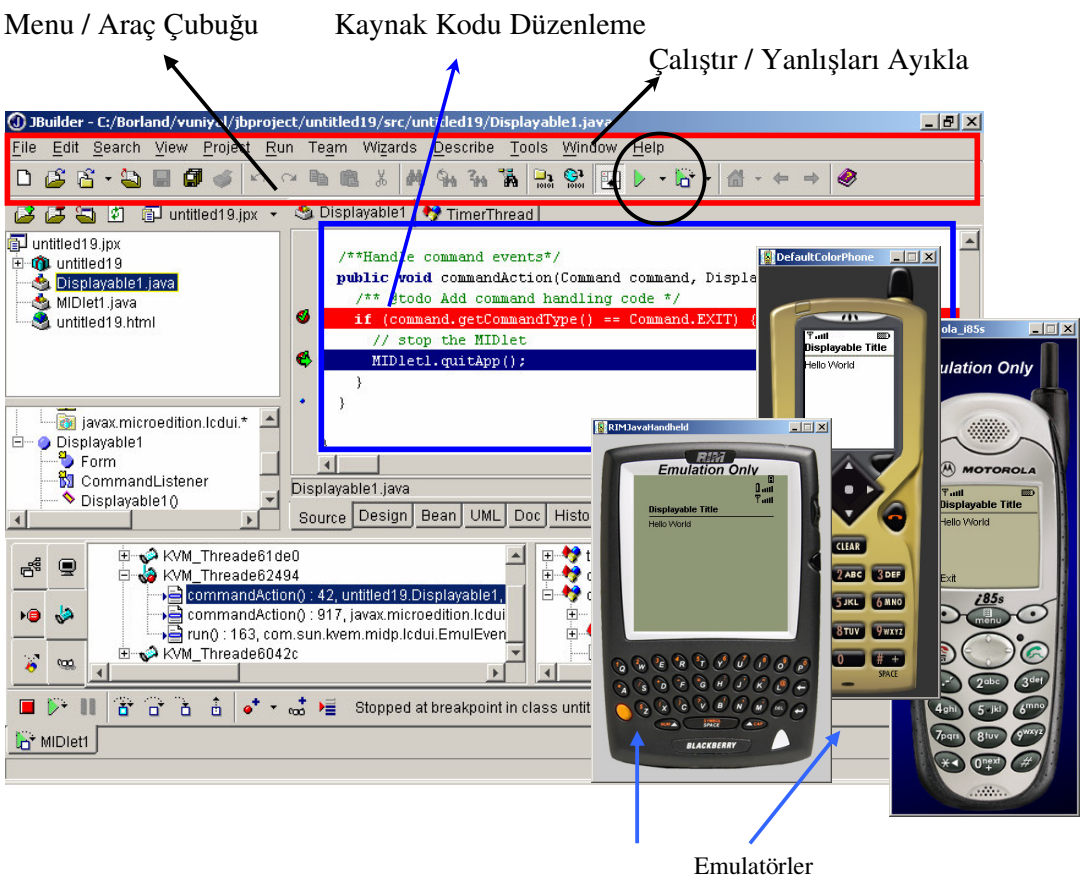
İzleyen bölümde bu uygulama geliştirme ortamlarına kısaca değinilecektir.

3.1.2.4.1. Borland Java Builder 9/X (Mobıle Set 3.0)

Borland J builder içerisinde J2ME araçları bütünleşik haldedir. J Builder ile geliştirilen gezgin uygulamalar aslında J2ME araçları kullanılarak geliştirilmektedir. Java desteği olan tüm aygıtlarda J Builder ile geliştirilen uygulamalar çalıştırılabilir (Aksu, 2005).

Borland J Bbuilder diğer benzeri yazılımlarda olduğu gibi sağladığı emülatör desteği sayesinde gerektiğinde orijinal cihaz olmaksızın, yazılan uygulamayı test etme, çalıştırma imkanı sunmaktadır. Mobil cihaz üreten her firma uygulama geliştiriciler için bir SDK kiti düzenler. Bu kit kolayca dağıtılan ve çoğunlukla C++/Java gibi diller ile yazılarak kullanıcıların yazılım geliştirme ortamlarına adaptasyonu kolaylaştırılır.

Borland J builder firmanın yeni bir sürüm çıkarmamasından dolayı uygulama geliştiriciler için güncelliğini kaybetme riski ile karşı karşıyadır. Bu nedenle uygulama geliştiriciler ileride ele alınan ve ücretsiz olarak kullanılabilen, Netbeans ara yüzünü mobil uygulama geliştirmek için tercih etmelidirler.



Şekil 3.12. Borland Builder Uygulama Geliştirme Ortamı.

3.1.2.4.2. C++ Mobil Sürüm

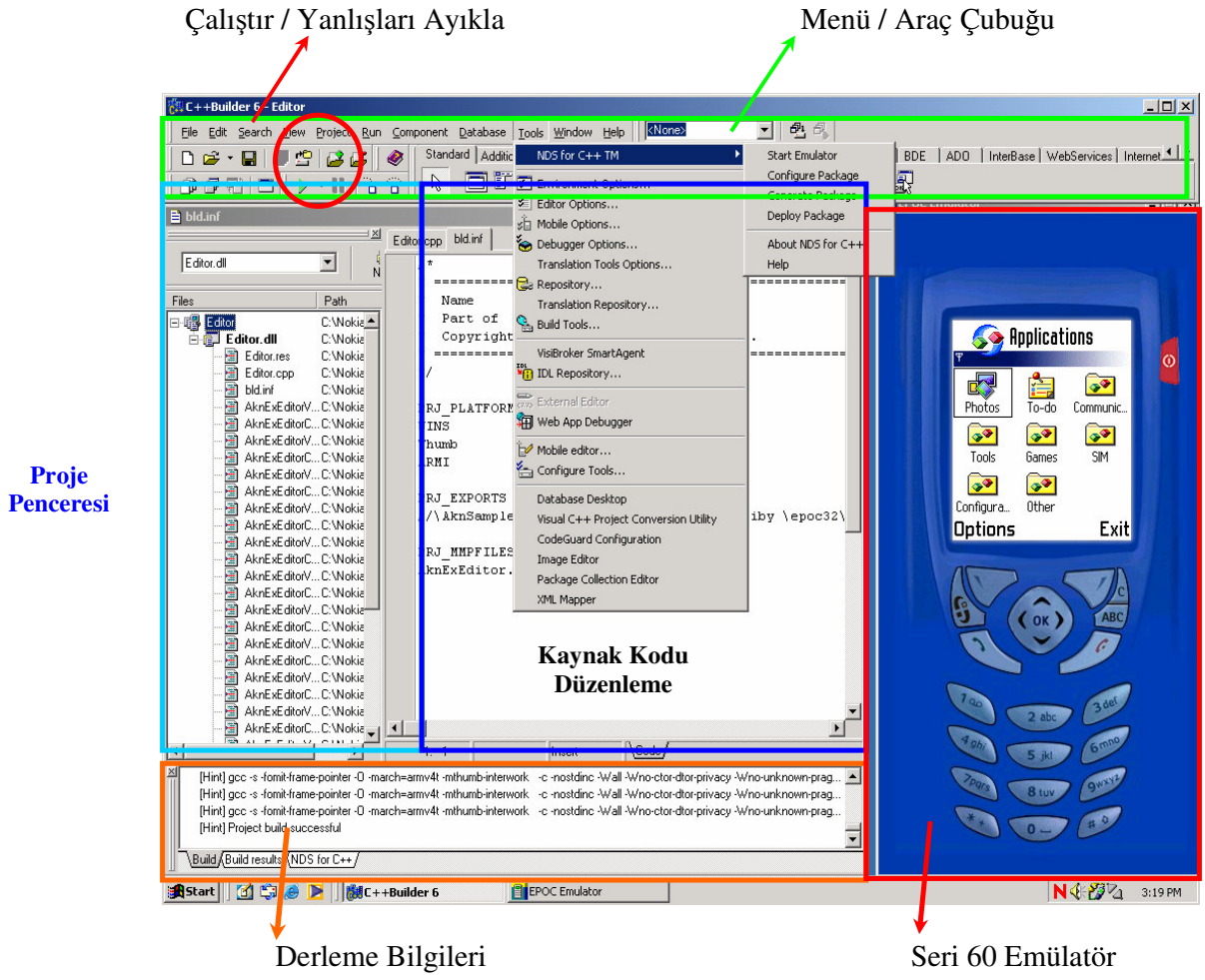
Bazı firmalar java dili yanında C++ dilinin de cihazları için yazılım üretmesini desteklemektedirler. Nokia 60 serisi bu anlamda C++ dili ile telefonlarında yazılım geliştirmesine müsaade etmekte ve bunun için de emülatörler üretmektedir.

C++ dili için farklı uygulama geliştirme ortamları olmakla birlikte, Borland C++ Builder, Symbian C++ dilini kullanarak C++ uygulamalarının geliştirilmesi için güçlü bir ortam sunar.

Borland C++ Mobile Edition yazılımı, Symbian C++ uygulama geliştirme özeliklerinden daha fazlasını destekler. Bu özellikler arasında, hata ayıklama, yerleştirme araçları (deployment), emulasyon aygıtı, gezgin uygulamalar oluşturmak için grafiksel tasarım araçlarını bulunmaktadır (Özçelik, 2006)

Symbian işletim sistemi yüklü telefonlar için uygulama geliştirmek isteyen herkes Borland C++ Builder'i kullanabilir. Nokia ve Borland'dan elde edilen ürünler Nokia 60 serisi aygıtlar için C++ uygulamaları geliştirmeyi destekler (Aksu, 2005).

Java'nın standart bir dil olarak hemen hemen tüm mobil cihazlarda kullanılması C++ açısından handikap oluştursa da bu geliştirme ortamı da uygulama geliştiricilerin ilgisini çekmektedir.



Şekil 3.13. C++ Builder Uygulama Geliştirme Ortamı.

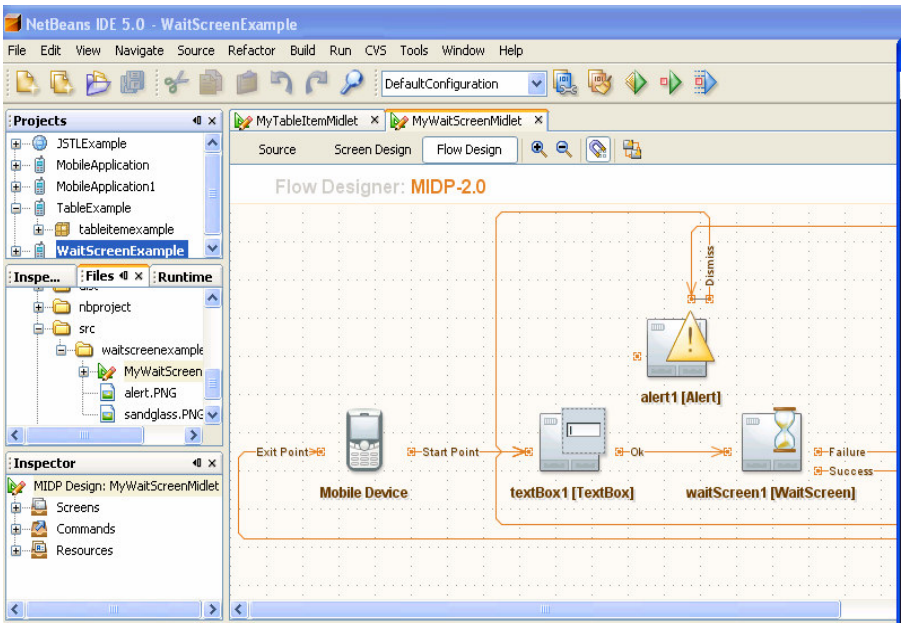
Yukarıdaki şekilde gösterilen emülatör, test için yapılan girişlere neredeyse gerçek bir telefon gibi cevap verir. Bu şekilde cihazın açılıp kapanması, geliştirilen yazılımın başlayıp durdurulması, yazılımın çıktılarının gözlenmesi gibi çok sayıda işlev gerçek bir cihaz olmadan emülatör aracılığı ile çalışma zamanı rahatlığını sağlar. Böylece uygulama geliştirici mobil yazılımının bir çok cizahı desteklemesi için gereken testleri yapabilme imkanına sahiptir.

3.1.2.4.3. Netbeans Mobil Yazılım Geliştirme Ortamı

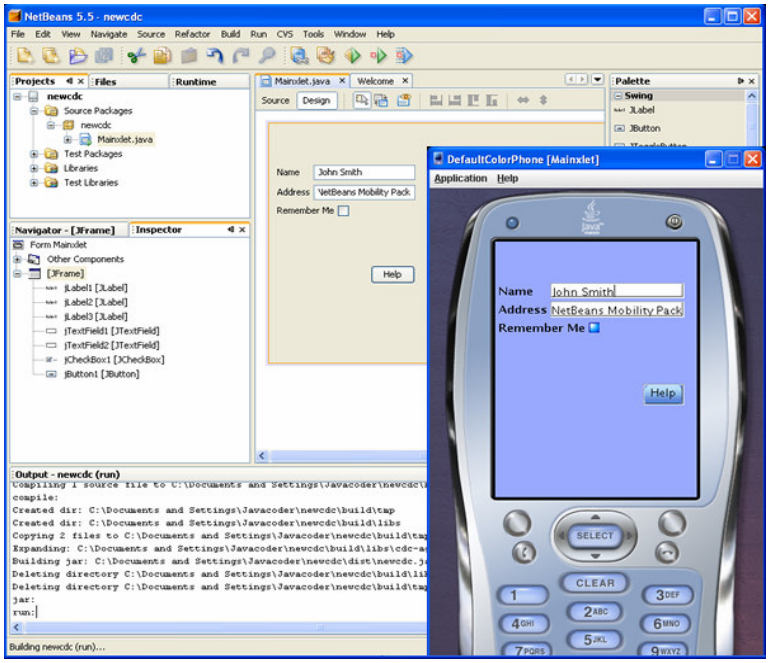
Önceleri SUN'ın bünyesinde geliştirilen Forte java uygulama geliştirme ortamı sonraları Netbeans geliştirme ortamı olarak kendisini gösterdi. Netbeans, gerek normal

java programları gerekse mobil uygulama geliştirme anlamında güçlü arayüzü ile görsel programlama için en iyi IDE'lerden birisidir.

Netbeans mobil geliştirme için diğer ortamlardan farklı olarak "flow designer" isimli çok gelişmiş bir programlama arayüzünü kullanıcının hizmetine sunar. Kullanıcı bu arayüz yardımı ile programının akışını algoritma tasarımı gibi yaparcasına rahatlıkla tasarlayabilir. Aşağıdaki şekilde flow designer'ın kullanıldığı bir program akışı görülmektedir.



Şekil 3.14. Netbeans Flow Designer'da Program Akışı



Şekil 3.15. Netbeans'ta Emülatör Kullanımı

Netbeans yine mobil program geliştirme aşamalarında önemli bir yer tutan test aşamasını emülatörler yardımıyla gerçeklemeye izin vermektedir. Hemen hemen her mobil cihaz üreticicisinin ürettiği cihazlar için geliştirdiği mobil cihaz emülatörleri programa tanıtılarak kolayca kullanılabilmektedir.

3.1.3. Güvenlik, Kimlik Doğrulama, Kimlik Saptama, Güvenlik Düzeyleri

Güvenlik sözkonusu olduğunda öncelikle iki kavramın incelenmesi gereklidir. Authentication ve identification kelimeleri ile ifade edilen bu iki kavram sırasıyla, kimliğin doğrulanması, kimliğin saptanması şeklinde Türkçeleştirilebilir. Temel olarak bir kullanıcı bir girişl sırasında kendine has bir bilgiyi beyan eder. Bu bilgi veritabanında daha önce kayıtlı bilgi ise beyan ya da kimlik doğrulanmış (bu şekilde bir kullanıcı var-authentication) olur. Basit ifadeyle authentication'da sadece bilinen (kayıtlı) bir kullanıcının beyanının doğruluğu kontrol edilir. Bu birebir bir ilişki şeklinde düşünülebilir. Identification'da ise beyanı veren kişi veri tabanında kayıtlı tüm bireylerle karşılaştırılarak, beyan sahibinin kim olduğu saptanmaya çalışılır.

Güvenlik farklı seviyelerde incelenebilecek bir kavramdır. GSM ağını kullanmaya çalışan bir istemci için mobil telefon ile authentication merkezi arasında bir kimlik doğrulama prosedürü başlar. GSM ağı tarafından bilinen bir kişi olduğunu iddia eden kullanıcının SIM kartında ve authentication merkezinde saklı gizli anahtar bir algoritma yardımıyla sağlanmaya çalışılır. Bir diğer güvenlik örneği epostasına ulaşmaya çalışan bir kullanıcıdır ki, kullanıcı bu işlem için bir kullanıcı adı ile şifreyi girmek zorundadır. Burada birisi ağ seviyesinde diğeri uygulama seviyesinde iki farklı güvenlik düzeyi söz konusudur.

Ağ güvenliğinin en önemli görevi, veri iletişim güvenliğini uçtan uca bir ağdan ötekine korumaktır.

Uygulama güvenliği ise ağ güvenlik mekanizmalarından bağımsız olarak çalışan güvenliğini sağlamakla ilgilenir.

Organizasyonal güvenlik bir organizasyondaki tüm güvenlik prosedürlerini ve birbirleriyle ilgilerini dikkate alan bir güvenlik seviyesidir.

Sistem güvenliği ise bir cihaza özgü şekilde cihaz üzerinde uygun güvenlik yazılımın kurulu olup olmaması, yazılım ayarlarının yapılıp yapılmadığı şeklindeki kavramlar ile ilgilenir.

Güvenlik literatüründe güçlü güvenlik doğrulama kavramı, kullanıcının kimliğini doğrulama şansını arttıran işlem olarak bilinir. Bu çoğunlukla, uzun şifreler veya iki-üç doğrulama faktörünün birleştirilmnesi ile sağlanır. Genel olarak üç doğrulama faktörü dikkate alınır.

i) Bilgi faktörü: Kullanıcı bildiği bir şeyi (şifre gibi) sunmak zorundadır.
ii) Sahip olma faktörü: Kullanıcı sahip olduğu bir şeyi (anahtar gibi) sunar.
iii) Olma faktörü: Kullanıcı kendisine ait bir şeyi-uzvu (göz, el vs) sunar.

Güvenliğin artması, daha iyi bir güvenlik düzeyi bu faktörlerin değişik kombinasyonlarının kullanımına bağlıdır.

Bilgi faktörü (şifre) en çok kullanılan güvenlik türüdür. Kullanıcının şifresini hatırlama zorunluluğu, şifrenin tahmin edilebilir kolaylıkta olması veya zor şifrenin hatırlamak için bir yere not alınması gibi nedenlerden dolayı zayıf bir yöntem olmakla beraber diğer faktörlerle birleştirilmesi güvenirliğini arttıracaktır.

Sahip olma faktörü ise akıllı kartlar ve anahtarlar (dijital rastgele sayı üretebilen kartlar) olmak üzere iki türe sahiptirler. Akıllı kartlara SIM kartlar, banka kartları örnek verilebilir. Bu kartlar, bir kart okuyucu (Bir ATM, bir mobil cihaz) ve genellikle bir PIN (Personel Identification Number-Kimlik Saptama Numarası) ile birlikte kullanılırlar. Bu güvenlik düzeyi hem sahip olma hem de bilgi faktörlerini birlikte içerir.

Olma faktörlerine örnekler ise, el geometrisi, bir kalemle oluşturulmuş dijital bir imza, ses tanıma, iris tanıma, parmak izi gibi insandan insana değişen benzersiz özelliklerdir.

3.1.3.1. Multimedya Tabanlı Güvenlik Sistemleri Ve Biometri

Multimedya tabanlı güvenlik sistemleri genel olarak yüz, ses, parmak izi, retina gibi biometri olarak adlandırılan insan vücudundaki benzersizlikleri-benzeşmezlikleri referans alarak kimlik doğrulaması (authentication) yaparlar.

Genel olarak bu sistemler, tanımlaması ya da doğrulaması yapılacak kişiden alınan görüntü-ses örneği ile doğrulama anındaki örneği kıyaslayarak bunların aynı olup olmadığını saptamak esası üzerine çalışırlar.

Biometri cihazlar insanların benzeri olmayan parmak izi, göz retinası, iris, yüz sekli, ses, imza, avuç içi vs gibi karakteristiklerini ölçerek; bilgisayar sistemleri, veri bankaları ve benzer ortamlara giriş için kimlik doğrulamasını yapmaktadırlar. Bunun dışında, bu sistemler emniyet ve istihbarat birimlerinde de çok değişik amaçlarla kullanılmaktadır. Biometrik Sistemler, temelde, kişinin sadece kendisinin sahip olduğu, kendisi olduğunu kanıtlamaya yarayan, değiştiremediği ve diğerlerinden ayırıcı olan, fiziksel veya davranışsal bir özelliğinin tanınması prensipleri ile çalışmaktadırlar. Ancak bu sistemlerin güvenilir olmalarının yani sıra pratik olmaları da gerektiğinden dolayı, kişileri hangi yöntemler ile tanındıkları da önemli bir etkendir (Saday, 2005).

İnsanları; parmak izlerinden, gözlerinden ve fizyolojik özelliklerinden tanıyabilen Biometri Teknolojisi, her geçen gün biraz daha gelişiyor. Ancak bu teknolojinin yaygınlaşabilmesi için maliyetlerin daha uygun hale getirilmesi gerekiyor.

İnternet üzerindeyken, hiç kimse kim olduğunuzu bilemez. Kim olduğunuzu kanıtlamanızın geleneksel yolu, e-posta atarken, on-line alışveriş yaparken veya güvenlikli bir Web sitesine girerken şifre yazmaktır. Fakat bu yol şifreleme algoritmalarının çözümlenmesi sayesinde gün geçtikçe güvenliğini daha çok kaybetmektedir.

Şifreler ağ korsanları tarafından birçok kez kırıldığı için ya da kullanıcılar tarafından sık sık unutulduklarından artik yerlerini Akilli Kartlar ve Biometrik cihazlar gibi yeni teknolojilere bırakmaktalar. Biometrik Cihazlar insanların benzeri olmayan parmak izi, göz retinası gibi karakteristiklerini ölçerek kullanıcıların şifre kullanmaksızın bilgisayar sistemleri, veri bankaları ve benzer ortamlara giriş için kimlik doğrulamasını yaparlar. Bu fizyolojik ölçü yöntemlerinin tümü "Biometri" olarak tanımlanmaktadır. Biometrik bilgiler; kaybolmamak, unutulamamak ve bir başkası tarafından kullanılamamak gibi özelliklerinin yani sıra taklit edilememe gibi çok önemli olan bir özelliğe de sahiptir.

Biometri teknolojisiyle, bilgisayara parmak izi tarayıcısını kullanarak girmek, göz tarayıcısı yardımıyla ATM'den parayı çekmek, ses tanıma ile bankalara sesli talimat vermek, korunmakta olan mekânlara yüz tanıma cihazı yardımıyla girebilmek vs mümkün olabilmektedir.

Biometri teknolojisi, halen, yukarıda gösterilen gelişmelerin yani sıra aşağıdaki önemli problemlerle karşı karşıyadır.

- Biometri için gereken donanımın pahalı olması
- Farklı sistemlerin birbirleriyle sorunsuz bağlantısının henüz sağlanamamış olması
- Biometri teknolojisinin bir bütün halinde yeni yeni gelişmekte olmasıdır.

Bilgisayarlar günlük hayatin giderek daha önemli bir parçası haline gelmesiyle, belgelerin imzalanmasından alışverişe kadar pek çok işlem dijitalleşerek, biometri ürünleri vazgeçilmez bir hal alacak gibi görünüyor (Saday, 2005).

Biometri teknolojisini referans olarak kullanan sistemlerin mobil olması şüphesiz kullanım alanını genişletecek bir etkendir. Tam da bu noktada devreye giren çokluortam destekli cep telefonlarının sunmuş olduğu ses, görüntü işleme-iletme yetenekleri arzu edilen gelişmeleri hızlandıracak dinamik bir alanın habercisi olmaktadır.

İnternetin bilgi teknolojisi aracı olarak etkin kullanılmaya başlanması ile birlikte, bazı kişisel bilgilere veya firmalara ait gizli verilere, yetkili olmayan kişi veya kuruluşlarca ulaşmanın engellenmesi zorunluluğu doğmuştur. Bilinen ve yaygın olarak kullanılan sistemler, kullanıcıları tanımlamak yerine kullanıcının sunduğu tanıtıcılara onay vermektedir. Hâlbuki biometrik teknolojiler kişileri doğrudan tanıdıkları için, yetkisi olmayan kişilerin değerli bilgilere erişimini, ATM, cep telefonu, smart kart, masaüstü bilgisayar, is istasyonu ve bilgisayar ağları gibi sistemlerin uygunsuz kullanımının engellenmesi için en çok başvurulan yöntem olmaktadırlar. Günümüzde çeşitli biometrik sistemler, eşzamanlı tanıma uygulamalarında yaygın olarak kullanılmaktadır. Bunların en bilinenleri aşağıdakilerdir:

- Parmak izi eşleştirme
- İris tanıma
- Retina taraması
- Ses ve konuşma tanıma
- Yüz tanıma
- El tanıma

Biometrik referanslı çokluortam sistemlerinin en temel avantajı, kişilerin hiçbir zaman hiçbir yerde unutma veya kaybetme olanakları bulunmayan bir uzuvları ile kendilerini tanıtabilmeleridir. Bu yüzden gelecek için planlanmakta olan güvenlik sistemlerinin en esas amacı insanların hiçbir kart veya anahtar tasimadan veya şifre ezberlemeden evlerinden çıkabilmeleri ve belli bir kişinin sadece o olduğu için tanınabilmesidir (Anonim, 2001a).

3.1.3.2. Çokluortam Tanıma Sistemlerin Çalışma Prensipleri Ve Kullanım Alanları

Çokluortam tanıma sistemlerinin çalışma prensibi aşağıdaki şekilde özetlenebilir:

Önce kayıtlı bir imaj alınır. Bu imaj dijital koda çevrilir. Bu kod da gerekirse yapılan işleme göre şifrelenir ve bilgisayara kaydedilir. Daha sonra kullanıcı herhangi bir cihaz aracı ile kendini sisteme tanıtır. Genellikle ayni kişiye ait olsa bile, girilen kod ile kayıtlı olan kodun birebir tutuma olasılığı yoktur. Bunda birçok faktör etkili olabilir. Bunlarda en yoğun olarak rastlananları aşağıdakilerdir:

- Ortamın ışıklandırması
- Kişinin bakış açısı
- Teşhisi yapılacak uzvun cihaza göre durma açısı
- Cihazın ve kontrol edilen uzvun temizlik derecesi ve nemi

Bu olumsuz etkilerden dolayı girilen kod, belli bir yüzde tutuncaya kadar sistemde kayıtlı bulunan kodlarla karsılaştırılır. Gereken yüzde yakalandığında şahıs tanınır ve işlem için onay verilir.

Halen çokluortam doğrulama sistemleri aşağıdaki alanlarda kullanılmaktadır:

- Personel devam ve takibi
- Otomatik para çekme makinelerinde kullanıcı tanımlama
- Çağrı merkezlerinde kimlik saptama
- On-line bankacılık kullanıcı tanımlama
- Internet bankacılığında kullanıcı tanımlama
- Elektronik para transferlerinde kullanıcı tanımlama
- Kredi kartı uygulamaları
- Satış noktası terminallerinde (POS) kullanıcı tanımlama
- Askeri kaynakların etkin takibi
- Çek onaylama işlemlerinde kullanıcı güvenliği
- Hastane ve sigorta kuruluşlarında hasta takibi ve kimlik saptama
- Kamu hizmetlerine yönelik kayıt takibi (SSK, vergi, trafik)
- Hesap açma işlemlerinde kimlik tespiti
- Binalara, tesislere ve ofislere erişim güvenliği
- Elektronik ticarette kullanıcı tanımlama
- Şube bankacılığı işlemlerinde kullanıcı tanımlama (Saday, 2005)

3.1.3.3. Çokluortam Tabanlı Tanıma-Doğrulama Türleri

Çokluortam tabanlı güvenlik sistemleri hem klasik hem de daha sonra detaylı şekilde ele alınacak mobil sistemlerle aynı prensipleri kullanarak çalışırlar. Aşağıda bu bağlamda temel çokluortam güvenlik doğrulama türleri incelenecektir:

i)Parmak izi Doğrulama: Parmak izi doğrulamaya birçok farklı yaklaşım vardır. Bir kısmi bilinen polis metodu olan iz karsılaştırmasını taklit etmeye çalışır, diğerleri ise "mire ringe" şablonu yâda ultrasonik gibi kendilerine özgü yaklaşımlar ile düz şablon karsılaştırması yaparlar. Bazıları canlı bir parmağı hissedebilirler bazıları edemezler. Diğer biometriklere kıyasla parmak izi cihazlarında çok fazla çeşitlilik vardır. Yüksek verimli ve düşük hata paylı olmalarına rağmen tecrübesiz kullanıcıların hatalı işlemleri nedeniyle sorunlar doğurabilmektedir. Kullanıcı arabiriminin de geniş çaplı kullanımlarda nasıl olması gerektiği düşünülmesi gerekir. Parmak izi doğrulama, kullanıcılara yeterli eğitimin verilebileceği ev içi sistemlerde ve kontrollü ortamlarda kullanıma uygundur. Entegrasyon ve kullanım kolaylığı, düşük fiyatları ve küçük ebatları nedeniyle is istasyonu erişim sistemlerinde Parmak izinin yaygın bir kullanıcı kitlesi bulması şaşırtıcı değildir.

ii)El Geometrisi: İsminden anlaşılacağı üzere üç boyutlu bir perspektiften kullanıcının elinin ve parmaklarının fiziksel karakteristikleri esas alınır. En yaygın metotlardan biri olaraktan iyi performans sağlar ve kullanımı göreceli olarak daha kolaydır. Kullanıcı şayisinin fazla olduğu yâda sisteme çok fazla erişimin olmadığı ortamlarda ve fazla kullanım disiplini gerektirmemesi nedeniyle tercih edilebilir. Kararlılığın istenirse çok yüksek olabileceği gibi, esnek performans ayarları ve yapılandırma geniş uygulamalarda kullanıma izin verir. El geometrisi okuyucuları Personel Devam Kontrol

Sistemleri gibi senaryolarda popülerliğini kanıtlamıştır. Diğer sistemlere uyum ve kullanım kolaylığı el geometrisini birçok projede ilk adim olarak ön plana çıkarmaktadır.

iii)Ses Doğrulama: Günlük islerde ne kadar çok sesli iletişimin kullanıldığı düşünüldüğünde oldukça ilginç bir teknik olarak karsımıza çıkar. Bazı tasarımlar duvara monteli olarak karsımıza çıkarken bir kısmi da bilinen telefon cihazlarıyla entegre olarak kullanılırlar. Pazara birçok ses doğrulama ürünü girmiş olmasına rağmen çoğu lokal akustik ve âlici sorunları nedeniyle yetersiz kalmıştır. Ek olarak kullanıcı tanıtma işlemleri diğer biometriklere göre daha karışık olduğu için pek dostça karşılanmamıştır. Bununla birlikte birçok çalışma yapılması gerekmekte olup gelişmeleri izlemek ilginç olacaktır (Saday, 2005).

iv)Retina Tarama: Bir optik âlici vasıtası ile retinanın benzersiz şablonlarının düşük yoğunluklu bir ışık kaynağı ile taranmasına dayalı yerleşmiş bir teknolojidir. Kararlılığı kanıtlanmış bir teknik olmasına rağmen kullanıcının bir noktaya sabit bakmasını gerektirmektedir. Eğer gözlük kullanıyorsanız yâda okuyucu ile göz temasına girmekten endişe duyuyorsanız pek güvenilir bir yöntem değildir. Bu nedenlerden ötürü retina taramasının kullanıcılar tarafından kabullenilmesi zor olmakla birlikte teknoloji oldukça verimli çalışmaktadır. Doksanlı yıların ortalarında yeniden tasarımla son haline gelmiş olup gelişmiş bağlanılabilirlik ve kullanıcı arabirimi sağlamaktadır ama yinede marjinal bir biometrik teknoloji olarak görülmektedir.

v)İris Tarama: İris tarama, gözle ilgili biometrikler arasında şüphesiz en basitlerinden biridir. Basit sıradan bir cad kamera ile çalışır ve kullanıcı ile okuyucu arasında direk kontak olmasına gerek yoktur. Ek olarak, ortalamanın üzerinde şablon karsılaştırma potansiyeline sahiptir. Teknoloji olarak, üçüncü parti üreticilerin ilgisini çekmiş ve ilave ürünlerin ortaya çıkmasına öncülük etmiştir. Gözlükle birlikte kullanılabilmesi anlamında iyi çalışan birkaç cihazdan biri olarak kendini ispatlamıştır. Kullanım kolaylığı ve sistem entegrasyonu iris tarayıcılar için söylenmesi pek kolay olmamakla birlikte yeni ürünler tanıtıldıkça gelişmeleri takip edeceğimizi umuyoruz.

vi)İmza Doğrulama: İmza doğrulamanın diğer biometriklerde görülmeyen farklı yanları vardır. İnsanlar imzaya günlük işlemlerinde bir kimlik doğrulama aracı olarak kullandıklarından dolayı zaten alışıktırlar ve bunun biometrice aktarılmasında bir anormallik görmemişlerdir. İmza doğrulama sistemleri çalışmalarındaki kararlılığı ispatlamışlardır ve imzanın doğrulama aracı olarak kullanıldığı uygulamalarda yerlerini almışlardır. Ne yazık ki diğer biometrik ürünlere kıyasla çok az sayıda uygulaması görülmektedir

vii)Yüz Tanımlama: Oldukça fazla ilgi çeken ancak yetenekleri yanlış anlaşılmış bir tekniktir. Pratikte ispatlanması zor aşırı iddialar yüz tanımlamaya yapılmıştır. Tüm yapılan, sabit iki görüntünün karşılaştırılmasıdır (çoğu sistemin gerçekte yaptığı budur, biometrik ile pek ilgisi yoktur). Bir gurup içindeki kişinin kimliğini doğrulamak için kullanılır (bazı sistemler iddia etmektedir). Kullanıcı açısından yüz tanımlamanın çekiciliğini anlamak kolaydır, ama teknolojinin beklentileri konusunda realistim olmak gerekmektedir. şu ana kadar yüz tanımlama sistemleri uygulamalarda sinirli basarî sağlamışlardır. Ama çalışmalar devam etmektedir ve gelecekteki uygulamaların neler olacağını görmek ilginç olacaktır. Teknik zorluklar aşılabilirse, yüz tanımlamanın birincil

biometrik metod haline geldiğini görebiliriz. Sima, kulak memesi yâda birçok farklı parametreyi kullanan metotlar mevcuttur (Anonim 2003a).

3.1.3.3.1. Parmak İzinin Cep Telefonu Aracılığı İle Kimlik Doğrulamada Kullanımı

Cep telefonu tabanlı elektronik cüzdan uygulamaları ve buna bağlı olarak geliştirilecek ticari uygulamalar, mobil iletişim çağının yakın geleceği şekillendiren bir dinamizme sahip olacağını göstermektedir.

Yakın-Alan İletişim Teknolojileri (Near-Field Communication Technology) mobil cihazlar ekseninde kredi kartı ve benzeri nakit kartların kullanımını daha güvenli hale getirmektedir. Bu tür çalışmalarda cep telefonundaki elektronik cüzdan uygulamasında saklanan kart bilgileri üzerinden ödeme türü seçilerek gerekli ödeme yapmayı mümkün kılar.

Yakın Alan İletişim teknolojileriyle donatılmış olan mobil cihazlar güvenli bir geçit (gateway) aracılığı ile müşterilerin farklı bilgilere erişimini mümkün kılar. Bu şekilde kullanıcıların kredi kartı ve benzeri nakit kartlarının bilgilerini taşımakta ciddi bir alternatif olacaktır. Yakın alan iletişim teknolojilerine (bluetooth gibi) sahip cep telefonları bu şekilde benzer teknolojileri kullanan POS terminalleri ile iletişim kurarak ödeme yapmaya imkân tanıyacaktır. Burada tek sorun cep telefonunun kaybedilmesi halinde ilgili bilgilerin başkalarının eline geçmesidir.

Bu sorun, yukarıda bölümde izah edilen tekniğe benzer şekilde cep telefonlarının kullanıcısının parmak izini tanıması ve bu şekilde elektronik cüzdan uygulamasının aktif hale getirilerek aşılması mümkündür.

Cep telefonu aracılığı parmak izi tanımlaması yapmak için kullanıcının parmak izini okuyabilecek bir tarayıcının cep telefonuna montajı yapılabilir. Hâlihazırda cep telefonunu aktive edecek parmak izi doğrulamasının yapıldığı bir ticari ürün NTT DoCoMo Inc. Firması tarafından "biometrik telefon" satışa sunulmuştur. Telefon kullanıcısının daha önceden tanımlanmış parmak izini tarayıcısı aracılığı ile tanıyarak aktive olmakta ve erişim izni vermektedir (Kasavana, 2006) (Şekil 3.16).

Şekil 3.16. NTT DoCoMo Firmasının Biometrik Telefonu (Kasavana, 2006)

Cep telefonları bu tarz bir güvenlik adımıyla, ödeme yapma ve benzeri ticari işlemleri güvenlikli bir şekilde yapmaya imkân sağlayacaklardır.

Bu teknolojinin kullanımı cep telefonunun iç yazılımına yeni bir menünün ve tanıma işini gerçekleştirecek yazılımın eklenmesi barındıracak bir yonganın telefonun donanımına gömülmesi ile mümkündür.

Nokia firması benzeri bir uygulamayı Nokia NFC kabuğu-teknolojisi adı altında 3230 modeline koymuştur. Bu telefon uygun bir POS'a dokunarak NFC yongasında saklanmış olan kredi kartı ve benzeri kişisel bilgilerin kullanımını ödemeler sırasında karşılıklı değiştirerek, ödeme yapmayı mümkün kılmaktadır (Kasavana, 2006).

NFC uygulamalarının cep telefonlarına eklemlenmesi sayesinde temassız ödeme sistemleri gerçeklenebilmektedir. Bu alan ister istemez yakın bir gelecekte yaygınlaşarak, kredi kartı uygulamalarının ve benzeri uygulamaların yerini almaya adaydır.

3.1.3.3.2. İris'in Cep Telefonu Aracılığı İle Kimlik Doğrulamada Kullanılması

Her insandan diğerine değişen iris tabakasının parmak izi gibi kimlik doğrulaması için kullanılması mümkündür. Bu doğrulama türü klasik bilgisayar tabanlı sistemlerin yanında gündelik hayatın bir parçası olan çokluortam telefonlarının da ilgi alanına girmiştir.

Kamera eklentisi olan mobil telefonlar ve PDA'lar için OKI firması tarafından gerçekleştirilen "iris doğrulama" tekniği cep telefonlarının güvenlik anlamında kullanılması için yeni ve ilginç bir örnektir.

Şekil 3.17. Mobil Cihazlar İçin İris Tanıma Uygulaması (Anonim, 2006b)

Oki Electric tarafından yapılan bu sistem OKI'nin mobil terminaller için iris tanıma algoritmasının kameralı cep telefonlarına uyarlanması şeklinde gerçeklenmiştir. Bu ürünün ticari satışına ise 2007 yılında başlanacağı düşünülmektedir.

Bu doğrulama teknolojisi sayesinde kullanıcının geleneksel PIN kodu girme ve benzeri uygulamalar yerine sadece "iris" ile daha kolayca ve yüksek bir kesinlik ölçeğinde kimlik doğrulaması yapması sağlanmaktadır (Anonim, 2006b).

Mobil ödeme terminallerinin dağıtıklığı ve sofistike bir hal alması güvenlik sorununu beraberinde getirmektedir. Bu ekipmanların yanlış kullanımı veya çalınması durumunda kullanımının engellenmesi isteği güvenlik beklentilerini de değiştirmiştir. Bu güvenlik ihtiyacına verilen cevaplardan birisi de her insandan insana değişen gözdeki iris tabakası ile kimlik doğrulamasıdır. Bu ağ yapısının taklidi imkânsız derecede karmaşık oluşu onun güvenlik sistemlerinde yüksek bir kesinlikle kullanılmasına izin vermektedir.

Klasik iris kimlik doğrulama sistemlerinde bir kızılötesi kamera bulunur ve doğrulama için örnekleme bu kamera vasıtasıyla güçlü bilgisayarlar kullanılarak gerçekleştirlir. Cep telefonlarındaki klasik kameralar ve cep telefonlarındaki işlemci kapsitesi düşünüldüğünde uygulamanın zorluğu ortaya çıkar. OKI bu teknolojiyi cep telefonlarındaki işlemci kapasitesi ve kamera yeteneğine uygun şekilde geliştirerek uygulanabilir bir hassaslık seviyesini yakaladığını duyurmuştur (Anonim, 2006b).

Cep telefonu ve benzeri mobil cihazlar üzerinde iris tabanlı kimlik doğrulaması ister istemez mobil güvenliğin gelecekte ulaşacağı gelişim ve yaygınlık hakkında ciddi ipuçları vermektedir.

3.1.3.3.3. İnsan Yüzünün Cep Telefonu Aracılığı İle Kimlik Doğrulamada Kullanılması

Cep telefonlarının çokluortam özelliklerinin gelişmesi ile beraber, telefonların bu özelliklerine uygun güvenlik sistemlerinin geliştirilmesi için sürekli çalışmalar yapılmaktadır. Bu çalışmalar kameralı cep telefonlarında yüz tanıma ve bu esasa dayanarak kimlik doğrulama şeklinde ürünleri sonuç vermiştir.

Vodafone firması tarafından duyurusu yapılan ve yüz tanıma ile güvenliği sağlayan cep telefonu bu çalışmalardan birisidir.

Cep telefonu, kullanıcısının resmini kamerası tarafından çekerek üzerindeki yazılım aracılığı ile bir referans kayıt oluşturmaktadır. Cep telefonu kilitlendikten sonra kilidin açılması için kullanıcının kamerası ile yeni bir resim çekmesi ve bu yeni resmin referans resim ile karşılaştırılarak doğrulanması gerekmektedir.

Bahsi geçen sistem kameranın aynı pozisyonda olmasa dahi kullanıcının yüzünü çektiği frame içersinden ayırt edebilmesini mümkün kılacağı ifade edilmektedir.

3.1.3.3.4. İnsan Sesinin Cep Telefonu Aracılığı İle Kimlik Doğrulamada Kullanımı

Cep telefonlarının güvenlik anlamında diğer bir kullanım alanı da ses ile kimlik doğrulaması yapılmasıdır. Bu uygulama alış veriş ve bu işlemin müşterinin kimliğini doğrulaması şeklinde gerçeklenir.

Telefon aracılığı ile kimlik doğrulama seçeneği müşteriye ait özel bilgilerin (doğum tarihi, anne kızlık soyadı vs) müşteriden talep edilmesi esasına dayanır. Klasik güvenlik doğrulama sadece müşterinin bildiği varsayılan bilginin müşteriden talep edilmesi gerekirse bu tarz bilgilerden bir kaçının sağlanması (müşterinin bilip bilmediğinin kontrol edilmesi) esasına dayanır. Bu işlem hem sıkıcı hem de uzun bir süreci gerektirebilir. Bazen müşterinin yoğunluğa göre bekletilmesi ve bu işlem sırasında geçen zamanın telefon maliyetlerini arttırması istenmeyen sonuçlardır. Telefon bankacılığı ve benzeri servisler bu tarz bir hizmet için ister istemez yukarıda sözü edilen süreçleri gerektirirler.

Ses tanıma sistemleri ise sözü edilen sorunlara bir çözüm olarak ortaya çıkar. Kullanıcının bahsi geçen süreç yerine sesinin tanınması ile, kimlik doğrulama sürecinin kısaltılması hedeflenen bir noktadır. Ancak bu teknolojinin kullanımı bazı soru ve sorunları beraberinde getirir:

i) Bu teknolojiyi hangi müşteri segmenti kullanacaktır?
ii) Teknolojinin müşterilerin risk almayacağı nasıl garanti edilecektir?
iii) Sistemin hassaslığı güvenliği sağlamaya yetecek midir?

Anovea Authentication Teknoloji şirketi bahsi geçen sorunlara kullanıcı eksenli bir ses tanıma çözümü sunmuştur (Anovea, 2003). Sistem doğrulama için, parmak izi veya iris taramaya benzer şekilde sesteki karakteristikleri yani "ses izlerini" referans olarak kullanır. Ses tanıma sistemini çekici kılan, kullanıcıyla fiziksel temasa gerek duyulmaması kullanıcının ses örneğinin karşılaştırmanın yapılacağı veritabanına gönderilmesinin (bunun için üretilmiş özel bir yazılımın kurulu olduğu bir mobil cihazın kullanılması) kolay olmasıdır.

Bu sistem GPS ile birleştirildiğinde farklı seçeneklerin, güvenliği arttıran değişik seçeneklerin ortaya çıkmasını da beraberinde getirir. Çoğu uygulamada sadece bir tek

şifreye dayanan güvenlik teknolojisi kullanılırken bu teknikte, cihazın güvenliği, coğrafik konumun sorgulanabilmesi ve ses tanıma sistemi gibi üç ayrı güvenlik tekniği birleşir (Anovea, 2003).

Teknoloji temel olarak java tabanlı bir uygulama çalıştıran cep telefonu ile alınan ses örneğinin bir sunucu üzerindeki ses örneği ile karşılaştırulması ve kimliğin doğrulanması esası ile çalışır.

Sistemin bankacılık, hastahane ve benzeri ortamlarda da güvenliğin sağlanması için kullanılabileceği öngörülmektedir.

Hemen hemen herkesin cep telefonu kullandığı ve en alt modellerin dahi java yazılımlarını çoğunlukla destekliyor olduğu düşünüldüğünde, bu tarz bir güvenlik doğrulams teknolojisinin kullanımının yaygınlaşma ihtimali daha çok dikkat çekecektir.

Kullanılan teknoloji, yapı itibariyle çokluortam özelliklere sahip cep telefonlarındaki görüntü (yüz) doğrulama teknolojisi ile benzerlik taşır. Bu konu daha sonra detaylı şekilde incelenecektir.

3.1.4. MMAPI Temelleri

Bir mikro java uygulamasına audio/video yakalama ile ilgili yeteneklerin kazandırılması için, MMAPI (Mobil Media API-Hareketli Medya API'leri) yapısının bilinmesi gereklidir.

Mobil cihazlardaki çokluortam yeteneklerin mikro-java sürümü ile programlanması, bir medyanın yönetilmesi, kontrol edilmesi MMAPI kavramının sağlıklı kullanılması ile mümkündür.

Dijital MP3 cihazlarının ve kameralı cep telefonlarının yoğun kullanımı mobil cihazlarda çokluortam uygulamalarını kullanmanın önemini göstermektedir. Bu tür uygulamaların java cihazlarına uyarlamasının temeli J2ME Mobile Media API (MMAPI)'lerine dayanmakta olup, bu API'ler java üzerinde çokluortam yetenekli uygulamalar yazılmasına izin verirler.

Bu bölümde MMAPI temellerinden söz edilecektir.

3.1.4.1. MMAPI'ye Giriş

MMAPI'lerin en güçlü özelliklerinden birisi hangi protokol (http veya rtp) veya medya formatı (MP3, MIDI veya MPEG-4) olursa olsun destekleyebilmesidir.

MMAPI tasarımı gereği J2ME-tabanlı hangi sanal makine olursa olsun (CDC ve CLDC sanal makineleri başta olmak üzere) üzerinde çalışmaktadır. J2ME'nin kablosuz araçkiti bir MMAPI ile birlikte gelir (Sharp, 2005).

MMAPI'ler uygulama geliştiricileri izleyen özelliklerle desteklerler:

i) Ses Üretimi, Ortam Yürütme, ve zamana bağlı medya (audio-video) kaydı.

ii) Düşük kaynak tüketimi (CLDC cihazlarının sınırlı hafızları bağlamında).

iii) Protokol ve İçerik Duyarsızlığı (API spesifik bir içerik yada protokolü tanımaya zorlanmamıştır).

iv)Genişletilebilme (Yeni özellikler fonksiyonelliği bozmadan eklenebilirler)

vi)Uyarlayıcılar için seçenekler (API farklı amaçlar için farklı seçenekler sunar)

3.1.4.2. MMAPI Kullanımı İle Çokluortam İşleme

MMAPI'ler ile çokluortam işleme iki bölümden oluşan bir işlemdir:

i) Protokol İşleme: Veriyi bir dosya veya sunucu gibi bir ortamdan okuyarak medya işleme ortamına aktarmak.

ii) İçerik İşleme: Veriyi pars ederek-çözerek bir çıkış cihazına (hoparlör veya ekran) göndermek.

Bu iki işlemi gerçeklemek için API iki yüksek seviyeli nesne sağlar. Bu nesneler DataSource ve Player nesneleridir.

DataSource nesnesi, protokol işlemlerini gerçekleştirerek verinin kaynaktan nasıl okunduğunu saklar. Bu nesnenin metod'ları Player nesnesinin içeriği işlemesini sağlarlar.

Player nesnesi veriyi DataSource nesnesinden okuyarak veriyi uygun bir çıkış cihazına (hoparlör, ekran vs.) yönlendirir. Bu nesne değişik medya türlerinin yürütülmesi-yönetilmesi ile ilgili kontroller için metot'lar sağlar.

MMAPI'nin bir üçüncü önemli medya nesnesi Manager'dir. Bu nesne uygulamanın DataSource nesnesinden ve InputStream nesnelerinden Player'lar üretmesine imkan tanır. Manager nesnesi API'ye en yüksek giriş noktası olan createPlayer() metodunu sağlar. Aşağıdaki kod parçası bu metodun kullanılışına bir örnektir (Sharp, 2005).

```
Player player = Manager.createPlayer(String url);
```

Burada url protokol ve içeriği [(<protokol> : <içerik adresi>) formatında] tanımlar. Uygulama medyayı yürütmek için geri döndürülen Player'a ait metod'ları kullanır. Uygulamanın yaşam döngüsü UNREALIZED, REALIZED, PREFETCHED, STARTED, ve CLOSED durumlarını içerir. Bir player oluşturulduğunda UNREALIZED durumundadır. Eğer realize ( ) metodu çağrılırsa player, REALIZED durumuna geçer ve media çalma ortamının ihtiyaç duyacağı bilgiyi başlatır. Prefetch ( ) metodunun çağrılması nesneyi PREFETCHED durumuna taşır ve nesen bu durumda iken sürekli-veri için ağ bağlantılarını başlatır. Start ( ) metodu nesneyi STARTED durumuna değiştirir ve player bu durumda veriyi işleyebilecek konumdadır. Medyanın sonuna gelindiğinde yani veri işleme sona erdiğinde player önce PREFETCHED durumuna döner ve sonra close ( ) metodunun çağrılmasıyla CLOSED durumuna geçer (Knudsen, 2003).

Bir player işlediği medya türüne özgü kontroller sağlar. Örneğin MIDI ortamı için player getControl ( ) metodunu çağırarak bir MIDIControl elde eder.

MMAPI üç tür paket içerir. Bu paketler Manager (player gibi sistem bağımlı kaynaklar için erişim noktası) sınıfı ve bazı arayüzler içeren javax.microedition.media

paketi, bir player ile birlikte kullanılabilecek VolumeControl, VideoControl gibi kontrolleri içeren javax.microedition.media.control paketi ve özel kontrolleri için protokolleri işlemeye yarayan javax.microedition.media.protocol paketleridir.

Bu paketlerde içerilen sınıflar, arayüzler, ve exceptions (istisnalar) aşağıdaki tablolarda özetlenmişlerdir (Mahmoud, 2003).

Çizelge 3.2. MMAPI Sınıfları (Mahmoud, 2003)

Paket	**Sınıf**	**Tanım**
javax.microedition.media	Manager	Player gibi sistem bağımlı nesnelere sistem kaynaklarını sağlar
javax.microedition.media.protocol	ContentDescriptor	Medya Türlerini Tanımlar
javax.microedition.media.protocol	DataSource	Player için ortam kontrollerini sağlar

Çizelge 3.3. MMAPI Arayüzleri

Paket	**Arayüz**	**Tanımlama**
Javax.microedition.media	Control	Medya işleme ile ilgili fonksiyonları sağlar
Javax.microedition.media	Controllable	Bir nesneden kontrolleri döndürmek için arayüz imkanı sağlar
Javax.microedition.media	Player	Medya verisini render etmek ve player nesnesinin yaşam döngüsünü kontrol etmek için metodlar sağlar
Javax.microedition.media	PlayerListener	Player'lar tarafından üretilen olayları işler
Javax.microedition.media	TimeBase	Medya ortamının zamana bağlı senkronizasyonunu sağlar.
Javax.microedition.media.control	FramePositionControl	Player'da video frame'inin hassas yerleşimini destekler
javax.microedition.media.control	GUIControl	GUI bileşeni destekleyen kontroller tarafından kullanılır
javax.microedition.media.control	MIDIControl	MIDI render ve render edilen veriyi ilgili cihazlara iletme işlevleri
javax.microedition.media.control	RateControl	Player'ın ortam yürütme hızının belirlenmesi
javax.microedition.media.control	RecordControl	Player'dan medya kaydını kontrol eder
javax.microedition.media.control	StopTimeControl	Player'ın önceden belirlenmiş bir zamanda durdurulması işlevi
javax.microedition.media.control	VideoControl	Video'nun görüntülenmesini kontrol eder
javax.microedition.media.control	VolumeControl	Player'ın sesini kontrol eder
javax.microedition.media.protocol	SourceStream	Player'a giriş ara yüzü olur

Çizelge 3.4. MMAPI İstisnaları (Exception)

Package	**Exception**	**Description**
Javax.microedition.media	MediaException	Medya işleme metodlarında, yürütme sırasında ortaya çıkan beklenmeyen durumları rapor eder

3.1.4.2.1. MMAPI İle Ses İşleme

Mobil cihazların gelişen çokluortam yetenekleri ile güvenlik (ses, görüntü tanıma) veya medikal tanı sistemlerinde (web üzerinden kablosuz görüntü alışverişi) kullanılması ile ilgili uygulamalar ve b yöndei araştırmalar yoğun şekilde devam etmekte ve bir kısmı teorik araştırmalardan pratik güncel uygulamalara geçmiştir.

Bu bölümde öncelikle ses tanıma, ses kontrol uygulamalarında önem taşıyan ses MMAPI'leri incelenecektir (Mahmoud, 2003).

MMAPI dokümanları mikrofondan ses yakalama işlevini gerçeklemek için

Player p= Manager.createPlayer("capture://audio");

kodunu kullanmayı tavsiye eder. Bu şekilde kayıt edilen ses tekrar dinlendiği zaman kalitesi düşük bir çıkış elde edilmiş olur. PCM formatındaki sorunlardan dolayı kötü çıkan ses için player oluşturulurken

Manager.createPlayer("capture://audio?encoding=pcm&signed=unsigned");

Manager.createPlayer("capture://audio?rate=8000&bits=16");

eklemesi yapılmalıdır.

Örneklenen sesin işlenmek için kayıt edilmesi istenir. Bu durumda sesi saklayacak ve tekrar dinlemeyi sağlayacak kod parçası aşağıdaki şekilde olur.

```
RecordStore store; // kayıt işlemi
        int id;
        // kayıttan tekrar yürütme
        try {
        InputStream is = new ByteArrayInputStream
        (store.getRecord(id));
        Player player = Manager.createPlayer(is, " capture://audio ");
        p.start();
        }
        catch (IOException ioe) {
        }
        catch (MediaException me) {
        }
```

Mobil cihazlarda ses doğrulama ile kimlik denetimi işlemleri bu tarz MMAPI'lerin etkin kullanımını gerektirirler.

Mobil cihazın kişinin sesini bir şekilde kayıt edip doğrulamayı yapacak sunucuya göndermesi ses ile doğrulamanın istemci tarafındaki yapıdır. Öte yandan ses örneği ile kişinin sunucuda kayıtlı sesinin karşılaştırılabilemesi için sunucuda güvenlik doğrulaması yapılan kişiye ait ses örneği bulunmalıdır. Bu ses örneği kişinin belli bir sesi-kelime dizisini birkaç kere söylemesi ile sesi örneklenen kişiye ait akustik bir modelin oluşturulması ile elde edilir. En nitelikli sonuçlar, ses örneklemesi yapılan kişinin nümerik

bir kodu arka arkaya birkaç kez tekrar etmesi ile elde edilir. Akustik model, sesin tüm ayırt edici ve kişiye özgü karakteristiğini ortaya koyar. Elde edilen model kullanıcının hasta olması durumunda bile sesin ayırt edilmesini sağlar (Mahmoud, 2003).

MMAPI, J2ME mobil setin desteklediği farklı audio and türlerini destekler. Desteklenen ses türleri PCM, WAV ve MIDI şeklindedir.

3.1.4.2.2. MMAPI İle Görüntü Yakalama

Bir mobil cihaz kamerası ile kullanıcının görüntüsünü yakalama ve sonra bu görüntüyü web üzerinden kimlik doğrulama, tıbbi görüntüleme (teleradyoloji uygulaması) gibi uygulamalarda kullanma günümüz mobil yaşamının bir parçası olmak üzeredir.

Teleradyoloji uygulaması Motorola MPx 200 cep telefonu kullanılarak gerçekleştirilmiş ilginç bir mobil uygulamadır. Bir hastaya ait görüntülerin uzaktan görüntüleme yöntemiyle incelenmesinde kullanılan bu uygulama, bir görüntü yakalama ve Web üzerinden GPRS ile sunucuya aktarılma uygulamasıdır (Pantelis, 2000).

Cep telefonu aracılığı ile görüntü yakalama ve yakalanan görüntünün kimlik doğrulama anlamında kullanılması ile ilgili çalışmalar devam etmektedir. Bu konudaki örnek bir çalışmayı incelemeden önce MMAPI'lerin kameralı mobil cihazlar yardımıyla görüntüyü nasıl yakaladıklarını inceleyelim (Knudsen, 2003):

Bir mobil cihaz kamerasından görüntüyü almak için öncelikle bir player oluşturulmalıdır. Bunun için aşağıdakine benzer bir kod yapısı kullanılır.

Player player;…player=Manager.createPlayer("capture://video");

Bu adımdan sonra player'ın başlatılması (initialize) edilmesi gerekir. Player'ı başlatmak player.realize(); metodunun kullanılmasıyla olur. Bu noktada görüntülenecek kişiyi canlı şekilde ekrana taşıyan video kontrolü kullanılmalıdır.

VideoControl videoControl;…videoControl=(VideoControl)player.getControl ("VideoControl");

Video kontrol'ün iki görüntüleme modu vardır. Bu kontrol ya kendini düşük seviyeli UI Canvas nesnesine çizer veya görüntü yüksek seviyeli bir MIDP UI Form'una çizdirilebilir.

Görüntüyü Canvas üzerine çizdiren kodumuz;

videoControl.initDisplayMode(VideoControl.USE_DIRECT_VIDEO,canvas);

şeklinde olacaktır. Bu durumda player'ın başlatılarak kullanıcının kameranın neyi gösterdiği (nereye yöneldiği) hakkında bilgilendirilmesi gerekir. Bunun için

player.start();

kodu ile player başlatılır. Player'ın aktif olduğu bu durumda artık snapshot adı verilen anlık görüntü alınabilir. Bunun için de png formatında görüntü alma işlevini gerçekleştiren

byte[]pngData=videoControl.getSnapshot(null);

kodu kullanılmalıdır.

İsternirse görüntü için png dışında bir format tanımlanabilir. Eğer kod "null" değeri ile gerçeklenirse png formatı seçilirken, null ifadesi başka bir format türü ile değiştirilirse onun kabul edilmesi sağlanır.

Elde edilen bu veri bir "record store" (ses API'lerinde olduğu gibi) da sonraki kullanımlar için saklanabileceği gibi, arzu edilirse http üzerindeki bir sunucuya gönderilebilir veya

Imagephoto Img=Image.createImage(pngData,0,pngData.length);

kodu ile ekranda direkt olarak görüntülenebilir (Knudsen, 2003).

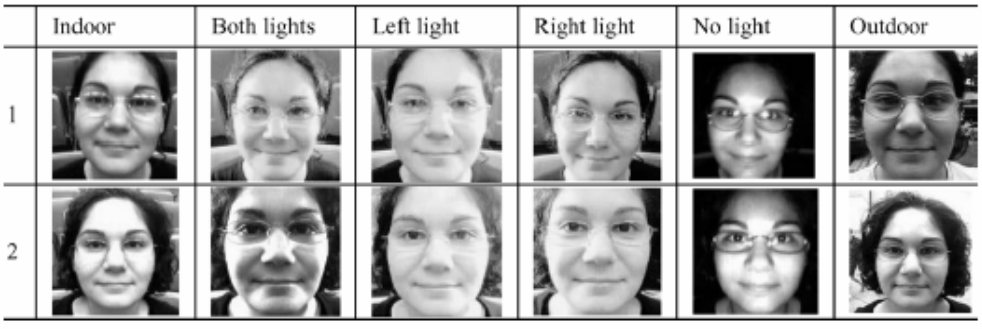
3.1.4.2.2.1. Cep Telefonu İle Örnek Bir Yüz Tanıma Uygulaması

Bir cep telefonu kullanılarak çekilen yüz görüntülerinin bir veritabanındaki görüntülerle karşılaştırılarak tanınması uygulaması elbette mobilize olmuş sosyal hayatın içerisinde kendine güçlü bir uygulama alanı bulmaya adaydır.

Klasik görüntü (yüz) tanıma algoritmaları yüksek çözünürlüklü kameralar kullanılarak gerçekleştirilen uygulamalarda oldukça başarılı sonuçlar elde edilmektedir. Ancak, gerçek hayattaki olumsuz aydınlatma koşulları, ortalama veya düşük çözünürlüklü resimler bu çalışmaların gelmesi gereken noktayı temsil etmektedir. Cep telefonu veya PDA cihazlarındaki kameraların kullanıldığı çalışmalarda verimin arttırılması için farklı yüz tanıma algoritmaları test edilmiştir. Halen yüz tanıma algoritmaları olarak bilinen algoritmalardan birisi PCA (eigenface görüntü tanıma temeli üzerine inşa edilmiştir) ve diğeri ise FisherFaces (Fisherfaces adı verilen görüntü tanıma tekniği üzerine inşa edilmiştir) algoritmalarıdır.

Carnegie Mellon Üniversitesinde cep telefonu kamerası kullanılarak bu algoritmalardan hangisinin bu tarz düşük seviyeli bir çözünürlük düzeyinde başarılı olacağı araştırılmıştır (Vijayakumar, 2005).

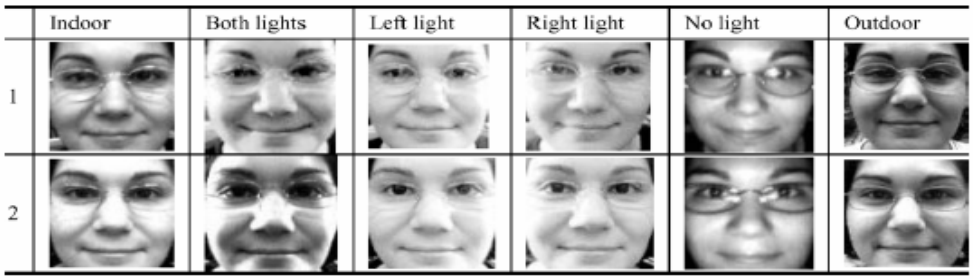
Görüntülere ait veritabanının oluşturulması için bir cep telefonu kamerası (1.7 megapiksel'lik çözünürlüğe sahip) ile farklı aydınlatma koşullarında (açık hava, ışıksız ortam, sağdan-soldan aydınlatma vs) kişilere ait yüz örneklemeleri yapılmıştır.



Şekil 3.18. İşlenmemiş Ham Veritabanı Kayıtları

Kayıtların işlenerek yüz tanımanın gerçekleşmesi için şu şekilde bir sıra takip edilmiştir:

Öncelikle gözer arasındaki mesafeler belirlenmiş ve gözlerin konumu tespit edilmiştir. Aynı şahsa ait ilk görüntüdeki göz konumlarını bulmak için manüel bir yol seçilmiş sonra bu referans imajdan oluşturulan UOTSDF filtresi kullanılarak geri kalan resimlerin (aynı kişi için) göz konumları otomatik olarak bulunmuştur. Son olarak tüm resimler üzerinde kontrast ve ışık ayarlamaları yapılarak resimler normalize edilmiş ve tüm resimlerin ortak bir enerji seviyesine sahip olması sağlanmıştır.



Şekil 3.19. İşlenmiş Veritabanı Kayıtları

Farklı filtreleme teknikleri kullanılarak yapılan testlerde ulaşılan sonuçlara göre PCA tekniğinin modifikasyonu ile daha sağlıklı sonuçlar elde edilebilsede cep telefonu kemerası ile elde edilen görüntülerin işlenerek yüz tanıma (ya da kimlik doğrulama) amacıyla kullanılması için henüz yeterli sonuçlar üretilememiştir (B. V. K. Vijayakumar, 2005).

3.1.4.3. MIDP ve MMAPI Güvenliği

İnternet gibi güvenli olmayan bir ağ üzerinde haberleşen cihazların authentication adı verilen bir işlem ile kimliklerini birbirlerine ispatlamak durumundadırlar. MIDP 1.0 authentication (doğrulama) için direkt API desteği sağlamazken, MIDP 2.0 HTTPS ile sunucu authentication'ı sağlar. Ancak ne yazık ki MIDP 2.0 istemci doğrumala mekanzimaları konusunda eksiktir.

En güvenli doğrulama metotları şifre adı verilen veherkesçe bilinmeyen bilgi parçacıklarına dayanır. Şifreyi bildiğinizi göstermek veya özel bir anahtara sahip olduğunuzu ispat etmek doğrulamanın iki tekniğidir.

Ağ iletişimi servis isteyen istemci ve servisi sağlayan sunucu olmak üzere iki cihazı içerir. Bu iki cihaz söz konusu olduğunda bunlar arasında doğrulama iki türlü yapılır:

i)Sunucu Doğrulaması: Sunucu kimliğini istemciye ispatlar. MIDP 2.0, bir HTTPS uyarlaması olan X.509 sertifikaları aracılığı ile direkt olarak sunucu doğrulamaya imkan tanır.

ii)İstemci Doğrulaması: İstemci kimliğini sunucuya doğrular.

Tipik bir doğrulama örneği, bir Web sayfası üzerinden online alış veriş sırasında yapılan kimlik doğrulamasıdır. Müşterinin alacağı malları sepete eklemesi ve sonra gerekli kart bilgilerini-adresi girerek alış verişi tamamlaması sırasında yapılan kimlik doğrulaması bir sunucu doğrulaması (HTTPS bağlantısı üzerinden) olur (Knudsen, 2002).

Bir sunucunun kimliğinin doğrulanması DNS (Domain Name System) doğrulamaya dayanır. Ancak bu doğrulama IP adreslerinin, DNS tablolarının bir şekilde yönlendirilebileceği gerçeği düşünüldüğünde kesinlik sağlamayacağı açıktır. Kriptoğrafik tekniklerin uygulanmadığı bir doğrulama sisteminde istemcinin doğru sunucuya bağlandığının garantisi yoktur.

Web tabanlı eticaret siteleri bu nedenle kimliklerini (sunucu kimliği) ispatlamak için TLS (Transport Layer Security) düzeyindeki handshake sırasında, kriptolojik sertifikalarını (kullanıcının browser'ında gömülü sertifika sağlayıcılardan birinden alınmış olması gerekir) yani yasal bir sunucu olduklarını istemciye iletirler.

Bu teknik browser tabanlı istemciler ve MIDP istemcileri için sağlıklı şekilde çalışan bir yapıdır. MIDP 1.0 spesifikasyonu HTTPS desteğini içermese de, bir çok MIDP 1.0 cihazı http üzerinden TLS ve SSL yapılarını destekler.

Genel olarak HTTPS geliştiriciler ve kullanıcılar için uygun bir çözümdür. HTTPS tabanlı güvenlik sertifikası sunucunun bu sertifikayı gösterip kendini doğrulaması düzeyinde basit bir yaklaşım değildir. Burada sözü edilen sertifika genel bir anahtar (public key) içerir ve bu anahtar serbestçe dolaşımda olan bir anahtardır. Sunucu kendisini doğrularken sertifikadaki genel anahtara karşılık gelen özel bir anahtarı (private key) bildiğini istemciye iletir. İstemci bu genel anahtarı kullanarak bir şifreli değer elde eder ve bunu sonraki iletişimde kullanır. Eğer sunucu istemciden gelen bu şifreli değeri elde edemez ise bu durumda kendisinin doğru sunucu olduğunu ispat edemez ve iletişim kesilir (Knudsen, 2002).

MIDP uygulamaları için SSL ve TLS uygun protokoller olarak ortaya çıkarlar. Çünkü bu protokoller kablosuz eticaret uygulamaları için yeterli desteği sağlarlar.

Sunucu tarafı doğrulama göz önüne alındığında istemcinin bir MIDlet veya normal bir browser olmasının farkı yoktur. Ancak istemci tarafı doğrulama dikkate alındığında ortaya farklı taraflar çıkar. Çünkü Web uygulamaları ile MIDP uygulamaları kullanıcılarıyla farklı bir etkileşim tarzı içindedirler.

İki tür istemci arasındaki en belirgin fark sahiplik kavramından kaynaklanır. Web uygulamaları her hangi bir makineden veya her hangi bir browser'dan erişilebilen uygulamalardır. Bu uygulamalarda browser'ın sahibinin olup olmaması (ki zaten umuma açık internet kafe gibi ortamlarda bu tarz bir sahiplikten söz edilemez) durumu yoktur.

J2ME cihazlarındaki browser'lar ise çalıştıkları cihaz bir şahsa ait olduğu için kendileri de sahiplenilmiş olur. Bu kullanıcının şifre bilgisini cihazın kendisi üzerinde saklayabilmesi imkanını tanır.

Web doğrulama tekniklerinden alınmış bir teknik şifre doğrulamasıdır. Burada kullanıcı bir kullanıcı adı ve bir şifreyi girer. Girilen bu değerlerin doğruluğu bir veri tabanındaki bilgiler ile karşılaştırılır. Bu iki bilginin aynı anda doğru olması durumunda kimlik doğrulanmış olur. Bu yaklaşımın temel iki sorunu vardır. İlk sorun kullanıcıların kötü (kolay tahmin edilebilir) şifreler seçmeleri ve şifrelerin gizliliğinin sağlıklı şekilde devam ettirilmemesidir. İkinci sorun ise basit şifre doğrulamada istemcinin gizli verisinin açık bir metinsel ifade ile sunucuya gönderilmesidir. Bu problem şifre bilgisinin şifreli bir bağlantı (HTTPS gibi) üzerinden gönderilmesi ile azaltılabilir. Diğer çözüm yöntemi ise istemci sunucu arasında şifrenin değil, şifrenin sağlamasının (SHA gibi bir algoritma yardımı ile) karşılıklı değiş tokuş edilmesidir (Knudsen, 2002).

MIDP'de bir kullanıcı ve şifre HTTP veya HTTPS URL'si ile aşağıdakine benzer şekilde uyralanabilir:

```
String user = "ahmet";
String password = "kitap2007";
String base = "https://somehost.com/someservlet";

String url = base + "?user=" + user + "&password=" + password;

HttpsConnection hc = (HttpsConnection)Connector.open(url);
```

Her MIDP cihazı bir kişiye ait olduğu için şifre ve kullanıcı bilgisi cihaz üzerinde saklanabilir. Ancak cihazın çalınma riskine karşılık bu veriler bir elektronik cüzdan uygulaması içinde şifrelenebilir: Bu elektronik cüzdanın kullanıcıya açılması ise parmak izi veya benzeri bir biometrik parametreye dayandırılarak şifre güvenliği sağlanabilir.

İstemci doğrulamasının "message digest" adı verilen bir başka teknik ile yapılması mümkündür. Bu uygulama şeklinde istemci şifrenin ve benzeri gizli bilginin kendisi yerine o verinin digest'ini (SHA gibi bir özel tersinmez algoritma yardımıyla şifrelenmesi) gönderir.

İstemci doğrulamasında sertifikaların öneminden daha önce bahsedilmişti. Eğer doğrulama bilgisi istemci uygulamasına gömülecekse, X.509 adı verilen sertifikalar yardımıyla istemci sunucuya doğruluğunu ispat edebilir (Knudsen, 2002).

3.1.4.4. CLDC Perspektifinden Mobil Java Güvenliği

J2SE güvenlik uygulama türleri bu mekanizmaların hafıza gereksinimlerinden dolayı CLDC (veya MIDP) uygulamaları için uygun değillerdir. Daha detaylı bir bakış için J2SE ve applet güvenlik modeli incelenmelidir.

J2SE güvenliği üç katmandan oluşmaktadır. Bunlar Java'nın kendisi, Java derleyicisi ve run-time sistemi ve SecurityManager 'dır.

Dil katmanında java güvenliğini farklı şekillerde sağlar. Öncelikle java veri türleri makinenin mimarisinden bağımsız olarak kendine özgü uzunluktadır. İkinci olarak, pointer

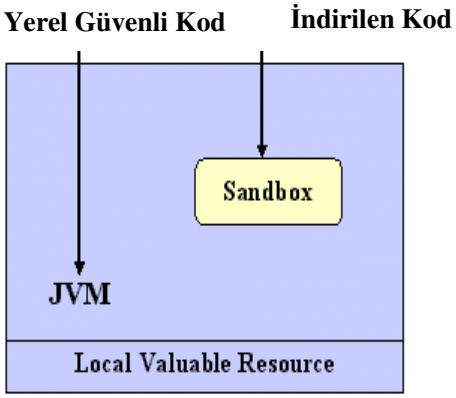
kavramı ya da dışarıdan nesnelere erişim izni yoktur. Üçüncüsü, java'nın array-bound kontrolü (array'ların belirli indeks değerlerinin sağlanması) yaparak, bunu ihlal eden durumlarda bir exception (istisna) üretmesidir.

Java derleyicisi ve run-time sistemi güvenlik katmanı sistemin geçersiz bir kod'la manipülasyonuna engel olacak önlemlere sahiptir. Bunlar class (sınıf) dosyalarının kontrolü, çalışma zamanında kütüphanelerin kontrolüdür. Bunun anlamı hiçbir sınıfın JVM tanımlamasına uygun olmayan tarzda çalıştırılamamasıdır.

Bu ilk iki katman java sisteminin geçersiz bir kodla manipüle edilmesinin önüne geçer. Ancak Java sistemi istemci-sunucu uygulamasında yabancı komutların işlemesini engelleyecek her hangi bir mekanizmaya sahip değillerdir. Bunun için JDK 1.0 SecurityManager sınıfını bir applet veya güvenilir olmayan bir uygulama yüklendiğinde kodun ne yapıp yapamayacağını belirleyerek, özel bir güvenlik yaklaşımı uygulamaya imkan tanır (Mahmoud, 2002).

Bu üç katman "sandbox" adı verilen ve güvenli olmayan applet'ler ile uygulamaların çalıştırılabileceği bir sınırlı ortamın oluşturulmasında kullanılır. Sandbox güvenliğinin arkasındaki temel fikir yerel kodun güvenilir olduğu ve altta yatan dosya sistemine serbestçe ulaşabileceği, indirilen bir uygulamanın ise güvenilir olmadığı (varsayım) ve sistem kaynaklarına sandbox içerisinden ancak sınırlı şekilde ulaşabileceğidir. Bu model Şekil 3.20 de gösterilmiştir.

Bir kullanıcı bir siteyi ziyaret ettiğinde bir applet'in çalışması için onun kullanıcının makinesine indirilmesi ve orada çalıştırılması gerekir. Bu durumda güvenliğin sağlanması için applet'in sanbox ortamında çalıştırılması (yani yerel değerleri okuma, yerel değerlere yazma dolayısıyla kullancının dosyalarına erişmesinin engellenmesi) istenen bir durumdur. Gerektiğinde applet'in ağ bağlantılarına (indirildiği makine haricindeki) erişiminin engellenmesi de mümkündür. Bu şekilde mobil cihaza indirilerek çalıştırılan kodların cihazın izin verilmeyen bölümlerine erişmesi engellenerek cihazın illegal kullanımlarının önüne geçilmiş olur (Mahmoud, 2002).



Şekil 3.20. Sandbox Güvenlik Modeli

Sandbox güvenlik modelinin bir parçası olarak SecurityManager sınıfının örnek kullanımı aşağıdaki kod parçasında gösterilmiştir:

```
public boolean Operation(Type arg) {
  SecurityManager sm = System.setSecurityManager();
  if (sm != null) {
    sm.checkOperation(arg);
  }                }
```

Bu kod sınıfın applet'in çalışması sırasında bir dizi kontrolü (okumayı kontrol-checkRead, silmeyi kontrol-checkDelete) yapmasını sağlar.

Java'nın sonraki sürümleri (JDK1.1 ve yukarısı) imzalanmış applet'ler (signed applet) ve koruma kümesi (protection domain) kavramlarını getirmiştir. Protection domain kavramıyla uygulama geliştirici kodun sahip olacağı izinleri detaylı şekilde belirlemeye müsaade eder.

Kablosuz J2ME güvenliğinin CLDC/MIDP cihazlarına uygun olmamasından dolayı, bu cihazlar için bazı uyarlamalar yapılmıştır. Bu manada iki noktaya dikkat edilmiştir.

i) Düşük seviyeli KVM güvenliği
ii) Uygulama seviyesi güvenliği

KVM seviyesindeki güvenlik katmanı cihaza indirilen ve KVM (K sanal makinesi) tarafından çalıştırılan uygulamanın cihaza zarar vermesinin engellemesi beklenir. Bunun için de Java dosya sağlayıcı ile, Java sınıflarının geçersiz hafıza bölgelerine erişiminin engellenmesi sağlanır (Mahmoud, 2002).

Sınıf sağlayıcı geçersiz sınıf dosyalarının red edilmesini sağlar. Ancak bu işlem küçük çaplı cihazlar için zaman alıcı olduğundan ön sağlama işlemi sunucuda veya masaüstünde aptırılır. Geri kalan basit bir iki kontrol ise KVM tarafından yapılır. KVM önsağlaması yapılmamış sınıfları veya geçersiz sınıfları red eder. Bu iki aşamalı sağlama aşağıdaki şekilde gösterilmiştir.

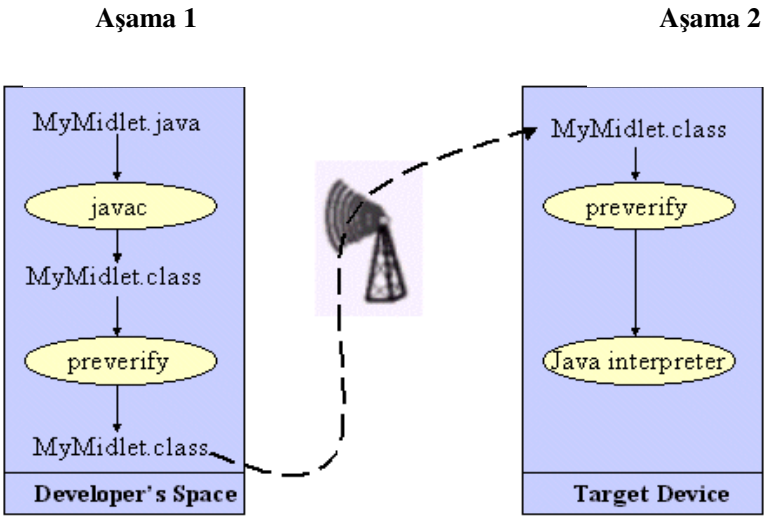
Uygulama katmanındaki güvenlik ise Java sınıfının geçerli bir sınıf olmadığının belirlenmesi esasına dayanır. Klasik masaüstü uygulamalarındaki sandbox uygulaması detaylı bir kontrol (harici dosyalara erişim kısıtlaması, kızılötesi-bluetooth cihazlarına erişimin sınırlanması, ağa erişimin kısıtlanması vs.) imkanı sağlasa da bu MIDP cihazları için ağır bir işlemdir. Bunun için sanbox uygulama ortamı CLDC/MIDP cihaları için yeniden uyarlanmıştır (Mahmoud, 2002).

KVM klasik Java sandbox modelinden farklı bir sandbox uygulaması sunar. SecurityManager veya güvenlik tedbirlerinden farklı olarak CLDC spesifikasyonuna göre bu güvenlik modeli şunları destekler:

Java dosyaları uygun şekilde sağlanarak bu dosyaların geçerli Java dosyaları olduğunun belirlenmesi.

Uygulama geliştiricilere sadece önceden tanımlanmış bir grup API'nin sunulması.

Uygulama geliştiriciler CLDC ve MIDP spesifikasyonlarında belirlenmiş fonksiyonelliğe sahip yeni kütüphaneler indirip kullanmasının engellenmesi.



Şekil 3.21. CLDC/MIDP Sağlama İşlemi

CLDC tarafından tanımlanan sandbox uygulaması SecurityManager sınıfının avantajlarına sahip değildir. Burada güvenlik sorunu oluşturabilecek Java diline ait özellikler baştan elimine edilmişlerdir. Elimine edilmiş özellikler, kullanıcı tanımlı sınıf yükleyicilere izin verilmemesi, reflection özelliğinin engellenmesi, zayıf referanslara ve java doğal arayüzüne izin verilmemesi şeklinde sayılabilir.

CLDC ve MIDP uygulamaları Java uygulamalarının KVM'ye indirilmesini gerekrirebilirler. Buradaki indirilen sınıfların sistem sınıflarını aşması (override) şeklinde bir güvenlik açığı ortaya çıkabilir. Bu güvenlik sorunu java.* ve javax.microedition.* gibi korunmuş sistem paketlerinde olmayan sınıfların önceden araştırılması ve sınıf dosya düzenine uyduğunun belirlenmesi mantığı ile çözülür. Sistem aynı zamanda uygulama geliştiricinin de sınıf düzenini aşmamasına-bozmamasına dikkat eder.

Buraya kadar Java'nın güvenlik yaklaşımı incelendi. Ancak java'nın kendisinin kablosuz güvenlikle ilgilenmediği görülür. Ancak eticaret uygulamalarının gelişmesi gizli verinin (kredi kartı bilgisi gibi) bir şekilde mobil cihazlar üzerinden transferi gibi kavramları ortaya çıkarmıştır. Burada ister istemez kablosuz ortamda hareket eden bu bilginin bir aracı tarafından yakalanıp kullanılması riski ortaya çıkmaktadır. Bunun için önerilen bir çözüm gönderilen verinin gönderilmeden önce şifrelenmesidir. Alıcı kendisine gönderilen bilgiyi (anahtarı bilmesi şartıyla) çözümler.

3.2. METOD

Asp/php gibi yorumlamalı diller aracılığıyla C++ veya Java ile yazılmış uygulamaya görüntü/sesin iletilerek işlenmesi sağlanarak sonuçların cep telefonuna iletilmesini sağlanacaktır.

Java/C++ ile yazılacak uygulama 'exe' veya 'dll' olarak server üzerine konulacaktır. Cep telefonundan gönderilen ses/görüntü bilgilerinin php/asp dili yardımıyla uygulama programına iletilmesi sağlanacaktır. Uygulama programından gelen bilgiler cep telefonuna yine php/asp dili sayesinde sağlanacaktır.

3.2.1. Mobil Cihazlar Üzerinden Bir Ses Tanıma Sistemi Oluşturma

Günümüzde bir kullanıcı yardım masası, genel olarak ya operatörlerin veya yardımcı robotların desteği ile çalışmaktadır. Bir bankacılık işlemine erişim, bir bilgiye erişim gibi nedenlerle kullanıcı ya bir mobil cihaz üzerinden veya bir telefon üzerinden belli bir numarayı çevirerek arzu ettiği işlemi gerçekleştirmeye çalışır.

Uygulamaların güvenliği ise tuş takımından kodlanan numaralar/şifreler/özel bilgiler veya kullanıcıya sorulan bir soruya (anne kızlık soyadı, doğum yeri vb.) kullanıcının cevabının, kullanıcının daha önce vermiş olduğu kayıtlı bilgiye uygun olup olmadığının belirlenmesi esasıyla sağlanır.

Bu tür bir işlem ister istemez zaman alıcı ve aynı zamanda yoğunluğa bağlı olarak müşteri üzerinde (beklemekten ötürü) negatif etkiler, konuşma ücretinin yüksek maliyetleri gibi olumsuz durumların ortaya çıkmasına neden olur.

Yapılan araştırmalarda yardım masalarının en çok arandığı konular arasında bilgisayar kullanıcılarının şifre değişikliği veya kayıp şifrenin öğrenilmesi gibi "kişisel" nedenlerdir. Yardım masalarının bunlara ek olarak telefon bankacılığı gibi işlevleri kullanan banka türü organizasyonlarda müşterilerin işlemlerine cevap vermek gibi faaliyetleri de vardır.

Bu pahalı ve zaman alıcı işlemlerin yerine kullanıcıların seslerini tanıyarak onların kimliklerini otomatik olarak daha önce kayıt edilmiş oldukları veritabanından bulmaları mümkündür.

Bir insanın sesi, seste gizli olan ve parmak izi gibi kişiden kişiye değişen ses-izlerini (voiceprint) tanıyarak doğrulanabilir. Bir kullanıcıya ait ses doğrulama sistemi, uygulamayı kullanan ne söylerse söylesin tanımlama-doğrulama yapabilmek zorundadır. Çünkü ses doğrulama her seferinde aynı kelimeyi-cümleciği söyleyerek yapmak üzerine kurulduğunda, kötü niyetli bir kişi yasal olmayanbir ses kaydı ile de güvenliği aşabilir. Bunun önüne geçebilmek için bu tür sistemler kullanıcıdan kendisine verilen bir grup rastgele sayıyı tekrar etmesini isterler. Ses tanıma bu her seferinde farklı sayıyı-kelimeyi söyletme durumunda seste gizli olan ses-izlerini belirleyerek çalışır.

Ses tanımayı gerçekleştirecek uygulama katmanı (buna analizör diyelim) aşağıdaki noktalarda verimli çalışma aralığına sahip olmalıdır:

- Gürültülü ortamlarda çalışabilme toleransı
- Sesin zamana bağlı değişimlerine karşı tanımayı gerçekleştirme
- Ses taklidi veya kayıt edilmiş sesle güvenliğin aşılmasına engel olma
- Hastalık durumunda kullanıcının sesindeki değişmelere rağmen tanıma yapabilme

Bu tür parametrelere karşı duyarlı olmayan bir sistem ile yapılması muhtemel güvenlik doğrulamaları bir şekilde aşılma, kırılma riskiyle karşı karşıya kalır (SentryCom, 2006).

Geleneksel ses tanınma ya da analiz teknikleri sinir ağları veya Markov modelleri gibi teknolojiler yardımıyla yapılmaktadır. Ancak burada sadece bu tarz bir teknikle başarılacak bir uygulama yukarıdaki sorunların tamamına bir çözüm getiremeyebilir. Bu nedenle ses analizörünün sonuçlarını yorumlayacak ve karar verebilecek bir yapay zekâ yazılımına veya uzman sisteme ihtiyaç duyulur. Syscom firması benzeri bir uygulamayı gerçeklerken analizörün sonuçlarını yorumlayarak karar veren bir algoritmayı uygulamaya eklemiştir.

Kullanıcının sesini tanıyarak bu tanıma işlemini güvenliği sağlamak anlamında kullanacak bir sistem telefon bankacılığı ve benzeri ticari sistemlere adapte edilebilecek bir teknoloji imkânı sağlar.

Bankacılık işlemlerini telefon üzerinden yapmak isteyen kullanıcılar karşılarındaki robotun kendilerine sorduğu sorulara doğru cevaplar (müşteri numarası, ATM şifresi, doğum tarihi vb.) vermeleri halinde sisteme giriş yaparak sistemi kullanabilmektedirler.

Kullanıcı açısından uzun süren bir telefon görüşmesi, akılda tutulması gereken bir çok şifre-kod, banka açısından ise uzun süren işlemlerden dolayı kullanıcı yığılması, servisin güçleşmesi, bazen canlı operatöre ihtiyaç duyulması gibi (doğrulama bazı durumlarda insanlar tarafından yapılmak zorundadırlar) sorunları beraberinde getirmektedir. Mobil cihazlarla konuşmanın normal telefon ücretlerine göre pahalı sayıldığı Türkiye gibi ülkelerde mobil bir hizmet almanın maliyeti yükselmekte ve bu tarz hizmetleri şube dışından vermek isteyen ticari müesselerin iş yükünü arttırmaktadır.

Burada ses tanıma işlemi ile hem güvenliği arttırmak hem de bahsi geçen hizmet süresini kısaltarak kullanıcıları mobil işlemle yapmaya teşvik etmek mümkündür.

Ses tanıma eksenli bu tür bir uygulamanın gerçekleştirilmesi için şu temel aşamalara aşamalara ihtiyaç vardır:

i)Kullanıcıların ses örneklerinin kayıt edileceği bir veritabanı.

ii)Kullanıcıların seslerini (gerek örnekleme yaparken gerekse güvenlik uygulamasına geçildiğindeki sesi tanımak için) analiz edecek analizörün tasarımı.

iii)Güvenlik sistemi için sadece analizörün yeteneğine güvenilmiyorsa bir yapay zeka arayüzünün karar verici mekanizma olarak eklenmesi.

iv)Kullanıcı ses örneklerinin uzaktan alınacağı bir web sitesi.

v)Cep telefonunda arzu edilen güvenlik tarzına uygun olarak senkron (kullanıcı hizmeti kullanmaya başlarken sesinin tanınması) veya asenkron (kullanıcının sesinin cep telefonundaki program yardımıyla kayıt edilip veritabanına gönderilmesi) seçime göre bir java programının yazılması.

Asenkron uygulama seçildiğinde cep telefonunda sunucu ile bağlantıya geçerek sunucuya ses örneğini aktaran ve sonra sunucundan aldığı cevabı kullanıcıya ileten bir yazılımın kullanılması gerekir. Ancak asenkron sistem, yani kullanıcının ses örneğinin kullanıcının mobil cihazı ile alınarak sunucuya gönderilmesi ve daha sonra kulanıcıya tekrar cevap döndürülmesi kendi içinde sorunlar taşımaktadır. En önemli sorunlar, sistemin kablosuz ağ üzerinde yavaşlama riski, sesin illegal olmayan bir şekilde kayıt edilerek sunucunun (ses tanıma sisteminin) aldatılmaya çalışılmasıdır. Bunun yerine senkron doğrulama seçilmesi durumunda cep telefonunun mobil olmak dışında çok fazla bir önemi kalmıyor gibi görünse de önemli olanın güvenliği sağlamak olduğu gözden kaçırılmamalıdır.

4. BULGULAR VE TARTIŞMA

Bu çalışmada gezgin cihazlar olarak bilinen cep telefonu veya PDA türü cihazları üzerinden bir sunucu tabanlı kimlik doğrulama geliştirme yöntemleri incelenmiş, ses ile tanıma teknolojisinin bankacılık ve benzeri alanlarda kullanımı ile ilgili bir örnek prototip sunulmuştur.

Bu tarz kuruluşlarda klasik yöntemlerle güvenliğin sağlanması kullanıcının bildiği özel bir şifre veya özel bitr bilginin üzerinden gerçekleştirilir. Ancak şifre çözücü programların, illegal izleyici yazılımların ve benzeri tekniklerin kullanımı ile bu şifrelerin ele geçirilmesi mümkündür. Kullanıcıların bu riski en aza indirmek için şifrelerini sık sıkı değiştirmeleri ve her seferinde -kendi çıkarları açısından- bunu güvenli şekilde korumaları beklenmektedir.

Müşteri açısından bakıldığında sürekli değişen şifrelerin önceki şifrelerle karıştırılması veya unutmamak için bir yerlere yazılması gibi güvenliği tehdit eden veya müşteri hizmetleriyle uzun diyaloglar gerektiren sorunlu alanlar ortaya çıkar.

Tüm bu sorunları aşabilmek için yaygın şekilde kullanılan ve çoğu çokluortam yetenekleri ile donatılmış cep telefonları üzerinden daha sağlıklı bir doğrulama seçeneği olarak aşağıdaki tekniklerden birisi veya bir kaçı aynı anda kullanılabilir:

İris tanıma: İnsan gözünün bileşenlerinden birisi olan iris çok bilinen parmak izi yapısı gibi bir insandan diğerine farklılık göstererek doğrulama-güvenlik amacıyla kullanılabilecek bitr seçenektir. Cep telefonları üzerindeki kamera yardımıyla kişinin tanınması şu an yaygın bitr teknoloji olarak görülmese de, birkaç yıl içinde ciddi bir kullanım alanı bulacağı düşünülmektedir.

Parmak izi tanıma: En çok bilinen ve beklide doğrulama amaçlı olarak en sık kullanılan biometrik veri, parmak izidir. Mobil cihazlar üzerine küçük tarayıcıların yerleştirilmesi ile birlikte sunucu tabanlı bir güvenlik sistemi olarak bu veriden faydalanılacağı gibi, mobil cihazların kredi kartı ve benzeri saklayacağı birer elektronik cüzdan uygulamasında kullanılabilecektir. Parmak izi tarayıcısından elde edilen örnek veri boyut olarak küçük bir yer kapladığı için aynı zamanda ses-görüntü sistemleri için ön doğrulama şartı olarak kullanılabilecektir.

Yüz tanıma: Bu tanıma işlemi diğer bahsi geçen metotlara göre hem örnekleme veri boyutu büyük hemde uygulanabilirlik anlamında karmaşık olduğundan tercih edilmesi için mobil cihazların şimdiki hızlarının çok üstüne çıkması, sunucu tabanlı bir doğrulama için ise yine mobil cihazların kullanacağı internet bağlantısının hızının daha çok iyileştirilmesi gerekmektedir.

Ses tanıma: Çalışmamızda model olarak kullanmayı düşümndüğümüz bu tekniğin en önemli sorunu ses örneklemesinin mobil cihaza yaptırılmaya çalışılmasında ortaya çıkar. Ortalama bir ses örneği (birkaç rakamın ya da kelimenin söyletilerek elde edilmesi durumunda) 70-80 kB'lık bir veri anlamına gelecek ve bu da ister istemez şimdiki bağlantı hızlarında eşzamanlı ses tanımaya izin vermeyecektir.

4.1. Ses Tanıma Uygulamaları

Cisco, IBM ve SUN firmaları özellikle yardım masalarının yerini alacak ses (konuşmayı) anlama ve tanıma sistemleri üzerine ciddi çalışmalar yapmış olup bunlar hali hazırda ticari işletmelerin kulanımına sunulmuştur.

Ses tanıma sesin niteliğinden çok içeriği ve kullanılan dile bağlı bir sistemdir. Örneğin, bir seyahat acentasından bilet alma veya rezervasyon işlemi için sesin içeriğinin anlaşılması gerekmektedir. Burada sesin kime ait olduğundan çok içeriği yani taşıdığı anlam önemlidir.

Sesin, kişiden kişiye değişen ses-izlerinin tanınmasıyla kimlik doğrulamada kullanılması yeni bir uygulama olup mobil cihazların çoklu ortam özellikleri ve internet yeteneklerinin gelişmesi ile günlük hayatta pratik uygulamalar için ciddi çalışmalara başlanmıştır.

4.2. Önerilen Uygulama

Burada önerilecek sistemde herhangi bir banka için kullanıcının telefon bankacılığı işlemlerini yaparken ses ile kimliğinin doğrulanmasının sağlanması ve bir defa bu işlem yapıldıktan sonra kullanıcıya istediği işlemleri cep telefonu aracılığı ile yapmasının sağlanması amaçlanmıştır. Bunun dışında önerilecek olan sistem yardım masası uygulamalarında çalışmak zorunda olan operatörlerin sayısının veya iş yükünün azaltılması anlamında her hangi bir online çalışmada veya uygun modifikasyonlar ile e-ticaret uygulamalarında kullanılma imkanına sahiptir.

Ses tanıma işleminin cep telefonu üzerinde gerçeklenebilmesi uygulamanın gerektireceği sistem kaynağı açısından bakıldığında şu an için imkânsızdır. Bu nedenle bu tür bir sistemin sunucu tarafı uygulama olarak kurulması ve sunucunun taşıyacağı yükün kullanıcı sayısı ile orantılı olarak artabileceği dikkate alınmalıdır. Bu nedenle sistemin kalbini oluşturan güçlü bir sunucu kurulmalıdır.

Sunucu tarafı uygulamanın gerçeklenmesi birbirine bağlı olarak çalışan üç ayrı yazılımın birbirine entegrasyonunu gerektirmektedir. Bu nedenle seçilecek teknolojilerin birbirine uygunlukları dikkate alınmalıdır. Bu tarz sistemler için IBM firmasının pazarladığı websphere sunucu teknolojileri veya SUN firmasına ait Java teknolojileri temel olarak seçilebilir.

Bu çalışmada java tabanlı bir prototip önerilmektedir. Bu nedenle SUN firmasının J2EE (Enterprise Sürümü) yazılımı sunucu tarafı çalışmanın üzerine kurulacağı sistem olarak seçilecektir. J2EE mimarisi uçtan uca güvenlik yaklaşımıyla arzu edilen sistemin güvenlik politikaları için yeterli bir altyapı sağlar. Bunun dışında J2EE mimarisi güvenlik anlamında önemli bir genişleme imkânı olarak JAAS (Java Authentication and Authorization Services-Java Doğrulama ve Yetkilendirme Servisleri) ortamını destekler.

JAAS, kimlik doğrulama ve yetkilendirme servisleri için bir dizi API ile birlikte gelir. Yazılım bunun yanında farklı güvenlik mekanizmaları sunan üçüncü parti uygulama geliştiricilerin üretmiş oldukları farklı doğrulama mekanizmalarının (akıllı kartlar, insan

biyometrisi) eklemlenebilmesi imkânını tanır. JAAS yazılımı bu şekilde J2EE yani java tabanlı uygulamalar için tümleşik bir güvenlik modeli sağlar.

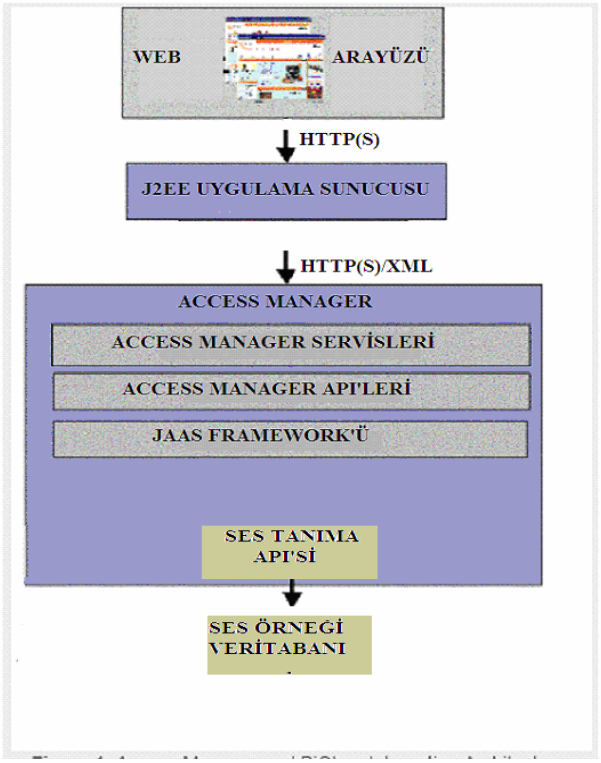
JAAS çalışma çatısı (framework) güvenlik uygulamaları için temel alt yapıyı sağlar. Ancak JAAS çatısını yönetmek için bu yapı üzerine kurulu Java System Access Manager yazılımının kurulması gerekir (Anonim, 2007b).

Sunucu tarafına ses tanıyıcı yazılım olarak hazır bir bioAPI, yapay sinir ağlarına dayanarak yapılmış bir uygulama veya üçüncü parti bir firmanın bu amaçla ürettiği Java tabanlı bir API kullanılabilir. Sistemimiz Java tabanlı uygulamalara kolay şekilde destek verebildiği için Java tabanlı bir analizör uygun bir seçim olacaktır.

Ses ile güvenlik uygulamasında analizörün kullanıcının sesine göre eğitilmesi, ya da kullanıcının sesini tanıması süreci web üzerinden gerçekleştirilmelidir. Kullanıcıya ait ayırt edici ses verisinin kayıt edilmesi için veritabanı uygulamasına ihtiyaç duyulacaktır.

Sistem java tabanlı uygulamalar etrafında şekillendiği için ses ve benzeri örnekleri tutacak veritabanı olarak JDBC veri tabanı sürücüsünü destekleyen bir yazılım seçilebilir. MySQL, Microsoft SQL Server ve Oracle gibi veritabanı yazılımları JDBC sürücülerini desteklediklerini için, uygun yazılım bunlar arsından seçilebilecektir. Test aşamasında ücretsiz olan SQL Server veya MySQL yazılımlarından birisinin kullanılması maliyeti oldukça düşürecektir.

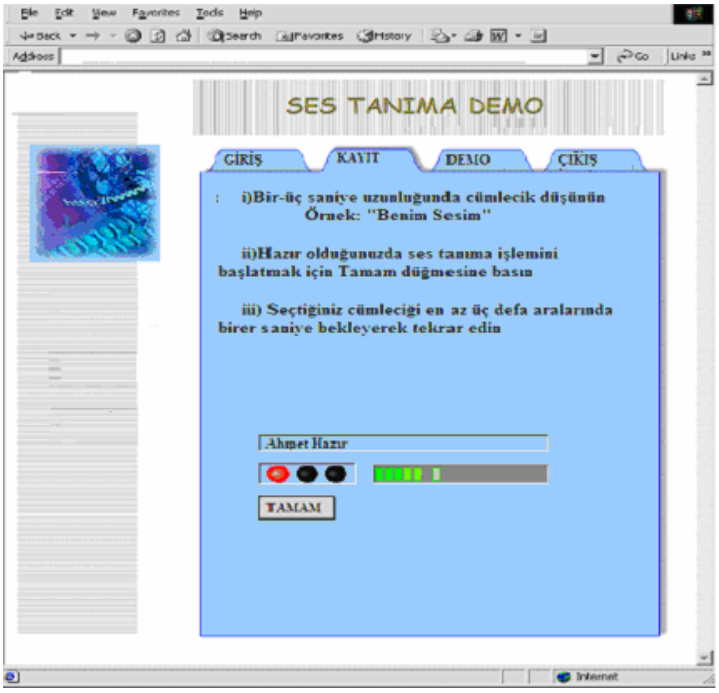
Sunucu tarafı yazılımları yüklendiğinde aşağıdaki şekildekine benzer bir mimariyi gösterir.



Şekil 3.22. Sunucu Tarafı Yazılımların Blok Diagramı

Sunucu yazılımlarını internet ortamına bağlayacak ve kullanıcının ses örneklemesini yapacak olan sistem bir JSP tabanlı tasarımla gerçekleştirilecektir.

Kullanıcının ses örnekleme sistemini eğitmesi (kendi sesini örnekleyerek sonraki girişlerine referans olacak ses kaydı) işlemini yapmak için web üzerinden bir defaya mahsus olmak üzere kayıt yapılması gerekir. Bu işlemin mobil telefonla yapılması güvenlik açısından sorun doğuracağı için kullanıcı kendisine ticari firma tarafından verilen bir şifre ile tasarlanan web sitesine bağlanır. Buraya güvenli bir giriş yaptıktan sonra kendisinden istenen kısa birkaç kelimeyi aralıklarla kayıt eder. Bir servlet kullanıcıya adım adım yapması gerekenler konusunda yardımcı olur. Bunun için aşağıdakine benzer bir tasarım önerilmektedir.



Şekil 3.23. Ses Tanıma Web Arayüzü

Ana hatlarıyla oluşan sistemin bir telefon bankacılığında veya benzeri bir ticari ortamda çalışma tarzının şu olması önerilir:

i)Kullanıcıya firmanın vermiş olduğu şifre ve kullanıcı adıyla (müşteri numarası gibi bir benzersiz numara da olabilir) kullanıcı ya önerdiğimiz tasarıma benzer şekilde bağımsız bir web sayfası üzerinden veya firmanın kendi sitesi üzerindeki bir bölüm aracılığı ile ses tanıma sayfasına güvenli bir giriş yapar.

ii)Kullanıcı ses tanıma sayfasında ses örneğinin alınması için yönlendirilir. Burada kullanıcıdan seçmiş olduğu bir iki kelimelik bir cümleciği üç kez aralıklarla tekrar etmesi

istenir. Tüm bu işlemler bir servlet aracılığı ile sunucuya çalışma zamanında aktarılır. Ses kaydı kullanıcının cihazına bağlı mikrofonla yapılır. Eğer kullanıcının mobil cihazı destekliyorsa bu işlem direkt olarak kullanıcının cep telefonu, PDA'sı veya benzeri cihazıyla da yapılabilir.

iii)Ses örneği ses API'si tarafından analiz edilerek ses-izleri, sese ait karasteristikler orijinal ses kaydı ile birlikte ses tanıma veritabanına (müşteri numarası birincil anahtar seçilecek şekilde beraberce) kayıt edilir. Ortalama ses kaydı her müşteri için birkaç yüz kilobayt'lık bir alan kaplayacaktır. Ses örneğinin alınması ile birlikte müşteri ticari firmanın ses tanıma sistemine kayıtlı olacaktır. Tasarlanan web sitesi istenirse müşteriye ses kaydını yenilemek seçeneğini de sunabilir. Ancak bunun pratikte çok faydası olduğu düşünülmemektedir.

iv)Bu aşamada müşterinin sistemi kullanması mümkündür. Müşteri ilgili firmanın telefon servisini hizmet talebinde bulunmak için arar. Ancak müşteriye sistemi kullandırırken iki yaklaşım söz konusu olabilir:

Müşteri sisteme girer girmez kendisine sistemin önerdiği rastgele üç sayıyı aralıklarla tekrar etmesi istenir. Bu sırada müşterinin ses kaydı ilgili sunucuya yönlendirilir. Yapılan analiz sonucunda elde edilen ses örneği, veritabanında kayıtlı örneklerle kıyaslanarak müşterinin kimliği (eğer ses kaydı yapmış bir kişi ise) bulunur. Ancak bu hizmet verme süresini uzatmaya ve veritabanı yükünün artmasıyla yavaşlamaya neden olur.

Bunun yerine müşterinin sürekli kullandığı müşteri numarasını tuş takımıyla girmesi istenir. Bundan sonra müşteriye ses analizi yapılabilmesi için sistemin belirlediği rastgele üç sayıyı söylemesi istenir. Müşteri bu sayıları söyledikten sonra sesin analizi yapılarak elde edilen ses analiz sonucunun müşteri numarasıyla kayıt edilmiş ses numunesi ile uygunluğu sorgulanır. Uygun durumda müşterinin güvenlik testini geçtiği varsayılarak kişisel işlemlerini yapmasına izin verilir.

Burada müşteri numarasının başkası tarafından bilinmesinin hiçbir sakıncası olmadığı çünkü asıl güvenliğin müşterinin ses izleri, ses örneği ile ilgili olduğuna dikkat edilmelidir.

Bu çalışmanın benzeri uygulamalar için yazılım ve geliştirme ortamı olarak IBM'in websphere sunucusu üzerine, voice portal uygulamasının kurulması ve arayüz olarak JSP sayfalarına gömülü voiceXML imleri kullanılması mümkündür. IBM ve SUN firmaları ses anlama (sesin anlamlarının anlaşılması, ses metin, metin ses dönüştürücüler) şeklinde uygulamalar geliştirnek için hazır uygulama ortamları geliştirmişlerdir. Bu tür bir teknolojinin ses doğrulama tekniği ile birlikte kullanılmasıyla biraz daha farklı uygulamalar geliştirmek mümkündür.

5. SONUÇ VE ÖNERİLER

Mobil cihazların gelişen yetenekleri ve artan kapasiteleri, özellikle cep telefonlarının akıllı telefon adı verilen jenerasyonla kazanmış olduğu özellikler bu cihazların çok farklı alanlarda kullanılması için imkânlar tanımaktadır.

Mobil cihazların ses, görüntü gibi gittikçe gelişen çokluortam tabanlı özelliklerinin yanında dokunmaya duyarlı ekranlar, olası tarayıcı eklentileri gibi gelişimlerle çok daha yaygın kullanım alanları bulacağı kesindir.

Özelde cep telefonları olmak üzere mobil cihazlar gündelik hayatın ayrılmaz bir parçası olurlarken eticaret ve benzeri ticari uygulamaların bu kullanımı artan cihazların ekseninde gelişmesi kaçınılmazdır.

İnternet'in kablosuz ortama taşınması mobil cihazlar üzerinden internete girişi mümkün kılarken, mobil cihaz kullanıcıları normal internet bağlantısı ile yaptıkları hemen her şeyi bu cihazlar üzerinde yapmak eğilimindedirler. Mobil cihaz donanımlarındaki ve kablosuz bağlantı hızlarındaki gelişim ile artık bu istekler makul kabul edilmeye başlanmıştır.

Kablosuz bağlantı üzerinden yapılacak alış veriş, bankacılık işlemleri, online ticari işlemler, e-devlet uygulamaları kimlik tespitinin önemini daha çok ortaya çıkarmıştır.

Kimlik doğrulama ihtiyaçlarının artması kullanıcıların çok sayıda web uygulaması için farklı birçok şifre ve kullanıcı adını kullanması-hafızasında tutması gibi sorunlu bir alana işaret eder. Bu nedenle konvansiyonel güvenlik tedbirleri yerine biometri teknikleri veya SIM kartların ek özelliklerle akıllı bir kart gibi davranmasının sağlanması şeklinde arayışlar ortaya çıkmıştır.

Kişininin makine başında bulunarak (bir binaya, askeri bir tesise vs) girmesi sırasında insan sesi, yüz görüntüsü, parmak izi, iris taraması, retina taraması ve benzeri biometrik veriler bu güvenlik ihtiyaçlarına uzun zamandan beri cevap vermekte idiler. Bu klasik lokal çözümlerin mobil cihazlara taşınması, mobil cihazların sınırlı yeteneklerinden dolayı yakın bir zaman dek mümkün olmamıştı.

Güvenliği sağlayacak düzeydeki biometrik örneklerin boyutu ses, yüz görüntüsü haricindeki tanımlama biçimleri için birkaç yüz byte ile birkaç kilobeyte arasında değişiklik gösterir. Bu nedenle ses uygulaması pratikte parmak izi, iris, retina tarama gibi özelliklere göre uygulanması iletişim hızına (mobil cihaz anlamında) doğrudan bağlı olan bir seçenektir. Ancak günümüz teknolojilerinin mobil cihazlar üzerinden de 70-80 kilobayt'lık ses örneklerinin senkron olarak web ortamında taşınmasına imkan vereceği düşünülmektedir.

Yukarıda genel hatlarıyla izah edilen ses tanıma sisteminin cep telefonlarına küçük parmak izi okuyucular-tarayıcılar eklenmesiyle geliştirilmesi mümkündür. Çünkü cep telefonlarına parmak izi tarayıcılar ekleme teknolojisi seri üretime geçebilecek kadar pratikleşmiştir. Bu durumda ses örneğinin alınacağı siteye girişin mobil cihaz üzerinden olması ve bu örneklemenin başlatılması için kullanıcının parmağı ile tarayıcıya

dokunmasının istenmesi mümkündür. Böylece müşteri numarası ve benzeri hiçbir bilgiye gerek kalmadan (ya da en azından bu bilgiyi sadece veritabanı sorgulama işleminde hızı arttırmak için kullanarak) güvenlik sorgulaması yapılabilir.

Mobil cihaz teknolojileri kullanıcılara ait hemen hemen tüm gizli bilgileri saklama sürecine doğru değişirlerken ister istemez yasal olmayan şekilde bu bilgileri kullanmak isteyenlerinde aynı teknolojilerden faydalanarak karşı teknikler üretmesi riski vardır. Bunun önüne geçmek için de gerek biometrik doğrulama tekniklerinin gerekse SIM kart tabanlı akıllı kart uygulamalarının tersinmez algoritmalarla (SHA, MD5 vs) birleştirilerek güvenliğin derecesi arttırılmak zorundadır.

Tersinmez algoritmalar açık kaynak koduna sahip oldukları halde çalıştırıldıklarında neyi nasıl yaptıkları bilindiği halde, adım adım geri dönerek ilk adıma ulaşılması imkânsız algoritmalardır. Bunlardan SHA (Secure Hash Algorithm) algoritmasının geleneksel ataklar ile kırılma ihtimali 2^{160} ihtimalde birdir. Bu ise bu günkü teknoloji ile varolan tüm bilgisayarların birbirine paralel olarak çalışsalar bile yıllarca çözemeyeceği bir ihtimaldir.

SIM kart teknikleri ve biometrik tekniklerin beraber kullanımı ile birlikte mobil cihazların kişilerin kimlik kartlarının, kredi kartlarının ve benzeri tüm bilgilerinin saklı olduğu komple cihazlar haline gelmesi çok uzak bir gelecek değildir. Böylece kullanıcıların çok sayıda şifreler yerine kişisel ve benzersiz biometrik verileri ile tanımlandığı ortak bir veritabanı ihtimali güçlenmektedir. Bunun Türkiye ölçeğinde TC Kimlik Numarası olarak bilinen sistemin yan uzantısı olarak merkezi bir vatandaşlık bilgisi veritabanı ile bütünleştirilerek güvenlik protokolleri ile ticari kullanıma açılması dahi beklenebilecek gelişmelerdendir.

KAYNAKLAR

ANONİM, 2001a. GPRS nedir? Nasıl avantajlar sunacak? , Özel Dosyalar, Ericsson Mobility World WEB Sayfası, http://www1.ericsson.com.tr/mobilityworld/articles/essentials/102803-27082001.htm.

ANONİM, 2001b. Gprs and Edge to 3G, http://www.3g-generation.com/gprs_and_edge.htm.

ANONİM, 2001c. 3G'ye Uzanan Yollar, Özel Dosyalar, Ericsson Mobility World WEB Sayfası, http://www1.ericsson.com.tr/mobilityworld/articles/essentials/102205-27082001.htm

ANONİM, 2001d. GPRS: 3G Yolunda Önemli Bir Adım, Temeller, Ericsson Mobility World WEB Sayfası, http://www1.ericsson.com.tr/mobilityworld/articles/essentials/104401-30082001.htm

ANONİM, 2003a. Biometrics, http://www.ergosis.com.tr/biometrics_tr.html

ANONİM, 2004a. Symbian Media center Picture Library Web sayfası, www.symbian.com/press-office/picture-library_phones.html

ANONİM, 2006a. Java Documents, SUN Microsystems, www.sun.com veya www.java.com

ANONİM, 2006b. Iris Recognition Through Mobile Devices, www.okielectric.com

ANONİM, 2007a. Camera MIDlet Application, Nokia 2003, www.forum.nokia.com

ANONİM, 2007b. JAAS FrameWork, SUN Microsystems, www.sun.com

AKSU, M. 2005 3. Nesil Cep Telefonları İçin Symbian İşletim Sistemi Üzerinde Çalışabilen C++ Tabanlı Uygulama Geliştirilmesi, K.S.Ü. Fen Bilimleri Enstitüsü, s1-5

ANDERSSON, C. 2001. GPRS and 3G Wireless Aplications. Wiley Computer Publishing, New York, United States of America, s317.

ARSLAN, S. 2000. GSM 900 baz istasyon servis sayılarının simülasyon (benzetim) ve amaç programlama tekniklerinin kullanılması. Gazi Üniversitesi Yüksek Lisans Tezi, Ankara.

ANOVEA, A. T., 2003, Voice Recognition SDK, Anovea Authentication Technology, www.anovea.com

BUCKINGHAM, S. 1999. Data on GPRS, Mobile Lifestreams Limited. s22

CANDAN, M. M. 2002. Üçüncü Nesil Mobil Haberleşme sistemleri için Türkiye'de Uygulanacak frekans bandı, Lisans, servisler, Uygulamalar ve Ülkemizdeki Durumu. Uzmanlık Tezi, Ankara, s127.

FINAN, T. 2002. Developing Applications fort he Microsoft Smartphone. http://msdn.microsoft.con/library/default.asp?url/library/en-us/dnsmtphn/html/ devappsp.asp

GEORGIADIS, P., 2004 A Smartphone-Based Teleradiology System

GHRIBI, B., LOGRIPPO, L. 2000. Understanding GPRS: The GSM packet radio service, Computer Networks, cilt 34, s763-779.

HELIN, J. 2002. The Future of Comms Devices and Customer Interfaces, www.medialab.sonera.fi, IIR's 5.European ISP Forum, Amsterdam, Netherlands. 23s

JANSEN, W. 2004. Authenticating Mobile Device Users Through Image Selection, Commerce and Security, K.Morgan, v.30, s10.

KASAVANA, M. L., 2006. Authentication of Fingerprints Through A Mobile, http://www.amonline.com/publication/bio.jsp?id=5&pubId=1

KNUDSEN, J., 2002. Authentication in MIDP, http// developers.sun.com

KNUDSEN, J., 2003. The Basics of the MMAPI for Java Developers, http//developers.sun.com

MAHMOUD, Q., 2002. Wireless Java Security, http// developers.sun.com

MAHMOUD, Q., 2003. The J2ME Mobile Media API, http// developers.sun.com

MALLICK, M. 2003. Mobile and Wireless Design Essentials. Wiley Publishing, Indianapolis, Indiana, s454.

ÖZÇELİK, M.A., 2006. Bluetooth Üzerinden Güvenli Veri İletimi, K.S.Ü. Fen Bilimleri Enstitüsü

PERRIG A. ,SONG D., 2000. Hash Visualization: a New Technique to improve Real-World Security, Computer Science Department Carnegie Mellon University s12.

SADAY, T. 2005, Bilgisayar Destekli Kimlik Tespit Sistemlerinde Biometrik Yöntemlerin Değerlendirilmesi, T.C. Selçuk Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisligi Bölümü

SELIAN, A. 2001. 3G Mobile Licensing Policy: From GSM to IMT-2000-A Comparative Analysis. ITU, http://www.itu.int/osg/spu/ni/3g/casestudies, s20-25.

SHARP, K., 2005. The Basics of the MMAPI for Java Developers, http://www.informit.com/authors/bio.asp

SUNG, L., SWEENEY, D., FOSSA, C., D'SOUZA, M. 2001. 3G Migration in North America-Final Paper, Virginia Tech, s10.

ŞEN, Ö. 2001. Mobil Sistemlerin Evrimi: 2G'den 3G'ye, EMO Elektrik Mühendisleri Odası WEB Sayfası , www.emo.org.tr/merkez/dergi/408/sen.html.

VIJAYAKUMAR, B. V. K., 2005. Face Authentication From Cell Phone Camera Images with Illumination and Temporal Variations, IEEE Transactions On Systems, Man, And Cybernetıcs—Part C: Applications And Reviews, Vol. 35, No. 3

YANIK, D. 2001. Üçüncü nesil (3G) mobil telekomünikasyon sistemleri ve 3G lisanslarının verilmesi konusunda dünyadaki uygulamalar ile Türkiye analizi, Telekomünikasyon Kurumu Web sitesi / Yayınlar / Teknolojik gelişmeler. http://www.tk.gov.tr/54.html

ZHENG, Y., 2004. Enhancing Security in GSM, University of Wollongong

ÖZGEÇMİŞ

M.Erdal DAYAK 01 Mart 1977 tarihinde GAZİANTEP'te doğdu. İlk ve orta öğrenimini GAZİANTEP'te, lise öğrenimini Gaziantep Cumhuriyet Lisesi'nde tamamladı. 1994 yılında Karadeniz Teknik Üniversitesi Bilgisayar Mühendisliği bölümünü kazanarak 1999 yılında mezun oldu. Askerliğini yedek subay olarak Ankara-Genel Kurmay'daki İstihbarat Bilgi İşlem Bölümü'nde bilgi işlem ve yazılım sorumlusu olarak yaptı.

Halen ErSoft Bilgi ve Sistem Yöneti Ltd. Şti.'de yazılım geliştirme ve pazarlama sorumlusu olarak çalışmaktadır.