Sağlık Sistemlerinde Akıllı Kart Uygulamaları

ÖZET

Sağlık alanında akıllı kart uygulamaları analiz edilmiş, standartlara uygun bir tasarım yapılmıştır. Hastanın önemli sağlık verileri akıllı kart üzerinde tutulur. Hasta ile ilgili diğer sağlık kayıtları ise internet üzerinden erişilen merkezi bir veri tabanında tutulur. Kişisel verilere güvenli erişim için bir asıllama protokolü tasarlanmıştır.

Smartcard Applications on Healthcare Systems

ABSTRACT

After the analysis of card projects in healthcare systems, a health card system was designed according to the standards. Critical health data is stored in the health card. Other health care records' history is stored on a central database which is connected to internet. An authentication protocol is designed for the protection of personal data.

ÖZGEÇMİŞ

Araş. Gör. Çiçek Çavdar

1998'de İstanbul Teknik Üniversitesi Elektrik-Elektronik Fakültesi Kontrol ve Bilgisayar Mühendisliği Bölümü'nden mezun oldu. Aynı bölümde 1998'den beri araştırma görevlisi olarak görev yapmaktadır

.

Araş. Gör. Sanem Sarıel

1999'da İstanbul Teknik Üniversitesi Elektrik-Elektronik Fakültesi Kontrol ve Bilgisayar Mühendisliği Bölümü'nden mezun oldu. Aynı bölümde araştırma görevlisi olarak görev yapmaktadır

Doç. Dr. B. Tevfik Akgün

1996'da Bilgisayar Sistem Yapısı Dalı'nda doçent oldu. Halen İstanbul Teknik Üniversitesi Elektrik-Elektronik Eğitim Fakültesi Bilgisayar Mühendisliği Bölümünde çalışmaktadır.

1. GİRİŞ

Trafik kazalarında ve doğal afetlerde yaralı kişilere ait kan gurubu, önemli hastalıkları, alerjisi olduğu ilaçlar, kullanması zorunlu ilaçlar gibi temel sağlık bilgilerinin acil tedavi sırasında hayati önemi vardır. Yaralı kişilerin kaybı durumunda ise kimlik tespiti ve organ bağışı konuları önem kazanmaktadır. Ülkemizde trafik kazalarının çokluğu ve deprem gibi doğal afetlerin varlığı kişilere ait temel sağlık verilerinin o kişilerin üzerinde taşınabilir bir ortamda saklanmasını gerektirmektedir. Bu amaçla akıllı kart kullanımı bu verilerin güvenli bir ortamda taşınması açısından en uygun çözümdür. Yaralı kişilere ait önceden elde edilen raporlar, tahlil sonuçları ve tıbbi görüntüler gibi boyutları taşınabilir olmaktan çok uzak verilerin de acil tedavi sırasında kullanılması zorunlu olabilir. Normal tedavi açısından da özellikle yer veya hastane değişikliği gibi durumlarda bazı tıbbi kayıtların uzaktan erişimi yararlı olacaktır. Ayrıca bu türden önemli kişisel verilerin saklanması ve erişilmesi konusunda kişilerin kurulacak bir sisteme güven duyması sistemin varlığını sürdürmesi açısından zorunludur.

Yazılım ve donanım olanaklarının hızlı gelişimi bu alandaki uygulamalara da yansımış, ayrıca bu konudaki deneyimler yeni yeni bir olgunluk noktasına ulaşma evresine girmiştir. Sağlık alanında akıllı kart kullanımında bugün gelinen noktadaki yönelim, standartlara uygun tasarlanmış, donanım ve platform bağımsız bir sistemin tasarlanması yönündedir. Değişik ülkelerdeki sağlık kart uygulamaları incelenerek bu konudaki en uygun yaklaşımın geliştirilmesi amaçlanmaktadır.

Acil durumda erişimi gerektiren veriler kartın içinde saklanacak, geçmiş tedaviler veya MR sonuçları gibi ek bellek gerektiren veriler ise merkezi sunucu bilgisayarda tutularak gerek duyulduğunda Internet üzerinden erişilebilmelidir. Hasta ve yetkilinin erişimleri için asıllama işlemi yapılır. Asıllama birbirinden bağımsız iki basamakta yürütülür. Birinci basamakta kart kullanıcısının kartın gerçek sahibi olup olmadığı test edilir. Burada duruma göre farklı iki parametre asıllama için kullanılır: Kullanıcı PIN kodu veya biyometrik veri. İkinci basamakta ise sunucudaki bilgilere erişecek kişinin denetimi, hangi kategoriye girdiğine ve kimliğine bağlı olarak yapılır. Bu asıllamada anahtar, akıllı karttır. Asıllama protokolünün temel ögeleri kendisini sisteme tanıtacak hasta ve sağlık görevlisidir, protokolün etkin ögeleri olarak ta, onların akıllı kartları ve sunucu yer alır. Hastaya ilişkin doğru veriye erişimi sağlayacak işaretçiler, sağlık görevlisinin imzası ile birlikte asıllama için sunucuya gönderilir.

Sunulan bildiride dünyada sağlık kartları konusundaki uygulamalarda gelinen nokta incelenerek ortaya konmuş. Buradan yola çıkılarak bir tasarım yapılmıştır. Kullanılan standartlar araştırılarak tasarımın standartlara uygunluğu gözetilmiştir.

2. AKILLI KARTLAR

Akıllı kart, içine bir mikroişlemci ve bir bellek tümdevresi veya programlanabilme özelliği olmadan yalnızca bellek tümdevresi yerleştirilmiş bir elektronik karttır. Mikroişlemcili kartlar, kart üzerinde bulunan veriler üzerinde değişiklik yapılmasına olanak tanırken bellek kartları yalnızca önceden tanımlanmış işlemleri yürütebilirler. Akıllı kartlar üzerinde bilgi saklayabilmesi ve verilerin güvenliğini sağlayabilmesi açısından manyetik kartlardan ayrılır.

2.1. AKILLI KART İLE SAYISAL SERTİFİKA

Sağlık uygulamalarında kimlik denetimi ve asıllamanın gerçekleştirilmesi için kullanılan sayısal sertifikalar, bir çeşit sayısal imza işlevini görür. Örneğin bir kişinin sayısal sertifikası ele geçirildiğinde o kişi yerine imza atmak ve o kişinin kılığına bürünerek onun yetkilerini ele geçirmek mümkün hale gelir. Sayısal sertifika ile kişisel anahtarın bir akıllı kart üzerinde birleşimi, sayısal sertifikalarla ilgili bir dizi güvenlik ve uyumluluk konusunu çözüme kavuşturmaktadır. Bir sayısal sertifika bir kişi veya bir organizasyon için bir kez yayınlandıktan sonra korunur. Böylece başkaları sertifikayı ele geçirip sertifika sahibinin yerine geçemez. Akıllı kartlar, kopyası alınması zor olduğundan sayısal sertifikaların saklanması için en uygun mekanizmalardır. Akıllı kartlarda kullanılan PIN numarası ise kişiye ait bir bilgi olup kimliğin kontrol edilmesi için ikinci bir güvenlik mekanizması oluşturur. Kişinin kartı kullanabilmek için PIN kodunu bilmesi gerekir. Akıllı kartın sağladığı diğer bir yetenek ise sayısal sertifika ile birlikte ek özel verileri güvenli bir şekilde taşınabilir hale getirmesidir.

Böylece akıllı kartların kullanımı ile desteklenen sayısal sertifika yardımıyla gerçeklenecek internet üzerinden asıllama işlemi, günümüzde intranetler için de kullanılmaktadır. Asıllama problemlerine çözüm olarak akıllı kart üzerinde ek olarak Açık Anahtar Kriptografi Standartları (PKCS) kullanılır. PKCS, RSA Laboratuarları tarafından Apple, Microsoft, DEC, Lotus, Sun ve MIT ile de işbirliği içinde açık-anahtar kriptografi için geliştirilmiş bir dizi standarttan oluşmaktadır.

PKCS, standart biçime uyan bir kriptolama algoritması geliştirmeyi olanaklı kılmak amacıyla sayısal imzaların, sayısal zarfların, ve genişletilmiş sertifikaların, algoritmalarından bağımsız olarak birlikte kullanılabilmeleri için ortak bir standart yapı tanımlar.

2.2. ISO-7816 STANDARTI

Akıllı kartların geniş alanda ve ortak uygulamalarda kullanımının yaygınlaşması için kartlarda ve kart okuyucularda bazı standartların geliştirilmesi zorunlu hale gelmiştir. Bunun için Uluslararası Standartlar Enstitüsü (ISO) kontaklı tümdevre devre kartları için ISO 7816 standartlarını geliştirmiştir[4]. Bu standart bellek kartları ve mikroişlemcili kartları kapsamaktadır. Her ikisi için de kontakların yerleri tanımlanır. Fakat bellek kartları için kabloların ve bağlantıların işlevi tanımlanmamıştır. ISO 7816 birden fazla bölümden oluşur. Her bölüm fiziksel karakteristikler, kontakların

yönleri ve yerleri, veri erişim teknikleri, veri depolama teknikleri, sayılama sistemleri ve kaydetme işlem adımları konusunda en alt düzeyde sağlanması gereken özellikleri kapsar. Çoğunlukla kart üreticileri, kendi ürünlerini diğerlerinden ayırt etmek için yüzeyde kontakları farklılaştırmaktadırlar. Bu yüzden standart yalnızca kart ile okuyucu arasında iletişimi sağlayan elektriksel kontakların yerlerini tanımlar.

Standartlar fiziksel, elektriksel, ve veri bağlantı protokol katmanlarındaki uyumluluğu taban alarak tasarlanmıştır. Fakat aygıt bağımsız Uygulama Programı Arayüzleri (API), geliştirme araçları, kaynak paylaşımı gibi konularda uyumluluk kapsanmamaktadır.

PC/SC(Personal Computer / Smart Card) çalışma grubu Mayıs 1996'da Microsoft, Groupe Bull, Hewlett-Packard, Schlumberger ve Siemens Nixdorf gibi akıllı kart ve kişisel bilgisayar şirketleri tarafından bu konudaki gelişmelerin standartlarını oluşturmak için kurulmuştur.

2.3. AKILLI KART İŞLETİM SİSTEMLERİ

Farklı üreticiler tarafından üretilen akıllı kart işletim sistemlerinin şimdiye kadar birbirine uyumlu olduğu görülmemektedir. Bu da uygulama geliştiricilerinin işini zorlaştırmakla birlikte maliyeti artırıcı bir etkendir. Günümüzde öne çıkan işletim sistemleri "Multos" ve "JavaCard" dışında yeni olarak "Smart Cards for Windows" tur.

Multos, yüksek güvenlikli çoklu-uygulamalara dayalı bir akıllı kart işletim sistemidir. Kart fonksiyonları, bu sayede yüksek güvenlikli bir platform üzerinde geliştirilebilir. Akıllı kartlar için geliştirilmiş uluslararası standartlarla uyumludur. Multos'ta kart üzerine yerleştirilen her uygulama bellekte kartın geri kalanından soyutlanarak güvenlik sağlanır. Bu özellik kartın kullanımı sırasında da her hangi bir uygulamanın güvenli bir biçimde bir kişisel bilgisayar veya başka bir araç tarafından diğerlerinden bağımsız olarak silinebilmesine veya eklenebilmesine olanak verir. Multos için uygulamalar "C" gibi yüksek düzeyli bir dil kullanılarak da geliştirilebilir.

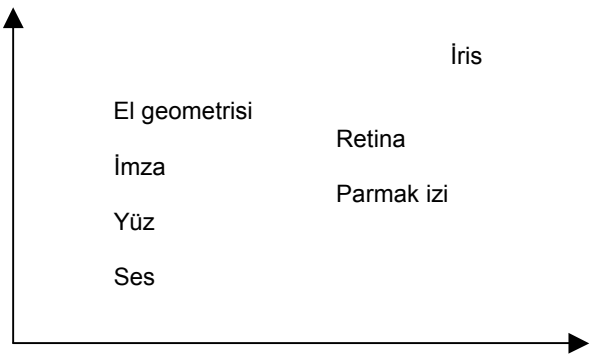
Java Card teknolojisinin platformdan bağımsız olması ve tek bir kart üzerinde farklı uygulamaların çalışmasına izin vermesi neden ile tercih edilmektedir. Kart bir kez üretildikten sonra değişen ihtiyaçlara bağlı olarak yeni uygulamalar yüklenmesine olanak tanır. Ayrıca, akıllı kartların programlanmasında nesneye dayalı programlama yeteneklerinden dolayı bir esnekliğe sahip olması ve var olan akıllı kart standartlarıyla uyumluluğu nedeniyle işletim sistemi olarak Java Card kullanılması yararlı olmaktadır.

Ekim 1998'de Paris'te düzenlenen Cartes sempozyumunda Microsoft, akıllı kartlar için geliştirdiği Smart Cards for Windows işletim sisteminin duyurusunu yaptı. Bu sistemde ağlar ve internet web sunucularına güvenli erişim, açık/ kapalı anahtara dayalı uygulamalar ve elektronik-ticaret uygulamaları yer almaktadır. Standart sürümün bir parçası olarak Windows 2000 işletim sistemi, akıllı kart tabanlı kullanıcı onayını desteklemektedir.

3. BİYOMETRİK TEKNİKLERİN ASILLAMADA KULLANIMI

Kimlik onaylama süreci için en sık kullanılan yöntem PIN (Personal Identification Number) kullanımıdır. PIN kullanımında bir problem, kullanıcının PIN numarasını aklında tutması gerektiğinden ortaya çıkar. PIN unutulduğunda sisteme erişim söz konusu olamayacaktır. İkinci büyük problem; bu yöntemin, güvenilir olmayan ortamlarda tek başına uygulandığında, yetkisiz kullanıcıların sisteme erişip gizli bilgileri eline geçirmesi olasılığına karşı açık olmasıdır. Bu duruda güvenliği artırıcı çözümlerin sisteme dahil edilmesi gerekir.

Biyometrik, genel anlamıyla, kullanıcıların kendilerine ait özelliklerini (fiziksel veya davranışsal özellikler) kullanarak kimlik tanıma ve onaylama yöntemleridir. Biyometrik tanıma sistemleri kullanıcının sahip olduğu özelliklerin tekilliğini kullanır. Bu özelliği ile biyometrik sistemler, kullanıcı verisi ve yetkisiz erişimler arasında bir engel oluşturur. Bu yöntemler; parmak izi, el geometrisi, iris/retina, ses, yüz tanıma, DNA, klavye kullanımı, imza tanıma vb. şeklinde sıralanabilir. Bu yöntemler arasında uygulamaya göre seçim yapılırken doğruluk, kullanım kolaylığı, uygulama için oluşturduğu veri miktarı, hata oranı ve maliyet ölçütlerinin göz önüne alınması gerekir. Şekil 1' de mevcut biyometrik teknikler, doğruluk ve maliyet açısından incelenmiştir.



Şekil 1 Biyometrik Teknikler

Çeşitli ölçümler sonucu elde edilen bilgilere göre ses tanıma yöntemi tek başına kullanıldığında tanıma için doğruluk faktörü fazla olmayacaktır. Eğer görüntü, ses ve parmak izi tanıma tekniklerinin hepsi aynı sistemde kullanılırsa etkin bir tanıma işleminin gerçeklenebileceğini söyleyebiliriz. Doğruluğu en fazla olan yöntem iris tanıma yöntemi olmasına rağmen maliyet oldukça yüksektir. Yüz tanıma yönteminde oluşturulan şablon diğer yöntemlerdekilerle karşılaştırıldığında oldukça yüksektir. Parmak izi tanıma yöntemi hem doğruluk hem de maliyet açısından optimum bir yöntemdir. Tüm bu ölçütler göz önüne

alındığında parmak izi tanıma yönteminin orta ölçekli uygulamalar için uygun olduğu görülmüştür.

Parmak izi tarayıcıları, taranan parmak izi şeklini görüntü işleme ve şifreleme algoritmaları ile saklama ortamı üzerine aktarılabilecek bir şablona dönüştürür. Parmak izinde bulunan temel şekiller her insan için farklı değildir. Bundan dolayı şablon, ayrılma ve birleşme noktaları, kıvrılma, bölünme noktaları ve bu noktaların birbirlerine göre bağıl konumları ve noktalar arası ilişkiler ile oluşturulur. Ufak ayrıntıların da eklenebileceği bu veri her insan için tektir. Oluşturulan şablon kullanıcı parmak izi bilgisini taşır ve saklama ortamında tutulur. Bu veri biyometrik sistemlerin tümünde olduğu gibi kod çözme gibi yöntemlerle yeniden elde edilemez. Bundan dolayı biyometrik sistemler yüksek ölçüde güvenli sistemler olarak karşımıza çıkar. Tarama sonucu oluşturulan bu veri, üretici firmanın tasarımına göre 100-1000 Sekizli arasında değişir.

Kullanıcının tanınması ve yetkili kişi olup olmadığının belirlenmesi için mevcut parmak izi bilgisinin daha önceden saklama ortamına saklanmış olan veri (orijinal veri) ile karşılaştırılması gerekir. Orijinal veri ile taranan veri arasındaki fark belli sınırlar içinde ise veri kabul edilir, değilse veri reddedilir. Yetkili kullanıcıların reddedilmesi ya da yetkisiz kullanıcıların kabul edilmesi de söz konusudur. Bu durumlar sırasıyla FRR (False Rejection Rate) ve FAR (False Acceptance Rate) olarak adlandırılır ve olasılık terimleri ile ifade edilir. Bu durumların hangi sıklıkta oluştuğu da biyometrik sistemin bir başarım ölçüsüdür.

3.1. PARMAK İZİ TANIMA AYGITLARI

Biometrics Identification MV1100 parmak izi tanıma cihazı ayarlanabilir FRR ve FAR imkanı sunar (1/100-1/1.000.000). Oluşturduğu şablon ise 350 sekizlidir. Gemplus ve Veridicom “Match-on-Card” parmak izi destekli akıllı kartlar projesinİ ortak yürütmektedirler. Bu projede parmak izi tanıma işlemleri tümüyle akıllı kartın üzerinde gerçeklenir. Oluşturulan şablonun ayrıca kişisel bilgisayara aktarılmasına gerek kalmaz. Böylelikle bu işlem 1saniyeden çok daha kısa bir sürede gerçeklenmiş olur.

Motorola ve Identix firmaları parmak izi tabanlı güvenliği sağlamak üzere DFR300(R) okuyucu birimini piyasaya sürmeye hazırlanmaktadırlar.

Compaq parmak izi tanıma birimi, 127 sekizli şablon oluşturur. SecuGen Parmak izi Tanıma Birimi (FDP01) giriş, kayıt ve onay işlemlerini 0,5 saniye gibi kısa bir sürede gerçekleyebilir. Bunun yanında oluşturduğu şifrelenmiş şablon 400 sekizli boyutundadır. Identix Parmak izi Okuyucusu 256 sekizli şablon bilgisi oluşturur.

4. AKILLI KARTLAR VE SAĞLIK ALANINDAKİ KULLANIMI

Akıllı Kartlar ilk kez 1974’te Moreno/Innovatron tarafından tanıtılmıştır. İlk büyük uygulaması 1982’de Fransa’da gerçeklenmiştir. Avrupa ülkelerinde GSM gibi yaygın kullanım alanları oluşurken, ABD’de yaygın kullanım çok sonraları başlamıştır. X.509 olarak da bilinen sayısal sertifikaların kullanıcı ve organizasyon tabanında asıllama amacıyla kullanımına dayalı olarak gelişen elektronik ticaretin yaygınlaşması, akıllı kartların bu alanda geniş bir pazar bulmasına neden olmuştur. Böylece akıllı kart teknolojileri hızla gelişmeye başlamıştır.

Akıllı kart tabanlı sağlık kartı uygulamaları da yaygınlaşmaktadır. Hastaların tıbbi kayıtları arasından küçük bir veri kümesi seçilerek sağlık kartına yüklenir. Böylece kart kullanımı ile, taşınabilir tıbbi kayıtlar, diğer kayıtlara erişim bağlantıları, veri tabanları için erişim anahtarları ve sağlık hizmetleri arasında bütünlüğü sağlayan bir sistem kurulmasını kolaylaştırma gibi yetenekler elde edilir [9]. Sağlık kartı uygulamalarında internet önemli bir yere sahiptir. İntranet/internet teknolojilerinin yayılması daha yüksek seviyeden güvenliği gerektirir. Güvenlik özellikle şu konularda önem kazanmaktadır: siteler arası haberleşmenin korunmasında, kişisel bilgilerin saklanmasında, elektronik hareketlerin korunmasında. Bu türden uygulamalarda kullanılacak olan hizmetler; istemci işlemlerinde sunucu tanımlama, sunucu işlemlerinde istemci tanımlama, kriptografi ve elektronik imzalar, kişisel verilerin saklanması (kişisel anahtarlar), genel bilgilerin saklanması (açık anahtarlar) olarak sıralanabilir. Sağlık kartlarının uygulama alanları arasında, acil yardım, toplumsal ve genel tedavi (diabetik, özürlü vb. tedavileri), koruyucu hekimlik, nüfus toplulukları (çocuklar, yaşlılar, hamile kişiler vb.), muhasebe ve yönetimsel amaçlar, veri bankalarını sorgulama ve farklı hizmetler arasında veri alış verişi sayılabilir. Sağlık kart, sosyal güvenlik kartı, sigorta kartı adı altında, kapsamlarında farklılıklar taşıyan uygulamalar aşağıdaki bölümde özetlenmektedir.

4.1.GERÇEKLENEN SAĞLIK KART UYGULAMALARI

Lombardia Bölgesi’nde bir çok işlevli kart sistemi hayata geçirilmiştir. Sosyal bilgi sistemi ve sağlık sistemi bir arada düşünülmüştür. Sağlık harcamalarını ve kaynak kullanımını kontrol etmek amacıyla yola çıkılarak tüm sağlık çalışanlarını birbirine bağlayan bir ağ kurulmuştur. Bu ağ Genel Yönetim/ Sağlık Bölümü ile iletişimin güvenli akışını ve verimli haberleşmeyi denetlemektedir. Lecco’da tüm halka mikroişlemci kartlar dağıtılmıştır. Kart, sisteme girebilmek ve ağdaki servislerden yararlanabilmek için bir anahtar işlevini görmektedir. Hasta ile ilgili bilgilerin bir kısmı kart üzerinde bir kısmı da hastaneler veya diğer yapıların veri ambarlarında tutulmaktadır.

Eylül 1999’da Amerikan Askeri Birliği, plastik kartların yerini, çoklu uygulamalı, akıllı kartların alacağını açıklamıştı. Yaklaşık olarak 800 000 personel bu yeni kartı kullanacak. Kartın mevcut ağ yapısı ile bağdaştırılacağı ve gelişmekte olan Açık-Anahtar Altyapı Sistemi ile uyumlu anahtarlara sahip olması düşünülüyor. Bu projenin 2003’te tamamlanacağı tahmin ediliyor.

ABD'de akıllı kart ile sağlık uygulamaları konusunda şimdiye kadar yapılan en büyük proje Ocak 1999'da Bismark, Kuzey Dakota ve Cheyenne, Wyoming'de başlatıldı [6]. 25 binden fazla akıllı kart ailelere dağıtıldı. Health Passport Project adı verilen proje ile hastanın geçmiş önemli sağlık kayıtlarının akıllı kartta güvenli bir şekilde saklanması amaçlanıyor. Ayrıca kartın yaygın olarak pek çok sağlık biriminde de kullanımı amaçlanmış. "Health Passport" projesi, akıllı kartlar, uç birimler, okuyucular ve yazılımlardan oluşmaktadır.

ABD'de bir başka pilot bölgede ise çok işlevli akıllı kartların uygulaması başlatılmış. VA/DoD Çoklu-Uygulama kartı, hasta/ kullanıcı kimliğini belirlemek, acil erişilmesi gereken veriyi tutmak, bilgiyi birimler arasında paylaştırmak gibi amaçların yanında genel amaçlı kullanım için bir elektronik-cüzdan uygulamasıdır.

Oklahoma'da 1997'de başlatılan sağlık alanındaki bir başka akıllı kart uygulaması ise bir acil durum projesidir. Akıllı kart birleşik sağlık hizmeti dağıtımı ağının ilk adımı olarak kullanılır. Ambulans çalışanları ve eczacılar için gerekli bilgileri içerir.

Fransa'da geçtiğimiz yıllarda uygulamaya konan akıllı kart uygulamasında sağlık ve sosyal güvenlik hizmetlerinin bir arada yürütülmesi amaçlanmış. 42 milyon kart halka dağıtılmıştır [6]. Sağlık personelinin güvenli yoldan haberleşmesi, ödemelerin kolayca yapılabilmesi, sağlık verilerine erişimin denetlenmesi gibi amaçlara yönelik olarak bu kartlar kriptografik işlemci içerir ve gizli-anahtar güvenli bir şekilde saklanabilir. Fransa'da bir sağlık ağı kurulmuştur. Ağdaki bilgiye erişimi denetlemek amacıyla Healthcare Profession Card adı verilen uzman personele ait kartlar kullanılmaktadır.

Almanya ise 1994-95 yıllarında 80 milyon kart dağıtarak bir sağlık, sosyal güvenlik uygulamasını başlatmıştır. Bu kartlar sosyal sigorta bilgisini taşır [6]. Okuyucu/yazıcı sistemi sayesinde hastanın sosyal sigorta formu yazıcıdan alınabilir. Sigorta fonu ile elektronik olarak haberleşme sağlanır. Bunun dışında Almanya'nın da uluslararası bir uygulama olarak tasarlanmakta olan NETLINK projesine dahil olabilmesi için ek işlevler geliştirilmektedir. Proje Berlin'de Sağlık Kurumu tarafından desteklenmektedir. Hem hasta hem de sağlık personeli için asıllama işlemi, sayısal imza kullanımı, internet üzerinde güvenli haberleşme konularında ilerleme sağlanmıştır.

NETLINK projesi, Avrupa Birliği tarafından desteklenen, sağlık kartındaki bilgilerin ülke dışında da geçerli olabilmesi için bir uyumlulaştırma projesidir. 1998'de başlatılan projenin pilot bölgeleri, Fransa, Almanya, İtalya, ve Kanada'dır.

Bir başka çok uluslu akıllı kart projesi ise Avrupa Komisyonu tarafından desteklenen CARDLINK'tir. Eylül 1994'te başlatılmış ve 5 yıllık pilot aşamasını tamamlamıştır. Bu kartlarda acil sağlık verileri ve kimlik bilgisi saklanmaktadır. Hastanın daha önceki tedavi bilgilerine erişim için bu bilgilerin merkezlerine internet üzerinden ulaşmayı sağlayan işaretçiler bulunmaktadır. Yaklaşık 100 bin kart dağıtılmıştır. Acil durum bilgisi katılımcı ülkelerin hangisinde kullanıldığına bağlı olarak o ülkenin diline çevrilmek üzere uyumlaştırılmıştır. 5 pilot bölge, Fransa'da Saint Nazaire, İrlanda'da Dublin, İtalya'da Milan ve Roma ve İspanya'da Valencia'dır.

Aynı amaçla 1995'te başlatılan bir başka proje G-8 ülkelerini kapsamına alan G-8 Sağlık Hizmeti Verisi Kart Projesi'dir.

Bir başka uluslararası proje ise TrustHealth İnsiyatifi'tir. Bu proje, tüm Avrupa'yı kapsayan bir açık sistemlerin bağlantısı içinde, modern güvenlik teknikleri kullanan güvenilir telematik sistemleri göstermek için tasarlanan bir çatıdır. Sağlık bilgilerinin güvenliğini sağlamak için RSA şifreleme ve akıllı kart kullanılmıştır. Burada ulusal güvenilir üçüncü şahıslar anahtarların bulunduğu kartları yayınlamak ve kullanıcı ile açık-anahtar arasındaki bağlantıyı sağlamak için gereklidir. Katılımcı 9 ülke arasında İsveç geniş rol oynamaktadır.

5. BIR SAĞLIK KART UYGULAMASI TASARIMI

Bölümümüzde sağlık-kart konusunu incelemek ve uygulama geliştirmek üzere bir çekirdek kadro kurulmuştur. Aşağıdaki bölümlerde, tasarımına başlanan projenin ana çerçevesi sunulmuştur.

Projede; kişilere ait sağlık verilerinin kişilerin taşıyabileceği bir ortamda ve bilgi merkezlerinde saklanmasını, erişilmesini, kayıt edilmesini ve bakımının yapılmasını gerçekleyen bir bilgisayar sisteminin tasarımı ve küçük boyutlu bir uygulaması amaçlanmaktadır. Sistemi kullanacak olan kişilerin sisteme güven duyabileceği bir ortam sağlanacaktır. Kişisel verilerin korunması ve izinsiz ve amacı dışında kullanılmamasının sağlanması amaçlanmaktadır. Ancak bu amacın, kullanıcı ve/veya yetkili hataları gibi bazı olağan dışı konularda sistemin işletilmesi ve denetlenebilen bir sistem yaratılması gerekir. Bunun için uygulamaya yönelik en elverişli çalışma biçimi oluşturulmalıdır.

Projenin kapsamında; sağlık verilerine erişimi kolaylaştırmak ve hızlandırmak, hizmet kalitesini artırmak, hasta bilgilerinin güvenli bir ortamda saklanması, sağlık verilerine değişik hastane, klinik vb. sağlık merkezlerinden erişimin ve bu verilerin hastaya yapılan işlemlerden sonra güncellenmesinin sağlanması, hasta ile ilgili verilerin yönetiminin tek bir merkezden yapılarak tutarlılığın sağlanması, hastanın geçmiş tedavi ve teşhis bilgilerini merkezi bir ortamda tutulması, kişisel verilerin güvenliğinin sağlanması yer almaktadır.

Sistemde saklanan ve aktarılan tüm kişisel veriler şifrelenmektedir. Veri şifreleme, akıllı kart okuyucusundan bilgi merkezine erişme olarak değişik aşamalarda kullanılmaktadır. Bilgi merkezinde ve akıllı kartta saklanan veriler sınıflara ayrılmıştır. Temelde 3 sınıf öngörülmüştür. Bunlar şu şekilde sıralanabilir: Akıllı kart ile erişilen veri sınıfı, kullanıcı şifresi ile erişilen veri sınıfı ve biyometrik imza ile erişilen veri sınıfı. Verileri

sınıflara ayırma kişiye özel ve kişi denetimindedir. Her sınıf veri farklı anahtar ile şifrelenmiş olur. Yetkili kullanıcılar için farklı yetki seviyeleri belirlenmiştir. Bilgi merkezi için küçük boyutlu ve ölçeklenebilir bir veri tabanı modeli tasarlanmaktadır. Sunucu bilgisayar, istemci bilgisayar ve uç birim bilgisayarı için gerekli programlar web tarayıcı üzerinden kullanılabilecek esneklikte ve geliştirmeye açık tasarlanmaktadır.

5.1. TASARIM İLKELERİ

Gerçeklenecek sağlık sisteminde güvenliğin planlanmasında 5 ilke gözetilmiştir [5]:

1. Kullanılabilirlik- Gerektiğinde uygun yerlerden erişilecek bilginin doğruluğundan, kesinliğinden, güncellenmiş olduğundan emin olma.
2. Sorumluluk- Sağlık çalışanlarının kendileri ile ilgili verilere erişim ve kullanımları konusunda sorumluluk sahibi olmaları.
3. Dışarıya karşı koruma- Bilişim sistemine fiziksel ve mantıksal olarak güvenli erişimin sınırlarının bilinmesi ve kontrol edilebilmesi.
4. Erişim Denetimi- Sağlık çalışanlarının yalnızca kendi işleri için gereken kadar bilgiye erişmelerine izin vermek, bu sınırın ötesindeki bilgiye erişimi kısıtlama.
5. Anlaşılabilirlik ve kontrol- Sistemi kullanan herkesin verilerin güvenliği ve erişimi konusunda bilgili ve denetim sahibi olmalarını sağlama.

Asıllama, erişim denetimi, işlemleri izleme, sistemin fiziksel güvenliği, dışarıdan haberleşme bağlantılarını ve erişimi denetleme, organizasyon içindeki yazılım disiplininin kullanımı, sistem yedekleme gibi çalışma başlıklarındaki organizasyon bu 5 ilkenin değişik bileşimlerini kapsar. Güvenlik konusunda ihmallerden dolayı oluşan risklerle bilgi güvenliğine yapılan saldırılar arasında dengeli bir yaklaşım sergilemek gerekmektedir. Çoğu sağlık sistemleri heterojendir. Örneğin bazı alt sistemlerde çok etkin güvenlik mekanizmaları tasarlanmış olabilir ama organizasyonun diğer alt sistemlerinde bu sağlanmadığında buradan sistemin tümden güvenliği sağlanamayacaktır.

5.2 SİSTEM BİLEŞENLERİ

Bilgisayar sistemi; tıbbi kayıtların saklandığı sunucu bilgisayarı kapsayan bir bilgi merkezinden; tıbbi kayıtları ve kişisel bilgileri sisteme sunumunu yapan, akıllı kartlara yükleyen, bunlara erişen, ve hastanelere yerleştirilen istemci bilgisayarlardan; veri erişimi sağlayan ve küçük boyutlu hastanelere, sağlık ocaklarına ve gezici birimlere yerleştirilen taşınabilme özelliğine sahip uç birim bilgisayarlarından oluşmaktadır. Uç birim bilgisayarlardan sunucuya erişim mümkün olsa da sunucu üzerindeki verilerin güncellenmesi işlemi istemci bilgisayarlar tarafından yapılabilecektir. Sistemin bileşenleri internet üzerinden bilgi akışını düzenlemektedir. Taşınabilir veriler akıllı kartlarda yüklüdür. Acil durumlarda sadece akıllı kart üzerindeki verilere erişilmesi için uç birim bilgisayarlarının sisteme bağlanmadan çalışması mümkündür. Ayrıca sisteme erişimi sağlayan yetkililerin asıllanması için de yine akıllı kartlar kullanılmaktadır. Sistemin donanım bileşenleri Şekil 2'de görülmektedir. Hasta kartında bulunan veriler aşağıda listelenmiştir.

Hasta kartındaki veriler:

-Kişisel veriler(adres, telefon, ad, soyadı)
-Yöneticilik ile ilgili veriler,
-Bilgi merkezinde bulunan sağlık durumu verilerine işaretçiler,
-Acil durum (kan grubu, alerji durumu, önemli kronik hastalıklar…)
-Elektronik imza
-Biyometrik veriler

Çözülmesi gereken güvenlik problemleri, bilginin bozulmadan yerine ulaşması, veriyi gönderen ve alan tarafın kimliklerinden emin olunabilmesi, verilerin hiç bir aşamada istem dışı müdahaleye uğramamasıdır. Sistem tarafından bakıldığında kart iki farklı işleve sahiptir:

1. verilerin donanım aracılığıyla şifrelenmesi.
2. yetki sınama/onaylama sağlanması amacıyla elektronik imza ile dokümanların imzalanması.

Sistemin temel işlevleri arasında tanıma, yetki sınama/onaylama (hakların ve izinlerin belirlenmesi), asıllama, günlük tutma, merkezi yönetim sistemleri, sağlık sisteminin veri tabanı yönetimi vardır.

5.3 ASILLAMA

Asıllama işlemi, temel olarak, gönderilen bilginin gerçekten doğru yetkili kişiye gönderildiğinden emin olunmasıdır. İşletim sisteminin, yapısını değiştirecek dış saldırılardan korunması gerekmektedir. Bu durumda sistemin güvenlik mekanizmaları işletim sisteminin yapacağı işlemlerin yerine getirilmesine engel olmalıdır [1].

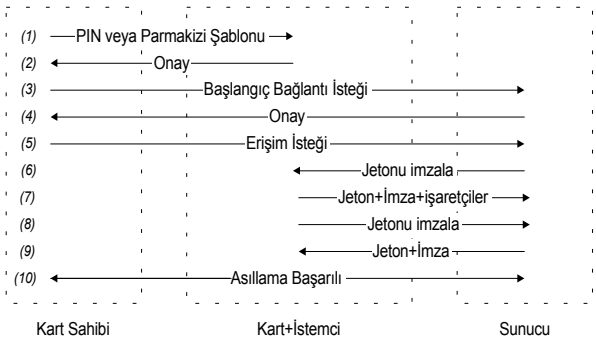
Asıllama işlemi iki basamaklı olarak düşünülmüştür. Kartın erişilebilir olması için kullanıcının sistem tarafından tanınıyor olması gerekir. Kartın fonksiyonlarından yararlanabilmek duruma göre koşullu (kişisel PIN kodunun veya biyometrik verinin doğrulanmasına bağlı) veya koşulsuzdur. Kart ve kart kullanıcı arasındaki bu asıllama işlemi birinci basamaktır. Yetkili kartları yalnızca yetkililer tarafından kişiye özel PIN kodunu girmeleri ile mümkün olurken, hasta için asıllama işlemi hastanın isteğine bağlı olarak farklı düzeylerde gerçekleşir.

1-Acil durumda hastanın bilinci yerinde değilken yetkili kartı kullanılarak hasta kartındaki acil durum verilerine erişim mümkün olmalıdır. Burada hastaya ilişkin kartta kayıtlı bulunan biyometrik veri kartın doğru kişiye ait olup olmadığını test etmek için kullanılır.
2-Hastanın seçimine bağlı olarak bazı erişimler kişisel PIN kodu ile denetlenirken bazıları ise biyometrik veri ile denetlenir.

İşlem yapabilmek için sağlık çalışanının ve hastanın kartının bir arada kullanılması gerekir. Merkezi bilgi merkezindeki bilgiye erişim için hasta kartı bir işaretçi

görevini görür. Bu işaretçilerin kullanılarak sunucu üzerindeki bilgiye erişim ise yetkili kartı ile sunucu arasındaki asıllamanın yerine getirilmesine bağlıdır. Böylece asıllmanın ikinci basamağı tamamlanmış olur.

Şekil 2' de bu iki basamaklı asıllamanın basit akışı görülmektedir. Kart ve kart sahibi arasındaki asıllama işlemi (1 ve 2) kartın tipine ve hastanın durumuna göre daha önce anlatıldığı gibi değişecektir. Bağımsız çalışma durumunda yetkili kartının yetkilerine ve hasta ise kartı arasındaki asıllamanın cinsine ve durumuna bağlı olarak hasta kartındaki bilgilere erişim sağlanacaktır.



Şekil 2. Asıllama akış şeması

Sunucu bağlantısının kurulması durumunda başlangıç bağlantı isteği ile birlikte (3), yapılacak uygulamaya bağlı URL seçilmiş olur. Kartlara ilişkin tanımlayıcı veriler de bu istekle birlikte sunucuya ulaşır. Bu verilerin anlamlı olması durumda seçime bağlı olarak uygun Java appleti isteğin geldiği istemciye veya uç birimlere gönderilir. (4)

Erişim isteğine yanıt olarak sunucu asıllama için bir jeton gönderir. Jetonu alan istemci bu jetonla birlikte hastaya ilişkin verilere işaretçileri yetkili kişinin imzası ile imzalayarak sunucuya geri gönderir. Burada yetkili kişinin asıllaması yapılır başarıyla tamamlandığında sunucudaki hasta bilgilerine gönderilen işaretçiler yoluyla erişilmiş olur. İşaretçi kullanımının amacı, sunucuda hastaya ilişkin kişisel verilerin hastanın kimliği ile birlikte aynı tabloda tutulmasının engellenmesidir. Böylece sunucudaki hastalara ilişkin geçmiş hastalıklara dair tablolara erişen birisi, buradan hangi hastanın verisi olduğunu çıkaramayacaktır. İşaretçi bilgileri hastaya ait akıllı kart üzerinde güvenli bir şekilde tutulmaktadır.

İstemcinin sunucuyu asıllaması işlemi de benzer şekilde bir jeton göndererek bu jetonun sunucu tarafından imzalanması ile sağlanır.

Bundan sonraki hastaya ilişkin verilerin internet üzerinden gönderilmesi güvenli kanalla sağlanır. Bunun için tarayıcılar tarafından da desteklenen SSL kullanılır. SSL'e ek olarak şifreleme yöntemlerinin kullanılması araştırılmaktadır.

5.4 JAVA'NIN SEÇİMİ

Java'nın platform bağımsız olma özelliğinden yararlanılacaktır. Bu özelliği istemci tarafında kullanılır. Java'da 3 tip uygulama desteklenir. Birincisi, Java servlet'tir. Servlet, sunucu tarafında koşması gereken bir uygulamadır. Servlet, bir CGI arayüzün arkasında koşar. Diğer iki uygulama ise istemci tarafında koşar. Bu iki uygulamadan biri Java applet'tir. Applet'in diğer uygulamadan farkı, appletin başlamak için bir tarayıcıya veya bir appletviewer'a gereksinim duyması, diğer uygulamanın ise bir Java yorumlayıcı ile başlatılabilmesidir. Dışarıdan yüklenen bir Java appletinin hakları, istemcide başlatılan bir Java uygulamasına göre çok daha kısıtlıdır. Applet mekanizması, internet tarafından kullanılır. Bir applet, istemciye sunucu tarafından HTML sayfası ile birlikte gönderilir. Bu HTML sayfası, applet'in çalışmasını başlatacaktır. Bu mekanizma sayesinde sunucudan istemciye kart için gerekli parametreleri içeren bir kart modülü gönderilebilir.

6. UYGULAMA YAZILIMININ YAPISI

Uygulama yapısal olarak iki ana bölüme ayrılmaktadır. Bunlar istemci yazılımı ve sunucu yazılıdır. Şekil 4'te sistemin tasarımına ilişkin şema gösterilmiştir. Aşağıdaki bölümlerde konu özetlenmektedir.

6.1 İSTEMCİ

İstemci veya uç birimler üzerindeki yazılım iki parçadan oluşur: Sunucudan yüklenen dinamik ve istemcide bulunan statik parçalar.

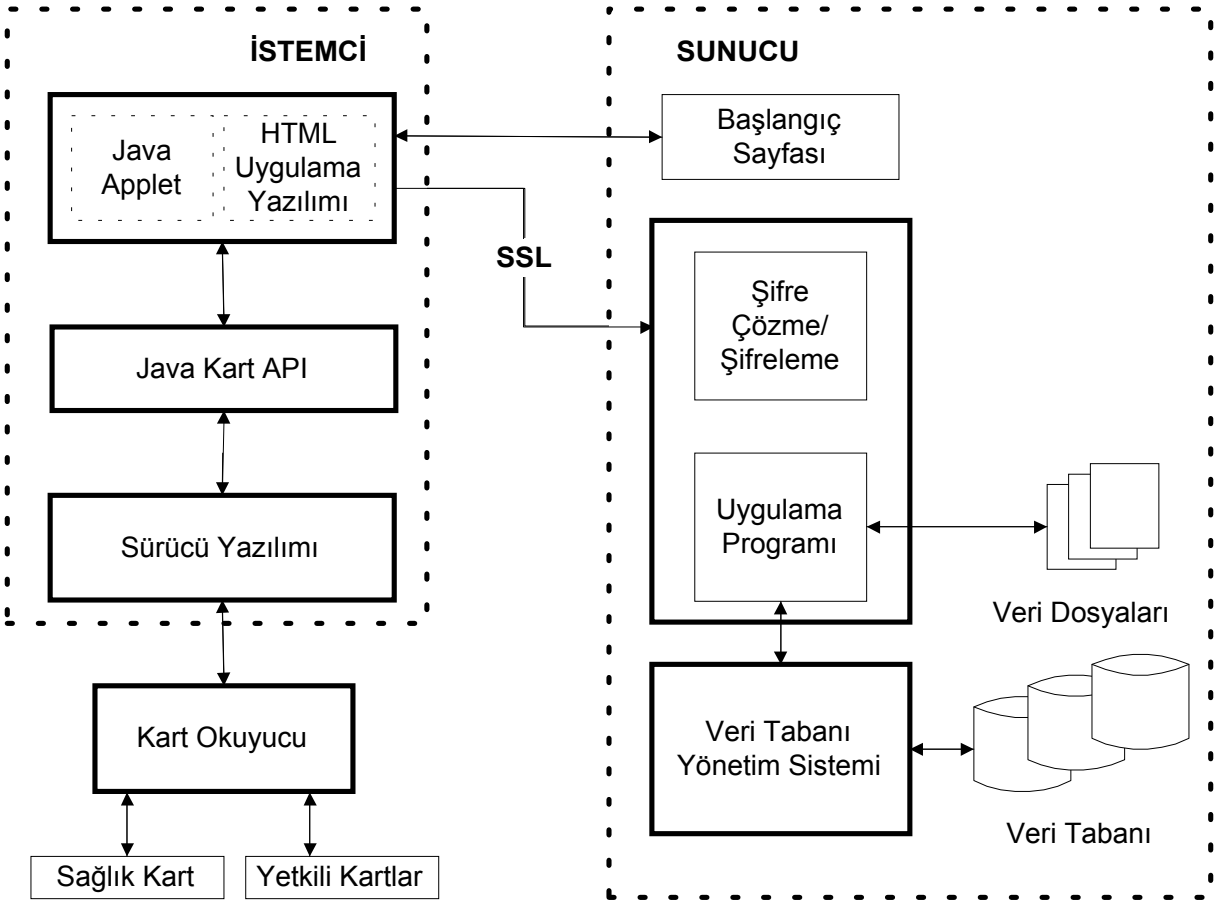
1. Dinamik bölüm: Sunucudan dinamik olarak yüklenen Java applet 'ini içerir. Sunucu ve istemci arasındaki veri akışını kontrol eder. Sunucu istemciye hangi applet 'i göndereceğini seçebilir ve istemciye uygun desteği sağlar. Java 'da yazılır.

Burada kullanılan applet'e saldırı oluşma olasılığına karşı ek koruma yöntemleri geliştirilecektir.

2. Statik Bölüm: HTML uygulama yazılımı, Java Chipcard API (Uygulama Protokolü Arayüzü), Java uygulaması ve sürücü kısımdan oluşur.

HTML uygulama yazılımı başlangıç sayfasıdır. Bağlantısız veya bağlantılı çalışma durumuna göre statik bölümdeki uygulama programını başlatır veya internet üzerinden sunucu ile bağlantı kurar. İkinci durumda uygulama programı yerine sunucudan yüklenecek applet devreye sokulur. Uygulama programı arayüzü (API), sınıflardan oluşur. En önemli iki sınıf akıllı kart okuyucu yöneticisi ve akıllı kart okuyucusudur. Bu sınıflar java uygulaması tarafından çağrılırlar. Uygulama programı, okuyucu yöneticisinden bir okuyucu yaratmasını ister. Okuyucu da bir başlatma dosyasından, okuyucu tipini ve seri iletişim iskelesi ayarlarını okur. İkinci aşamada ise akıllı kart okuyucuyu canlandırır. Uygulama, bir okuyucunun bağlı olduğunu bilmektedir ve okuyucudan akıllı kartı onaylamasını ister. Sürücü, RS232 seri iletişim iskelesini kotarır. Bu iskele ile bilginin iki yönde dış aygıta taşınması sağlanır.

alanda yapılacak çalışmalar önem kazanmaktadır.



Şekil 3. Sistemin genel şeması

6.2 SUNUCU

Sunucu tarafında HTML sayfası SGI-script'leri ve Java applet'leri vardır. Bu applet'ler karttan bağımsızdır. Sunucu tarafında ayrıca şifreleme ve şifre çözme birimi vardır: Bu birim, yönetici anahtar ve anahtar veri tabanını içerir. HTML başlangıç sayfasında uygulama ile ilgili bazı bilgiler vardır. Bu sayfa CGI-script 'i çağırır, CGI-script ise uygun Java applet 'ini çağırır.

HTML sayfası→ CGI-script → Java applet

Her yeni kart tipi için yapılacak tek değişiklik yeni bir applet eklemektir. Özel bir uygulamayı yürütmek için yalnızca sunucu üzerindeki script 'in gerekenleri tanımlamak üzere oluşturulması yeterlidir.

7. SONUÇ

Avrupa ülkelerinde ve Amerika'nın bazı bölgelerinde akıllı kart ile sağlık uygulamaları yaygınlaşmaktadır. Bu konudaki gelişmeler bölgesel uygulamaların ortaklaştırılması ve standartların oluşması ile dünyanın her yerinde geçerli olabilecek bir sağlık kartı uygulamasına doğru yönelimi işaret etmektedir. Bu nedenle ülkemizde de dünya standartları gözetilerek bu Tasarımı yapılan projede dünyadaki diğer uygulamarla da etkileşim içinde kullanılabilecek bir sistemin gerçeklenmesine çalışılacaktır.

KAYNAKÇA

[1] http://www.iscit.surfnet.nl/artikels/overige/isi.htm
[2] http://www.multos.com/
[3] http://java.sun.com/products/javacard/
[4] Henry Dreifus, J.Thomas Monk, Smart Cards, Wiley Computer Publishing, 1997
[5] For The Record, "Protecting Electronic Health Information" National Research Council, National Academy Press, Washington, D.C., 1997
[6]Daniel L.Maloney, Card Technology in Healthcare, CARTES 99 Conference Book
[8] Maurizio Amigoni, Loredana Luzzi ve diğerleri, The new Health and Social Information System of Region Lombardia. The Pilot Project of Lecco, CARTES 99 Conference Book
[9] F.Sicurello Card Applications in Healthcare, CARTES 99 Conference Book
[10] Sharath Ponkoriti, Ruud M. Bolle, "Biometrics: The Future of Identification "IBM T.S.Watson Research Center, IEEE Computer Society, Computer Magazine, February 2000
[11]P.Jonathan Phillips, Alvin Martin ve diğerleri, "An introduction to Evolving Biometric Systems", National Institute of Standarts and Technology