

BIYOMETRİK GÜVENLİK SİSTEMLERİ

Rüya ŞAMLI¹, M. Erkan YÜKSEL²

^{1,2} İstanbul Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul
{rsamli, eyuksel}@istanbul.edu.tr

Özet

Bilgi güvenliği günümüz teknoloji dünyasının en önemli problemlerinden biridir. Kişiler ya da kurumlar, her türlü bilgiyi güvenli bir ortamda tutabilmek ve bu bilgileri saklamak, korumak, gizli tutabilmek için büyük çabalar ve paralar harcamaktadır. Bir bilginin gizliliğinden ve güvenliğinden bahsedebilmek için söylenebilecek tek şey o bilginin kimsenin eline geçmemesi değildir. Bunun yanında bilginin bütünlüğü, bilgiyi gönderen kişinin gönderdiğini; alan kişinin de aldığını inkar edememesi gibi kavramlar da önem taşımaktadır. Bunlara bakıldığında gizliliğin en kritik noktalarından birinin yalnızca yetki verilmiş kişiler tarafından bilgiye erişmesi olduğu açıktır. Gerçek dünya ortamında kişilerin kimliklerini doğruladıkları imza, mühür gibi elemanlar, bu uygulamalar dijital ortamda gerçekleştiğinde geçerliliklerini yitirmektedirler. Dijital dünyada bunların yerine verilerin bazı matematiksel algoritmalarından geçirilmesi ile elde edilen dijital imzalar ya da sözkonusu kişilerin kendine has özelliklerinin kullanıldığı biyometrik güvenlik sistemleri kullanılarak sözkonusu kişinin kimlik doğrulaması sağlanabilir. Bu çalışmada dijital kimlik doğrulama yöntemlerinden biri olan biyometrik güvenlik sistemleri anlatılmıştır.

Anahtar Kelimeler : biyometrik güvenlik sistemleri, parmak izi tanıma, yüz tanıma, dijital imza

BIOMETRIC SECURITY SYSTEMS

Rüya ŞAMLI¹, M. Erkan YÜKSEL²

^{1,2} İstanbul Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul
{rsamli, eyuksel}@istanbul.edu.tr

Abstract

Information security is one of the most important problems in technology world today. People or companies spend serious force and money for holding every type of information in secure environments, storing these information and keeping them secret. The only thing that can be said while mentioning about an information's being secret and secure is not its not being obtained by anyone. In addition to this, completeness of the information, sender's and receiver's having no ability for denying that he/she sent or received the information are also important effects for information security. So it can be understood that one of the most and critical points of security is only authorized people's accessing to information. In real life, the elements like signature, seal etc that validate people's identification lose their validities when these applications are done in digital world. In digital world, instead of them, aforementioned person's identity validation can be provided by digital signatures that are obtained with data's operating in some mathematical algorithms or biometric secure systems in that personal properties of aforementioned people are used. In this paper, biometric secure systems that are one of the digital identity validation methods are explained.

Keywords : biometric security systems, fingerprint recognition, face recognition, digital signature

1. GİRİŞ

Bir bilgi gerçek anlamda hiçbir zaman tamamen gizli olamaz. Bu bilginin mantığına ters bir surumdur. Peki bilginin gizliliğinden bahsedilirken esas olarak kastedilen nedir? Bir bilginin gizli olması demek, iletilmesi amaçlanan kişiye bozulmadan, değiştirilmeden, başka birisinin eline geçmeden ulaşması demektir. Diğer bir deyişle sözkonusu bilgi, karşı taraf için gizli bir bilgi değilken, 3. şahıslar için gizli bir bilgidir. Buna dayanarak bilgi gizliliği için kimlik doğrulamasının ne kadar önemli olduğu açıkça görülebilir. Gönderilmesi istenen bilgi istenen kişiye değil de başka birisine gönderilirse istenmeyen, beklenmeyen sonuçlar doğurabilir. Kimlik doğrulanması işlemi temelde bilgi temelli, aidiyet temelli ve biyometrik temelli olmak üzere üç kısımda incelenebilir. Bu çalışmanın konusu biyometrik temelli güvenlik sistemleri olduğundan diğerlerinden yalnızca birkaç cümle ile bahsedilecektir.

Bilgi temelli kimliklendirmede kullanıcılar ve sistem yöneticisi genelde PIN olarak ifade edilen bazı numaralara veya kullanıcı adı - şifre gibi gizli bilgilere sahiptir. Bu bilgiler bir veritabanında sistem yöneticisinin yetkisi dahilinde tutulmaktadır. Kullanıcı bu bilgileri doğru bir eşleştirme ile sisteme girdiğinde veritabanı tarafından doğrulanan bilgi eşleniği sayesinde sistem yöneticisi tarafından sisteme giriş yapan kişinin doğru kişi olduğu anlaşılır ve bu sayede kullanıcının yapmak istediği işlemler kolayca gerçekleştirilebilir. Tahmin edilebileceği üzere bu tip sistemlerin en büyük dezavantajı kişinin kullanıcı adı - şifresinin ya da PIN numarasının başka biri tarafından kolaylıkla elde edilebilecek olmasıdır [1].

Aidiyet temelli kimliklendirmede; kullanıcılar genelde kapı anahtarı, şirket rozeti, kriptografik anahtar veya manyetik kart gibi eşi olmayan ve kendileri ile bütünleşen bir objeye sahiptirler [1]. Sisteme bu obje ile giriş yaparlar. Objenin içerisinde sisteme giriş yapanın sözkonusu kişi olduğunu doğrulayacak bilgiler sözkonusudur. Ancak bu yöntem bilgi temelli yöntemler gibi pek çok dezavantaja sahiptir. Kişinin sahip olduğu eşyası, sürekli olarak çalınma, unutulma, kaybolma gibi tehlikelerle karşı karşıyadır.

Biyometri temelli kimliklendirmede de kişi, aidiyet temellide olduğu gibi, kimliğini doğrulayan materyali üzerinde taşımaktadır. Ancak aidiyet temelli kimliklendirmeden farklı olarak kimlik doğrulayan eleman bu yöntemlerde kişinin zaten kendisinden ayıramayacağı ve onu diğer tüm insanlardan ayıran parmakizi, yüz, iris, ses, el izi,

imza gibi tekil fizyolojik veya davranışsal bir özelliğidir [2].

Bu şekildeki bir kimliklendirmenin gerçekleştirilme adımları şunlardır :

- Kullanıcı sisteme giriş yapmak istediğinde, kullanıcının sistem tarafından kullanılacak olan (el izi, ses, retina) biyometrik bilgisi alınır.
- Bu bilgi daha önce aynı kişiden alınıp veritabanına kaydedilmiş olan biyometri bilgisi ile karşılaştırılır.
- Veritabanı sonucu aynı ise kişi doğrulandırılması gerçekleştirilmiş olur..

2. BİYOMETRİK ÖLÇÜLER

Biyometri uygulayıcılarının amacı kişilerin kimlik ispatı için, yanlarında taşımak, kaybetmemek ya da unutmamak zorunda oldukları kart, anahtar ya da şifre gibi araçların yerine; bireyin kopyalanması ya da taklit edilmesi imkansız olan özelliklerini kullanmalarını sağlamaktır. Kimlik belirleme işlemi, fiziksel ya da davranışsal özelliğine dayanarak gerçekleştirildiği için başkasına devredilmesi, unutulması ya da kaybedilmesi durumu söz konusu değildir. Biyometrik sistemlerin oluşturulabilmesi için bazı ölçüler kullanılmalıdır. Bu ölçülere biyometrik ölçüler denir. Bu ölçülerin şifrelerde kullanımı için INCITS [3] (International Committee for Information Technology Standards-Uluslararası Bilgi Teknolojileri Standartları Komitesi) tarafından oluşturulmuş uluslararası bir standart mevcuttur. INCITS tarafından gerçekleştirilen biyometrik tanımlama sistemlerinde kullanılacak uluslararası bir standart oluşturma çabası sonucunda, örneğin, bir ülkede bir banka hesabı bulunan ve bu hesaba parmak izi ile erişebilen, bu sayede bankamatiklerden herhangi baş abir araç kullanmadan para çekebilen, bankacılık işlemlerini gerçekleştirebilen bir kullanıcı dünyanın başka bir ülkesindeki bir bankanın da bankamatığından, kendi ülkesindeki hesabına ulaşarak, işlem yapmasını mümkün kılmak için gerekli olan standartlar belirlenmektedir.

3. BİYOMETRİK SİSTEMLER

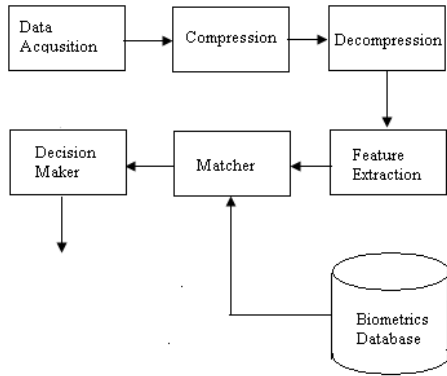
Biyometrik sistemlerin temel prensiplerinin anlaşılması ve uygulanması gerçekte çok öncelere dayanmaktadır. Binlerce yıl önce Nil Vadisi'nde yaşayan insanlar biyometrik tanımlamayı bir çok günlük iş süresince rutin bir şekilde kullanmışlardır [4].

19. yüzyılda kriminoloji araştırmacılarının insanların fiziksel özellikleri ve karakteristiklerin

suça eğilimleri ile bir ilgisinin olup olmadığını araştırmaları bu alana olan ilgiyi arttırmıştır. Günümüzde biyometrik incelemelerin boyutu ve çeşitliliği artmış, pek çok biyometrik sistemi sistemlerde yerini almıştır. Bunlardan belki de en önemlilerinden biri, polis tarafından kimlik tespitinde kullanılan ve artık pasaport başvurularında da kullanıcıdan alınan parmak izidir. Günümüzde kullanılan mevcut biyometrik tanıma sistemleri şunlardır :

- İris tanıma
- Retina tanıma
- Parmak izi tanıma
- El geometrisi tanıma
- Yüz tanıma
- Damar tanıma
- Ses tanıma

Biyometrik sistemlerin genel çalışma mekanizması Görüntü Yakalama > Özellik Çıkarma > ID Kod Oluşturma > Karşılaştırma şeklindedir ve aşağıdaki şekil ile ifade edilebilir.



Şekil 1 : Biyometrik Sistemlerin Genel Çalışma Mekanizması

Biyometrik sistemler, fiziksel (pasif) ve davranışsal (aktif) biyometrik sistemler olmak üzere temelde 2 gruba ayrılır. Fiziksel biyometrik sistemler; parmak izi, el geometrisi, yüz, ses, iris ve retina gibi kişide bulunan, diğer kişilerden ayrılmasını sağlayan sabit fiziksel özellikler üzerine kurulmuştur [5]. Davranışsal biyometrik sistemler ise; imza, yazı dinamiği, konuşma esnasındaki dudak hareketleri, yürüyüş şekli tanıma gibi belli bir zamanda belli amaçlar için gerçekleştirilmiş ve gene herkesin birbirinden farklı olarak gerçekleştirdiği davranışlar üzerine kurulmuştur.

3.1 Parmak izi Tanıma

Parmak izi en fazla kullanılan, taklit edilemez ve kişiye has bir biyometrik bilgidir. Parmak izi tanıma sistemlerinin otomatikleştirilmesi fikrinin doğduğu 1960'lı yıllardan beri parmak izi tanıma sistemlerinde kullanılan gerek yazılım gerekse

donanım alanında önemli bir ilerleme kaydedilmiştir [6]. Bir otomatik parmak izi tanıma sisteminde (OPTS) parmak izi tanıma genellikle parmak izinde bulunan özellik noktalarının ve bunlara ait parametrelerin karşılaştırılması esasına dayanır [7].



Şekil 2: Bir Parmak izi Örneği

Parmak izi tanıma sistemlerinin en önemli sorunu, taklit parmak izlerinde sistemin yanılmasıdır. Bu sorunu ortadan kaldırmak için parmak izinin alındığı parmağın canlılığını test edecek gelişmiş sensörlerin kullanımı önerilmektedir. Diğer bir sorun da bazı kişilerin deri hastalıkları, organ eksikliği, yanma gibi sebeplerden ötürü parmak izlerinin bulunmamasıdır.

3.2 DNA Tanıma

DNA tanıma günümüzde en güvenilir kimlik doğrulama yaklaşımlarından biridir. Bu yöntemde kişinin saç, kan veya diğer herhangi bir biyolojik materyali ele alınıp incelenmektedir. Yöntemde hücre nükleuslarındaki kromozomlarda saklanan DNA molekülleri kullanılmaktadır.

Doğruluğu çok yüksek bir yöntem olmasına rağmen diğer yöntemlerdeki gibi dezavantajları mevcuttur. Örneğin diğer biyokimyasal ve kimyasal analizlerde olduğu gibi DNA analizinde de yöntemin doğruluğu örnek kalitesine bağlıdır. Örneklerin karışması, kirletilmesi gibi örnek kalitesini düşüren durumlarda yöntemin başarısı da düşmektedir. Ayrıca DNA analizi diğer biyometrik teknikler ile karşılaştırıldığında maliyeti yüksek bir tekniktir. Bunun dışında işlem süresinin 24 saat gibi bir zaman gerektirmesi de bu yöntemi bazı durumlarda elverişsiz hale getirmektedir. Son yıllarda bu elverişsizlikleri ortadan kaldırmak için çalışmalar yapılmaktadır.

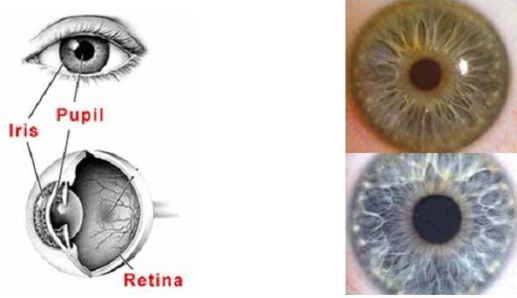
3.3 Yüz Tanıma

Bu yöntem özellikle son 10 yıldır cazibesini ve kullanılabilirliğini arttırmıştır. Askerî, ticarî ve yasal uygulama alanlarının artması nedeniyle yüzlerin otomatik olarak tanınması çok popüler bir konu haline gelmiştir. Yüz resimlerindeki bilgiyi işleyip

resmi analiz edebilecek tam otomatik bir yüz tanıma sistemi için güvenilir, iyi çalışan hızlı ve verimli algoritmalar geliştirmek gereklidir. Yüz işleme ile ilgili işlemler yüz tanıma, yüz takibi, poz kestirimi, yüz ifadesi analizi şeklinde gruplandırılabilir [8].

3.4. İris Tanıma

İris tanıma 1990'ların başında geliştirilmiş ve kişilerin iris desenlerinin analiz edilmesine dayalı, kişinin sahip olduğu iris şeklinin kişinin yaşamı süresince değişmediği gerçeğinden yola çıkılarak geliştirilmiş sistemlerdir. Genellikle havaalanları gibi kimlik doğrulama gerektiren giriş çıkış kontrol noktalarında kullanılmaktadır. Kesin bir doğruluk için parmak izi kullanılan biyometrik sistemlerde 60 veya 70 karşılaştırma noktası bulunurken, iris taramada karşılaştırma için yaklaşık 200 referans noktası kullanılmaktadır [9].



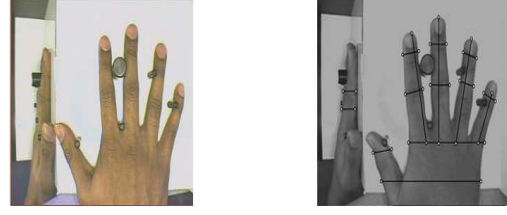
Şekil 3: İris Diagramı ve Yapısı

Bu yöntemle gözleri görmeyen, Nistagmus hastalığına sahip (gözleri titreyen) veya irisleri olmayan kişilerin kimliklendirilmesi mümkün değildir. Ayrıca iris resmi alınırken gözlerin durumu, gözkapaklarının ve/veya kirpiklerin iris desenini bozması gibi faktörler sistemi olumsuz yönde etkilemektedir.

3.5. El Geometrisi Tanıma

El geometrisi tanıma özellikle Amerika'da 20 yıldan beri kullanılan, özellikle havaalanları ve nükleer güç istasyonlarında tecih edilen bir yöntemdir. Bu metotta kişilerin elinin veya iki parmağının geometrik yapısı analiz edilir [10]. Parmakların uzunluğu, genişliği, eni ve büküm yerleri ayırt edici özellikler olarak kullanılmaktadır.

El geometrisi tanıma da yüksek doğruluk oranına sahip bir yöntem olmakla birlikte büyük ve ağır okuma cihazı nedeniyle maliyet ve kullanım açısından dezavantajlara sahiptir



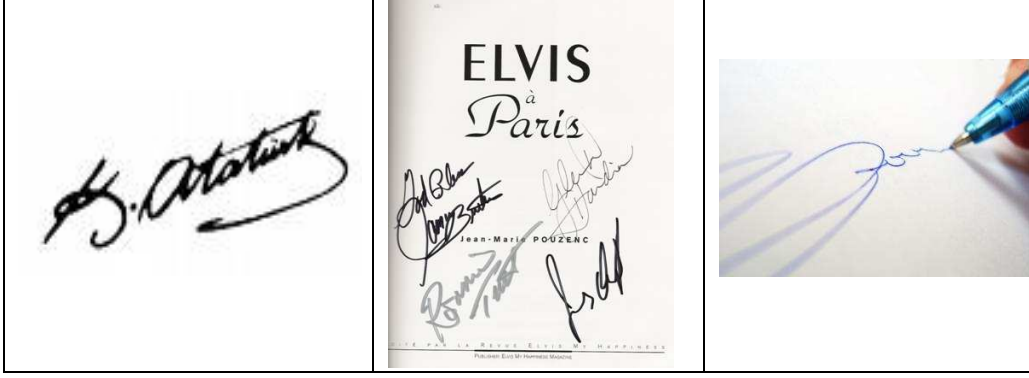
Şekil 4 : El Geometrisi ve Görüntünün Alınması

Resmin alınma süresinin uzun oluşu da sistemi yavaş yapan bir etmendir. Ayrıca yüzük, yara bandı gibi araçlar yaralanma ve parmakların kaybedilmesi, gut veya kireçlenme gibi bir takım hastalıklar nedeniyle sistem performansı düşmekte, çocuklarda ise ellerin çok hızlı büyüyüp gelişmesinden dolayı sistem hemen hiç kullanılamamaktadır.

3.6. İmza Tanıma

Kimlik doğrulanmasında güvenilir bir metot olarak tanımlanan ve uzun zamandır kullanılan imza kişinin kendi ismini yazma şekli olarak tanımlanabilir. İnsanlar imzalarını sosyal hayatın birçok alanında kullanmaktadır. İmza tanımda iki tip bilgi kullanılmaktadır. Bunlardan ilki imzalama süresi, hızı, ivmesi, kalemin basım şiddeti, kalemin gibi imzalama işlemi ile ilgili özellikler, diğeri ise bir desen olarak imzaya ait özelliklerdir. Gerçek kullanıcı olmayan herhangi birinin, kullanıcılardan birinin imzasını görsel olarak aynı şekilde taklit etse bile imza atış şeklini tekrarlaması güçtür. Bu sistemin dezavantajları olarak sistemin kullanıcının hızını, imza atma davranışını ve diğer özellikleri öğrenebilmesi için uygun sayıda örneğe ihtiyaç duyması ve imza atmanın kullanıcının o anki ruh haline, sağlığına, acelesi olup olmadığına bağlı olarak değişen bir sistem olmasıdır. Bunlar dışında damar tanıma, ses tanıma, yürüyüş şekli, tükürük sıvısı ile tanıma, retina tanıma, el yazısından tanıma gibi başka çeşitli biyometrik sistemler de az kullanılmakla beraber varlıklarını sürdürmektedirler.

Hakkında bilgi verilen bu biyometrik sistemlerin uygulama alanları günümüzde oldukça çeşitlidir [11]. Sigorta şirketleri, havaalanları giriş ve çıkış işlemleri, kredi kartı uygulamaları, kriminal amaçlı teşhis ve tespit uygulamaları, ağ ve veri güvenliği, sosyal güvenlik, vergi süreçleri gibi kamu hizmetleri, e-ticaret, elektronik imza uygulamaları, internet bankacılığı, ATM'ler, çağrı merkezleri, personel takibi, hasta takibi bu alanlardan en çok göze çarpanlarıdır.



Şekil 5 : Çeşitli İmzalar

4. BİYOMETRİ TABANLI YÖNTEMLER İLE DİĞER YÖNTEMLERİN KARŞILAŞTIRILMASI

Kullanıcı kimliğini belirleyen diğer sistemler (bilgi temelli ya da aidiyet temelli) ile biyometrik sistemler benzer yönere sahip olmakla beraber genelde birbirlerinden farklıdır. Biyometrik yöntemler dışındaki yöntemlerin biyometrik yöntemlere göre en önemli dezavantajı kullanıcıya ya birşeyler bilme ve hatırında tutma ya da

birşeyleri sürekli olarak yanında taşıma, kaybetmeme, çaldırmama, unutmama gibi sorumluluklar vermesidir. Halbuki biyometrik sistemlerde böyle bir durum sözkonusu değildir ve kişinin kimliğini doğrulayabilmek için kendisinden başka herhangi bir bilgiye, nesneye vs ihtiyacı yoktur. Biyometrik sistemlerin diğer sistemlerle avantajları, sezavantajları, benzer ve farklı yönlerini kısaca aşağıdaki gibi bir tablo ile ifade edebiliriz [12].

Tablo 1: Biyometrik Sistemler ve Diğer Kimlik Doğrulama Yöntemlerinin Karşılaştırılması

Diğer Kimlik Doğrulama Yöntemleri	Biyometrik Sistemler
Kullanılan veri her kullanıcı için kesinlikle farklı ve eşsizdir	Kullanılan veri her kullanıcı için farklı olmakla beraber bazı kullanıcıların verilerinde benzerlikler görülebilir
Kullanılan veri açıktır	Kullanılan veri açıktır
Veri kullanıcı tanımlamak için kullanılır	Kullanıcı tanımlamak için kullanılmakla beraber daha zengin bir veridir
Kullanıcı kimliği verisi kişinin istemesi halinde rahatça değiştirilebilir	Biyometrik veri kaza vs dışında değiştirilemez
Kullanıcı kimlikleri sabit olarak oluşturulur	Biyometrik veri sabit değildir
Genelde mevcut sistemlere uyumludur	Ek bir donanım maliyeti getirir
Çalınma vb durumlarda değiştirilmesi talep edilebilir	Biyometrik ölçüler değiştirilemediğinden herhangi bir şekilde elde edildiğinde geçerliliği kalmaz
Herkes için kullanılabilir	Herhangi bir biyometrik tarama sisteminde biyometrik özelliklere sahip olmayan (parmağı, gözü olmayan vb) kişiler bu sisteme dahil edemeyecektir
Zaman içerisinde değişim göstermesine sebep olacak bir durum sözkonusu değildir	Zaman içerisinde biyometrik veriler deformasyona, değişime uğrayabilir
Veri kaybı, çalınma, kaybetme tehlikesi büyüktür	Veri kaybı, çalınma, kaybetme tehlikesi needeysse hiç yoktur

5. SONUÇ

Bu çalışmada kağıt üzerinde yapılan pek çok işlemin dijital ortama geçirilmesi sonucunda ortaya çıkan dijital kimlik doğrulama yöntemlerinden biri olan biyometrik güvenlik yöntemleri incelenmiştir. Gerçek anlamda kullanılmaya başlanmaları kısa bir zaman öncesine dayanmasına rağmen kişinin şifresini kendi üzerinde taşıması olarak ifade edebileceğimiz biyometrik güvenlik sistemleri, her geçen gün daha fazla alanda kullanılmaya başlanmaktadır. İris, parmak izi, el geometrisi gibi fiziksel sabit özellikler ve imza atış şekli, yürüme şekli gibi davranışsal özelliklerin herhangi birisini kullanan sistemler günümüzde oldukça rağbet görmektedir.

Her güvenlik sisteminde olduğu gibi, biyometrik tabanlı güvenlik sistemlerinde de organizasyon dahilindeki herhangi bir yazılıma ya da sistemin donanımsal bir bileşenine yapılabilecek saldırılar mevcuttur. Biyometrik sensöre/algılama cihazına yapılan ve algılama sensörlerine yapay yöntemlerle canlı nitelikler taklit edilmeye çalışılıp sisteme giriş sağlamaya çalışan saldırılar olduğu gibi biyometrik referans veri kaynağına yapılan ve yolu kesilen verinin ardından aktif olarak alt sisteme tanıtıldığı saldırılar da sözkonusu olabilir. Bunun dışında iletişim kanalı saldırıları ya da man-in-the-middle saldırılar olarak adlandırılan ve sistemi gizlice dinleyip bilgi elde eden ve hatta transfer edilen bilgiler değiştirilerek sisteme geri veren saldırılar da biyometrik için tehdit oluşturmaktadır.

Tüm bu saldırılar ve bunların kombinasyonları biyometrik güvenlik sistemlerinde iyi tanımlanmalı ve saldırılardan korunmak için gerekli önlemler alınmalıdır.

Günümüzde özellikle havaalanları, karakollar gibi güvenliğin yüksek olarak tutulması gereken noktalarda ve şirket çalışanlarının şirkete giriş çıkışlarında kullanılan sistemlerin gelecekte kullanılması beklenen potansiyel kullanım alanlarından bazıları şu şekilde ifade edilebilir :

- Atm kullanımı: Binlerce kullanıcısı olan, bu kullanıcıların sıklıkla işlem yaptığı bankalarda sahteciliğin boyutları göz önüne alındığında bankaların bu sorunu biyometri gibi bir teknolojiyi kullanarak çözme çabası uygun bir çözüm olarak görünmektedir.
- Turizm: Yolcuların uçak, tren vs bileti alma, otel odası ayırtma ya da araç kiralama gibi çeşitli turizm hizmetlerinde ve havaalanı gibi kontrol noktalarından geçişlerinde kullanılabilecekleri biyometrik sistemlerin tasarlanması işleri oldukça kolaylaştıracaktır.
- İnternet işlemleri: Kişiyi özel biyometrik bir okuyucunun standart pc'lere entegre edilmesi ve bu sayede internetten yapılabilecek bankacılık işlemleri, resmî işlemler, pasaport vs başvuruları gibi dijital işlemlerin kişinin biyometrik kimlik doğrulaması sayesinde yapılabilmesi mantığı oldukça ön plana çıkmaktadır.
- Telefon işlemleri: Telefon cihazlarına entegre edilecek bir aygıt ile kişinin telefon üzerinden alışveriş vs işlemlerini gerçekleştirilmesi amaçlanmaktadır. Ancak, telefon cihazının, telefon hatlarının ve kullanıcı ortamlarının sabit olmayıp çeşitlilik göstermesi bu alanı zor kılan faktörlerden bir tanesi olmaktadır.

Biyometrik güvenlik sistemleri genelde ek maliyet getirmeleri, kullanımlarının bazen uzmanlık gerektirmesi, ele geçirildiği anda yenilenmesi sözkonusu olmadığından dolayı geçerliliğini kalmaması gibi dezavantajlarının yanında kişinin kendisi dışında ek bir donanım, yazılım, şifre, araç kullanmak zorunluluğunun olmaması, çalınma, unutulma, kaybolma gibi tehlikelerin yok denebilecek kadar az olması gibi avantajları ile biyometrik sistemler gelecekte daha çok yer edinecek gibi görünmektedir.

KAYNAKLAR

- [1] Açık Anahtar Altyapısı ve Biyometrik Teknikler, Necla Özkaya, Şeref Sağıroğlu
- [2] Bilgisayar Destekli Kimlik Tespit Sistemlerinde Biyometrik Yöntemlerin Değerlendirilmesi Taha Saday, Nurdan Akhan
- [3] www.incits.org

[4] <http://www.turkeyforum.com/satforum/archive/index.php/t-202.html>

- [5] Halici U.; Jain L. C.; Hayashi, I.; Lee, S.B.; Tsutsui T., Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC press, USA, 1999.

- [6] Avuç İzi ve Parmak İzine Dayalı Bir Biyometrik Tanıma Sistemi , Elena Battini Sönmez, Nilay Özge Özbek, Önder Özbek
- [7] Otomatik Parmakizi Tanıma Sistemlerinde Kullanılan Önişlemler İçin Yeni Yaklaşımlar, Şeref Sağırođlu ve Necla Özkaya, Gazi Üniv. Müh. Mim. Fak. Der. Cilt 21, No 1, 11-19, 2006.
- [8] <http://www.yuztanima.net/>
- [9] <http://www.turksan.com/biyometrik-sistemler-nedir.html>
- [10] <http://www.infomet.com.tr/handgeometry.aspx>
- [11] http://www.vizyotek.com/Teknoloji/Iris_Tanima.htm
- [12] E-Dönüşüm Türkiye Projesi 2005 Eylem Planı 6. Eylem Maddesi, “Akıllı Kartların Kamuda Kullanımı“ Konusunda Ön Çalışma Raporu, TÜBİTAK-UEKAE, Ocak / 2006.