

BİYOMETRİK GÜVENLİK SİSTEMLERİ

Bilgi Güvenliđi

- Bilgi güvenliđi günümüz teknoloji dünyasının en önemli problemlerinden biridir.
- Kişiler ya da kurumlar, her türlü bilgiyi güvenli bir ortamda tutabilmek ve bu bilgileri saklamak, korumak 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 algoritmalarla geçirilmesi ile elde edilen dijital imzalar ya da sözkonusu kişilerin kendine has özelliklerinin kullanıldığı biyometrik güvenlik sistemleri kullanılarak sözkonusu kişinin kimlik doğrulaması sağlanabilir.

Bilgi Güvenliđi

- Herhangi bir bilginin gizliliđinden dolayısıyla da güvenliđinden bahsedebilmek için kimlik dođrulama kavramı oldukça önemlidir.
- Bilgi, gönderilmek istenen kiřiye veya kuruma deđil de başka kiři veya kuruma gönderilirse istenmeyen sonuçlar ortaya çıkar.
- Özellikle bu bilgi tıp ya da askerîye gibi kritik sektörlerde ise kayıp daha fazla olabilir.

Bilgi Güvenliđi

- Bilgi güvenliđi için kullanılan kimlik dođrulama işlemi genel olarak bilgi temelli, aidiyet temelli ve biyometrik temelli olmak üzere üç farklı şekilde incelenebilir.

Bilgi Temelli Kimliklendirme

- Bilgi temelli kimliklendirmede kullanıcıların ve sözkonusu sistemi yöneten kişi(ler)in belirli bilgilere sahip olması gerekir.
- Bu bilgiler, kullanıcı adı ve şifre olabileceği gibi, pin olarak ifade edilen numara dizileri de olabilir.

Bilgi Temelli Kimliklendirme

- Bu çeşit sistemlerde kullanıcılar ve karşılık gelen bilgiler (şifre, pin vs) bir veritabanında tutulur. Kullanıcılar bilgilerini sisteme girdiklerinde veritabanında karşılaştırma yapılır.
- Eğer karşılaştırma sonucu birbirini tutuyorsa doğru kullanıcı olduğu anlaşılır ve sözkonusu kullanıcının sisteme giriş yapmasına ve sistemde yetkisi dahilindeki işlemleri gerçekleştirmesine izin verilir.

Bilgi Temelli Kimliklendirme

- Bu tip sistemlerin en önemli dezavantajı kullanıcının şifre-pin bilgilerini unutmasının ya da bu bilgilerin bir başkası tarafından elde edilmesinin kolay oluşudur.

Bilgi Temelli Kimliklendirme

- Günümüzde en çok bu kimliklendirme sistemi kullanılmaktadır.
 - Mail şifresi
 - Internet bankacılık şifresi
 - Internet sitesi üyelik şifresi
 - Banka şifresi
 - Kredi kartı / banka kartı / herhangi bir kart şifresi
 - Cep telefonu pin
 - Bilgisayar şifresi

Bilgi Temelli Kimliklendirme

YAHOO!

Yahoo ID

Password

☒ Keep me signed in

Sign In

I can't access my account
Help

OR

Create New Account

Sign in with Facebook or Google

Güvenli Bankacılığa
Hoş Geldiniz

Lütfen müşteri numaranızı ve parolanızı girin.

Müşteri Numarası

Parola

Müşteri numaramı ya da parolamı unuttum.



Kullanıcı Adı

Şifre

Giriş

[Giriş yapamıyor musunuz?](#)



Türkiye Cumhuriyeti Vatandaş Kimlik Doğrulama Sistemi

Giriş Yapacağınız Adres

www.turkiye.gov.tr

Giriş Yapacağınız Uygulama

e-Devlet Kapısı



e-Devlet Şifresi



Mobil İmza



Elektronik İmza



T.C. Kimlik Kartı

T.C. Kimlik Numaranızı ve e-Devlet Şifrenizi kullanarak kimliğiniz doğrulandıktan sonra işleminize kaldığınız yerden devam edebilirsiniz. Eğer farklı bir yöntem ile kimlik doğrulaması yapmak istiyorsanız, yukarıda bulunan diğer seçenekleri kullanarak da sisteme giriş yapabilirsiniz.

[Şifre Nasıl Alınır?](#)

[Şifremi Unuttum](#)

T.C. Kimlik No

*

☐ Sanal Klavye

☒ Numaramı Gizle

e-Devlet Şifresi

*

☐ Sanal Klavye

[Şifremi Unuttum](#)

İptal Et

Sisteme Giriş Yap

facebook

Email or Phone

☐ Keep me logged in

Password

[Forgotten your password?](#)

Log in

Aidiyet Tabanlı Kimliklendirme

- Kimlik doğrulamanın diğ er bir  eşidi olan aidiyet temelli kimliklendirmede; kullanıcılar kendileri ile eşleşen bir objeye sahiptirler.
- Bu obje genelde manyetik kart, rozet veya anahtardır.

Aidiyet Tabanlı Kimliklendirme

- Sözkonusu sisteme giriş, kullanıcılar tarafından bu objeler kullanılarak yapılır. Objenin içerisinde sisteme giriş yapanın kim olduğunu belli edecek ve kimlik doğrulaması yapacak bilgiler mevcuttur.
- Bu çeşit sistemlerde de kişinin sözkonusu objeyi unutması, kaybetmesi, çaldırması ihtimali bir dezavantaj yaratmaktadır.

Aidiyet Tabanlı Kimliklendirme



Biyometri Nedir

- Biyometri insanları birbirinden ayırt edebilecek fiziksel özelliklerini ve sergiledikleri davranışları inceleyen bilim dalıdır. İnsanları birbirinden ayırt edebilme şansını bize sunduğundan dolayı biyometri bir kimlik doğrulama sistemi olarak da kullanılmaktadır. Biyometrik tanıma sistemleri bir bireyin gerçekten 'kim' olduğunu kanıtlamasına olanak sağlar.

Biyometri Nedir

- İnsanların bunu yapması için ek olarak bir kart, cihaz, kimlik taşımamaları ve şifre gibi ezbere dayalı bilgileri kafalarında tutmamaları ise bu biyometrik tanımanın önemli avantajlarından. Unutulması veya başkası tarafından kullanılması söz konusu olmayan bir kimlik onaylama yoludur. Bu sayede kimlik, pasaport, ehliyet gibi kartların yerini tamamen alacak bir sistem geliştirilebilir. Hem daha güvenli hem de aşılması zor sistemler gün geçtikçe ortaya çıkacaktır. Örneğin üniversitemizin giriş kapısında bulunan kapılarda manyetik kartlar yerine araç sürücüsünü tanıyarak girişine izin veren bir sistemin kullanılması çok daha güvenli ve mantıklı olacaktır. Bu sayede yetki verilen kişi başka araçla da giriş yapabildiği gibi, yetkisiz bir kişi herhangi bir kartla giriş yapamayacaktır.

Biyometri Nedir

- Biyometrik tanımda kullanılacak birden fazla yöntem vardır. Gereksinimlere göre bu yöntemlerden biri veya birkaçı kullanılabilir. Birden fazla yöntemi bir arada kullanmak sonuçları kesinleştirmek için gerekli olabilir. Bu yöntemler her zaman doğru sonuçları vermeyebilir, bundan dolayı kullanım alanına göre yüksek başarı sağlayanlar seçilmelidir.
- Başarı oranının yanı sıra tanıma işleminin gerçekleşmesi için gereken sürede yöntemlerin seçilmesinde dikkate alınmalıdır. Gerçek zamanlı (real-time) tespit yapmak gerektiğinde yöntem seçimine çok daha fazla dikkat edilmelidir.

Biyometri Nedir

- Genel olarak bu sistemlerin çalışma prensibi; her yöntemin kendine ait girdi cihazıyla alınan verilerin analiz edilip daha önceden girilmiş değerlerle karşılaştırılıp eşleştirilmesine dayanmaktadır.
- Bilgisayarların birim zamanda yaptığı işlem sayısının sürekli artması göz önüne alındığında eldeki veriler ile anlık olarak alınan örneğin karşılaştırılma hızı da gittikçe artmaktadır. Saniyeler içinde yüzbinlerce veriyi karşılaştırıp doğru sonuçları veren sistemler günümüzde çeşitli alanlarda kullanılmaktadır.

Biyometrinin Tarihi

- İnsanoğlu biyometrik tanımayı doğduğu andan itibaren yapmaya başlar. Yeni doğan bebekler gerek annesini gerek çevresindeki diğer kişi ve cisimleri sıfırdan başlayarak öğrenir.
- Bu öğrenme işlemini veritabanına ilk bilgilerin girilmesi olarak düşünebiliriz. Yeni doğan bebekler örneğine dönersek bu bebekler daha sonradan gördüğü, duyduğu yani duyu organlarıyla algıladığı her şeyi önceki veriler ile karşılaştırıp belirli sonuçlar elde ederek tanıma işlemini yapar.
- Örneğin annesini sesinden ve kokusundan rahatlıkla tanıyabilir. Beynimiz bu tanıma işlemlerini otomatik olarak yapmaya başlar ve genellikle mükemmele yakın başarı sağlar.

Biyometrinin Tarihi

- Beynimiz tarafından otomatik olarak yaptığımız bu tanımanın yanı sıra sistematik olarak yapılan tanımanın ilk örnekleri insanoğlunun tarihi kadar eski değildir. Binlerce yıl önce yaşamış insanların birbirlerini göz rengi, ten rengi, boy gibi kolaylıkla ölçülen özelliklerle kesin olarak ayırt ettikleri konuyla ilgili kaynaklarda belirtilmektedir.

Biyometrinin Tarihi

- Birçok yeni teknolojinin geliştirilmesinde olduğu gibi biyometrinin de gelişiminde güvenlik unsuru öncülük etmiştir. Biyometrik tanıma birçoğumuzun filmlerden aşına olduğu parmak izinden suçluyu tespit etme gibi yöntemlerle hala kullanılmaktadır. Hızla gelişen teknoloji sayesinde parmak izinin yanı sıra günümüzde bir çok yöntem ile bu tip suçlu tespiti yapılmaktadır. Bunların en bilindik olanlarından biriye DNA testidir.
- İnsanların DNA'larının birbirinden farklı olduğu dış görünüşüne de yansıdığı gibi belirgin bir şekilde ortadadır. Tek yumurta ikizleri haricinde (tek yumurta ikizlerinin parmak izleri birbirinden farklıdır) bir insanın başka bir insanla aynı DNA'ya sahip olmadığından dolayı günümüzde bu testlerde geçerliliğini korumaktadır.

Biyometrik Temelli Kimliklendirme

- Biyometrik temelli kimliklendirme sistemlerinde kullanıcı sisteme kendisine ait olan ve üzerinde her daim taşıdığı parmakizi, iris, ses, el geometrisi, yüz gibi bir fizyolojik özelliğini veya imza atış, yürüyüş gibi bir davranışsal özelliğini kullanarak giriş yapar.

Biyometrik Temelli Kimliklendirme

- Kullanıcı bu şekildeki bir sisteme giriş yapmak istediğinde, sistem tarafından kullanıcının uygun biyometrik bilgisi (parmak izi, retina, ses retina) alınır. Alınan bu bilgi aynı kişiden alınıp veritabanına kaydedilmiş biyometrik bilgi ile karşılaştırılır. Karşılaştırma sonucu doğru ise aynı ise kişinin kimlik doğrulandırılması gerçekleştirilmiş olur.

Biyometrik Sistemler

- Biyometrik sistemlerin basit halleri ile binlerce yıl önceden beri kullanıldığı bilinmektedir.
- Yakın zamanda ise araştırmacıların insanların fiziksel özellikleri ve karakteristiklerin suça eğilimleri ile bir ilgisinin olup olmadığını araştırmaları biyometri alanına ilgiyi arttırmıştır.

Biyometrik Sistemler

- Günümüzde biyometrik incelemelerin boyutu, çeşitliliği ve kullanım alanları artmıştır.
- Bu sayede de pek çok yeni biyometrik kimlik doğrulama sistemi yerini almıştır.

Biyometrik Sistemler

- Biyometrik sistemlerin uygulama alanları günümüzde oldukça çeşitlidir.
 - havaalanları giriş ve çıkış işlemleri,
 - kredi kartı uygulamaları,
 - kriminal amaçlı teşhis ve tespit uygulamaları,
 - sigorta şirketleri,
 - 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
 - bilgisayarlar, pda olarak adlandırılan el bilgisayarları, cep telefonları ve ev kilit sistemleri

Biyometrik Sistemler

- Biyometri uygulayıcılarının genel amacı kişilerin kimliklerini doğrulayabilmeleri için, akıllarında tutmaları gereken herhangi bir bilgi ya da yanlarında taşımak, kaybetmemek ya da unutmamak zorunda oldukları kart, anahtar gibi araçların yerine; kopyalanması ya da taklit edilmesi imkansız olan özelliklerini kullanmalarını sağlamaktır.
- Biyometrik sistemlerde, kimlik belirleme işlemi, kişilerin fiziksel ya da davranışsal özelliğine dayanarak gerçekleştirildiği için başkasına devredilmesi, unutulması ya da kaybedilmesi durumu söz konusu değildir.

Biyometrik Sistemler

- Diğer yöntemlere göre çok daha az riske sahiptir.
- Ancak biyometrik sistemlerin oluşturulabilmesi için bazı standart ölçüler kullanılmalıdır.
- Biyometrik ölçüler olarak adlandırılan bu ölçülerin şifrelerde kullanımı için INCITS (International Committee for Information Technology Standards- Uluslararası Bilgi Teknolojileri Standartları Komitesi) tarafından oluşturulmuş uluslararası bir standart mevcuttur.

Biyometrik Sistem Çeşitleri

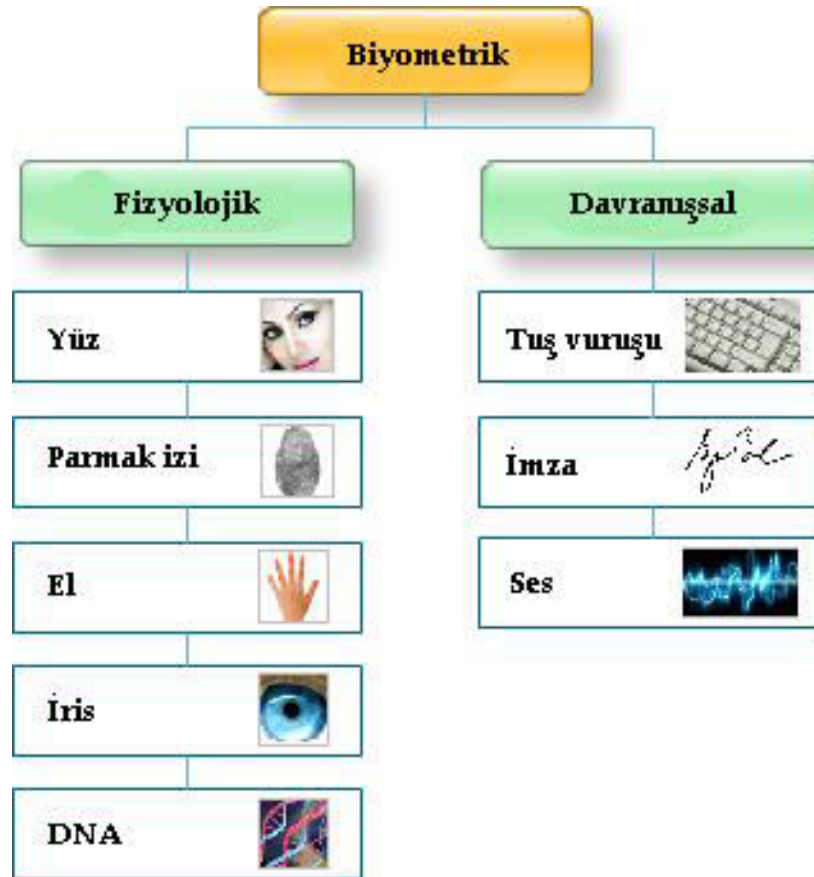
- **Fizyolojik sistemler:**

- Parmak izi
- Retina
- DNA
- Damar
- Yüz
- El Geometrisi
- Ses
- Yüz Termogramı
- İris

Biyometrik Sistem Çeşitleri

- **Davranışsal sistemler:**
 - İmza Atımı
 - Yürüyüş
 - Tuş Vuruşu
 - Konuşma

Biyometrik Sistem Çeşitleri



Biyometrik Sistem Çeşitleri - Parmakizi

- Parmak izi en fazla kullanılan, taklit edilemez ve bir biyometrik bilgidir. İlk kullanılmaya başlandığı yıllardan bu yana gerek yazılım gerekse donanım alanında parmak izi sistemlerinde önemli ilerlemeler kaydedilmiştir.
- Bir otomatik parmakizi tanıma sisteminde (OPTS) parmakizi tanıma genellikle parmakizinde bulunan özellik noktalarının ve bunlara ait parametrelerin karşılaştırılması esasına dayanır.
- Bu sistemlerin en önemli dezavantajı, parmakizinin taklit edilmesi durumunda sistemin yanılabilmesidir. Diğer bir dezavantaj bazı kişilerin pek çok sebepten ötürü (organ eksikliği, yanma, deri hastalıkları) parmak izlerinin bulunmamasıdır.
- Parmakizi taklit problemi, parmakizinin alındığı parmağın canlılığını test edecek gelişmiş sensörlerin kullanılması ile giderilebilecekken parmakizinin bulunmaması probleminin çözümü bulunmadığından bu sistem bu tip kişilerde uygulanamaz.



Biyometrik Sistem Çeşitleri - DNA

- Kişinin saç, tırnak, deri parçası, kan, sperm veya herhangi diğer bir biyolojik materyali ele alınarak hücre içerisinde bulunan DNA moleküllerindeki dizilim incelenir. Özellikle emniyet güçleri tarafından cinayet mahallinde kalan biyolojik materyaller incelenerek katillere ulaşılması veya babalık davalarının sonuçlanması işlemlerinde kullanılmaktadır.
- Doğruluğu çok yüksek bir yöntem olmasına rağmen maalesef pek çok dezavantaja da sahiptir. DNA'nın elde edileceği biyolojik dokunun kirlenmesi gibi durumlarda örnek kalitesi düşeceğinden analiz yapmak zorlaşır. Diğer dezavantajları işlemin 24 saat gibi bir sürede gerçekleştirilme zorunluluğu ve yüksek maliyet olarak sayılabilir.



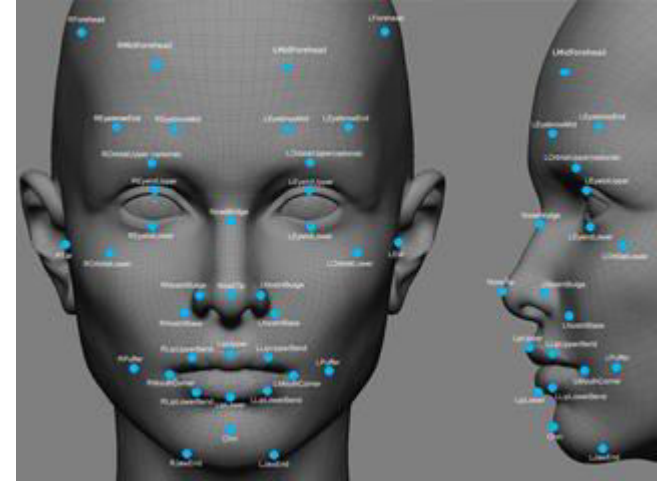
Biyometrik Sistem Çeşitleri - El Geometrisi

- Kişinin elinin veya kullanılan sisteme göre iki parmağının geometrik yapısı analiz edilir. Söz konusu yöntemde belirleyici özellikler parmakların uzunluğu, genişliği ve büküm noktalarıdır. Özellikle Amerika'da havaalanları ve nükleer güç istasyonlarında kullanılır.
- El geometrisi de diğer biyometrik yöntemler gibi doğruluk oranı yüksek bir yöntemdir. Ancak büyük ve ağır okuma cihazları nedeniyle maliyet ve kullanım açısından, resmin alınma süresinin uzun oluşu nedeniyle hız açısından dezavantajlara sahiptir.
- Bunun dışında elde bulunan yüzük gibi aksesuarlar, yara bandı gibi maddeler sebebiyle ya da yaralanma ve parmakların kaybedilmesi, gut veya kireçlenme gibi bir takım hastalıklar nedeniyle elin tanınması zorlaşır. Çocuklarda ve el ve ayakların çok hızlı büyüdüğü hastalıklara sahip olan kişilerde ise bu sistem kullanılamamaktadır.



Biyometrik Sistem Çeşitleri - Yüz

- Biyometrik teknolojide devrim sayılabilecek buluşlardan bir tanesi olan yüz tanıma sistemleri gelişen bir çok teknolojide olduğu gibi ilk kez askerîyede kullanılmıştır.
- Yüksek teknoloji silahlarının yönetimi için, özellikle ABD'de sıkça kullanılan bu sistemler bunun dışında, caddelere yerleştirilen güvenlik kameraları ile caddelerin izlenmesi ve aranmakta olan bir suçlunun bu şekilde yakalanması gibi uygulamalarda da kendilerine yer edinmişlerdir.
- Özellikle son 10 yıldır uygulama alanlarının artması nedeniyle yüzlerin otomatik olarak tanınması popüler bir konu haline gelmiştir.

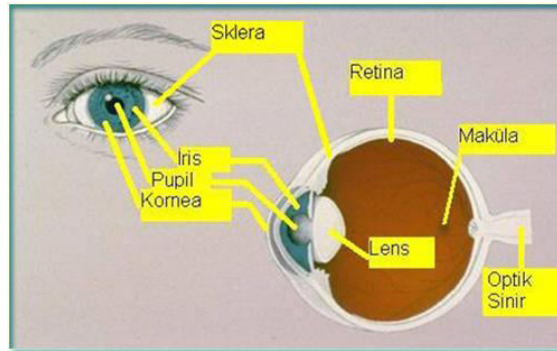


Biyometrik Sistem Çeşitleri - İris

- Yaklaşık 30 senedir kullanılan iri tanıma sistemlerinin çıkış noktası, kişinin sahip olduğu iris şeklinin ömrü boyunca değişmemesi ve diğer biyometrik sistemlere göre gözün daha az deforme olacak ve dış etkenlerden daha az zarar göreceği bir yapıya sahip olmasıdır.
- Uykusuzluk, gözyaşı, hastalıklar iris yapısını etkilemekle beraber diğer yöntemlerdeki kadar bariz bir etkilenme söz konusu değildir.
- Elbette ki bu yöntem gözü olmayan, gözleri görmeyen, Nistagmus hastalığına sahip (gözleri titreyen) veya irisleri olmayan kişilerde uygulanamaz. Ancak bu kişiler dışında havaalanı gibi kimlik doğrulamanın mutlak surette önemli olduğu yerlerde oldukça yüksek bir doğruluk oranı ile uygulanabilmektedir.

Biyometrik Sistem Çeşitleri - İris

- Genel olarak parmakizi tanımaya benzetilen bu sistemin, parmakizine göre en önemli avantajı, parmak izi kullanılan biyometrik sistemlerde 60 veya 70 karşılaştırma noktası bulunurken, iris taramada karşılaştırma için yaklaşık 200 referans noktası kullanılmasıdır.

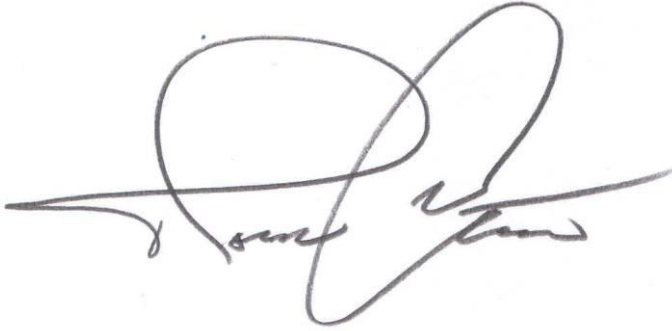
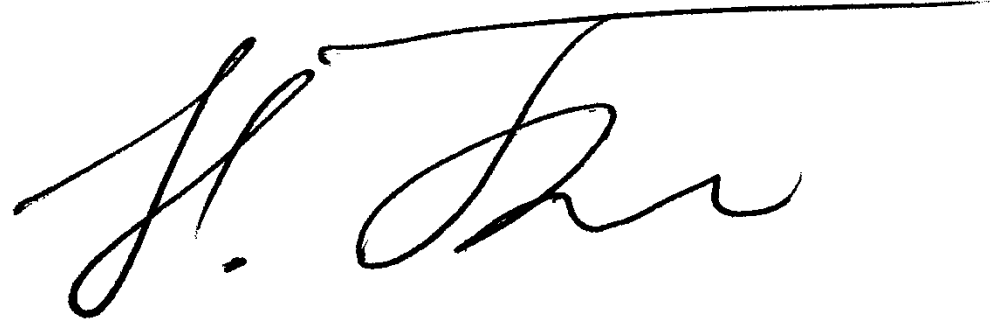


Biyometrik Sistem Çeşitleri - İmza

- Bir kişinin, herhangi bir yazının altına sözkonusu bu yazıyı yazdığını, okuduğunu veya onayladığını belirtmek için her zaman aynı biçimde yazdığı ad veya işaretler olarak tanımlanabilen imza kişiler tarafından yaşamları boyunca pek çok kez kullanılmaktadır. Özellikle hukuksal açıdan büyük yaptırımlarının bulunması ve taklit edilmesi sonucunda kişiyi borç altına sokabilmesi, tüm malvarlığını başka bir kimseye bağışlamasına sebep olması, işlemediği suçların üzerine kalmasına neden olması gibi sebeplerle hayati önem taşımaktadır.
- Dolayısıyla kimlik doğrulamasında belki de en sık kullanılan yöntem olan imzanın gerçekten o kişi tarafından atılıp atılmadığının belirlenmesi önemli bir sorun olarak karşımıza çıkmaktadır. Bu sebeple kullanılan imza tanıma sistemlerinde imzayı tanımak için iki tip bilgi kullanılmaktadır. Bunlardan ilki imzalama süresi, hızı, ivmesi, kalemin basım şiddeti, kalemin gibi kişinin imzalama işlemi ile ilgili özellikler, diğeri ise bir desen olarak imzaya ait özelliklerdir. Bir imzayı taklit eden herhangi bir kişi desen olarak imzayı taklit edebilse bile imza atış şeklini (süre, ivme, kalemi yerden kaldırma miktarı vs) tekrarlaması güçtür.

Biyometrik Sistem Çeşitleri - İmza

- İmza tanıma sistemlerinin dezavantajları, sistemin kullanıcının hızını, imza atma davranışını vs öğrenebilmesi için uygun sayıda örneğe ihtiyaç duyması ve imza atımının kullanıcının o anki ruh haline, özellikle de acelesi olup olmadığına bağlı olarak değişmesidir.

A handwritten signature in cursive script, featuring a large, looping initial 'D' and a long, sweeping horizontal stroke at the end.A handwritten signature in cursive script, featuring a large, looping initial 'J' and a long, sweeping horizontal stroke at the end.A handwritten signature in cursive script, featuring a large, looping initial 'D' and a long, sweeping horizontal stroke at the end.A handwritten signature in cursive script, featuring a large, looping initial 'J' and a long, sweeping horizontal stroke at the end.

Biyometri Tabanlı Yöntemler ile Diğer Yöntemlerin Karşılaştırılması

- Kullanıcı kimliğini belirleyen diğer sistemler (bilgi temelli ya da aidiyet temelli) ile biyometrik sistemler benzer yönlerle sahip olmakla beraber birbirlerinden ayrıldıkları noktalar da oldukça çoktur.
- Biyometrik yöntemler dışındaki yöntemlerin biyometrik yöntemlere göre en önemli dezavantajı kullanıcıya bazı bilgileri bilme ve hatırında tutma ya da bazı araçları sürekli olarak yanında taşıma, çaldırmama, unutmama gibi sorumluluklar vermesidir.
- Biyometrik sistemlerde böyle bir durum söz konusu değildir ve kişinin kimliğini doğrulayabilmek için kendisinden başka herhangi bir bilgiye, nesneye vs ihtiyacı yoktur. Biyometrik sistemlerin diğer sistemlere göre avantajları, dezavantajları, benzer ve farklı yönleri kısaca aşağıdaki gibi ifade edilir.

Biyometri Tabanlı Yöntemler ile Diğer Yöntemlerin Karşılaştırılması

- Diğer kimlik doğrulama yöntemlerinde kullanılan veri her kullanıcı için kesinlikle farklı ve eşsiz iken biyometrik veriler farklı olmakla beraber benzerliklere sahip olabilir.
- Diğer yöntemlerde kullanılan veri, kullanıcı tarafından değiştirilebilir (sistem yöneticisinin isteği üzerine, güncelleme amacıyla veya başka herhangi bir sebepten ötürü). Buna karşın biyometrik veri kişinin istemesi ile değiştirebileceği bir veri değildir, ancak kaza, hastalık vs geçirilmesi durumunda değişir.

Biyometri Tabanlı Yöntemler ile Diğer Yöntemlerin Karşılaştırılması

- Biyometrik sistemler genelde ek bir donanım, yazılım gerektirdiğinden ek bir maliyet getirir iken diğer yöntemler genelde kullanılan mevcut sistemlerle uyumludur. Diğer yöntemler çalındığı veya benzeri bir duruma uğradığı zaman yenisi ile değiştirilebilir, oysa ki biyometrik veriler herhangi bir şekilde elde edildiğinde, geçerliliği kalmaz.

Biyometri Tabanlı Yöntemler ile Diğer Yöntemlerin Karşılaştırılması

- Biyometrik veriler zaman içerisinde deformasyona uğrayabilir, buna karşın diğer yöntemler için böyle bir durum söz konusu değildir.

Biyometri Tabanlı Yöntemler ile Diğer Yöntemlerin Karşılaştırılması

- Biyometrik sistemler dışındaki tanıma sistemlerinde verinin unutulması, çalınması, kaybedilmesi riski oldukça fazladır. Ancak biyometrik sistemlerde kullanılan veri kişinin fiziksel ya da davranışsal bir özelliği olduğundan bu tarz bir tehlike ile karşı karşıya kalma ihtimali yok denecek kadar azdır.

SONUÇ

- Burada kağıt üzerinde yapılan pek çok işlemin dijital ortama geçirilmesi sonucunda bir gereksinim olarak ortaya çıkan dijital kimlik doğrulama yöntemlerinden biri olan biyometrik güvenlik yöntemleri incelenmiştir.
- Kişinin şifresini kendi üzerinde taşıması olarak ifade edebileceğimiz biyometrik güvenlik sistemleri, gerçek anlamda sosyal hayatta kısa bir zaman öncesinde kullanılmaya başlanmasına rağmen, her geçen gün daha fazla yerde kendini göstermektedir. Kişilerin parmak izi, iris, yüz gibi fiziksel sabit özellikler veya imza atış şekli, yürüme şekli gibi davranışsal özelliklerin herhangi birisini kullanan sistemler günümüzde oldukça rağbet görmektedir.

SONUÇ

- Kullanılan her güvenlik sisteminde olduğu gibi, biyometrik tabanlı güvenlik sistemlerinde de sistemin kullandığı herhangi bir yazılıma ya da donanıma yapılabilecek saldırılar mevcuttur. Biyometrik verileri algılayan cihazlara yapılan saldırılar olduğu gibi, biyometrik verileri taklit etmeye yönelik saldırılar da bulunmaktadır.
- Ayrıca iletişim kanalı saldırıları ya da man-in-the-middle saldırılar olarak adlandırılan ve kullanılan sisteme gizlice girip bilgi elde eden ve hatta bu bilgileri değiştiren saldırılar da biyometrik sistemler için birer tehdit unsurudur.

SONUÇ

- Bu saldırılardan korunabilmek kimlik doğrulama sağlayan sözkonusu biyometri sistemlerinde hayatî bir öneme sahiptir. Bu yüzden 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, şirket çalışanlarının şirkete giriş çıkışlarında ve bilgisayar gibi aletlerin kullanıcıyı tanıması sırasında kullanılan sistemlerin gelecekte kullanılması beklenen potansiyel kullanım alanlarından bazıları şu şekilde ifade edilebilir :

SONUÇ

- Turizm: Yolcuların araçlar için bilet satın alma, otel odası rezervasyonu yaptırma ya da araç kiralama gibi çeşitli turizm hizmetlerinde kullanabilecekleri biyometrik sistemlerin tasarlanması yapılacak işleri oldukça kolaylaştıracaktır.
- İnternet: Bilgisayarlara biyometrik bir okuyucunun entegre edilmesi ve bu sayede internetten yapılabilecek bankacılık işlemleri, resmî işlemler, pasaport vs başvuruları gibi dijital işlemlerin biyometrik kimlik doğrulama sayesinde yapılabilmesi işlemi oldukça ön plana çıkmaktadır.

SONUÇ

- Telefon: Bu yöntemde internette olduğu gibi telefon cihazlarına entegre edilecek bir aygıt ile kişinin telefon üzerinden alışveriş vs işlemlerini gerçekleştirilmesi amaçlanmaktadır. Ancak, telefon cihazının, hatlarının ve kullanıcı ortamlarının sabit olmayışı bu yöntemi zor kılar.
- ATM: Pek çok kullanıcısı olan ve bu kullanıcıların sıklıkla işlem yaptığı bankalarda sahteciliğin boyutları göz önüne alındığında bankaların bu sorunu biyometri teknolojisi kullanarak çözme çabası uygun bir çözüm olarak görünmektedir.

SONUÇ

- Biyometrik güvenlik sistemleri, genelde ek maliyet getirmeleri, kullanımlarının bazen uzmanlık gerektirmesi, ele geçirildiği anda yenilenme şansı olmamasından dolayı geçerliliğinin kalmaması gibi dezavantajlarının yanında kişinin kendisi dışında ek bir bilgi, 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.