AKILLI KİMLİK KARTLARININ FİNANSAL İŞLEMLERDE KULLANIMI: OLASI GÜVENLİK TEHDİTLERİ VE ALINACAK ÖNLEMLER

Eyüp Burak CEYHAN*
Bartın Üniversitesi, MF, *(eyupburak@gmail.com)*

İsmail Fatih CEYHAN
Bartın Üniversitesi, İİBF, *(ismailc@bartin.edu.tr)*

Ebru DEMİRYÜREK
Danıştay Başkanlığı, *(ebru_demiryurek@hotmail.com)*

Rümeysa BODUR
Imperial College London, *(rumeysa.bodur@gmail.com)*

ÖZET

Akıllı kartlar başta bilgisayar teknolojileri olmak üzere farklı teknolojilerin gelişmesiyle birlikte yaygın olarak kullanılmaya başlanmıştır. İnsanların farklı işler için kullandığı, yanında taşıması gereken banka kartları, kimlik kartları gibi birçok kart tek bir taşınabilir kartta birleşmiştir. Bu kartlar birçok açıdan kullanışlı olsa da güvenlik açığı olması durumunda kötü niyetli kişilerin saldırılarına maruz kalabilmektedir. Bu çalışmada akıllı kart sistemlerinde bulunan güvenlik açıkları ve meydana gelebilecek saldırı çeşitleri, akıllı kart sistemlerinde dikkat edilmesi gereken hususlar ve akıllı kartların finansal işlemlerde kullanımı açıklanmıştır. Ayrıca akıllı kart sistemlerinde görülen güvenlik sorunlarının çözümleri ve saldırılara karşı alınabilecek önlemler ile ilgili bir yazın taraması yapılmıştır. Yakın gelecekte Türkiye'deki tüm vatandaşların kullanımına sunulacak olan akıllı kimlik kartlarının güvenliğinin sağlanması için önerilerde bulunulmuştur.

Anahtar Kelimeler: *Akıllı Kimlik Kartı, Bankacılık, Güvenlik Açığı, Güvenlik Önlemi.*

USE OF SMART ID CARDS IN BANKING: POSSIBLE SECURITY THREATS AND MEASURES TO BE TAKEN

ABSTRACT

Smart cards have begun to be widely used along with the development of different technologies, especially computer technology. Multiple cards like bankcards, ID cards which are used by people for several purposes and should be carried along have been integrated in a single portable card. Although these cards are useful in many ways, in case of vulnerabilities they can be under attack. Security vulnerabilities and possible attack types that may be occur in smart card systems, issues to be considered in smart card systems and using smart cards in financial transactions were explained in this study. In addition, a literature review was made on the solutions of security problems in smart card systems and the measures that could be taken against the attacks. Recommendations were made to ensure the security of smart identity cards which will be available to all citizens in Turkey in the near future.

Keywords: *Smart ID Card, Banking, Security Vulnerability, Security Precaution.*

* *Sorumlu Yazar.*

www.ijmeb.org ISSN:2147-9208 E-ISSN:2147-9194
http://dx.doi.org/10.17130/ijmeb.2018343121
Başvuru Tarihi: 27.04.2018, Yayına Kabul Tarihi: 18.07.2018

1. Giriş

Akıllı kartların 1974'te Fransız gazeteci Roland Moréno tarafından bulunduğu kabul edilir. Bununla beraber, Almanya'dan Jargen Dethloff 1969 ve Japonya'daki Arimura Technology Institute'den Kunitaka 1970'de ilk patentleri almışlardır. Akıllı kartlar, farklı işlemler için kullanılan çok sayıdaki kartın yazılım olarak tek bir kartta toplanmasını sağlamıştır. Bu kapsamda günümüzde giriş kontrolü, elektronik ticaret, kimlik doğrulama, kişisel gizlilik gerektiren birçok uygulamada çok yaygın olarak kullanılmaya başlanmıştır. Ülkemizde en yaygın olarak kullanılan akıllı kart uygulamaları; elektronik bilet, kredi kartı, sağlıkla ilgili kayıtlar ve sürücü belgesi uygulamalarıdır (Karakülah vd., 2004). Bu kartlar, işlevselliği ile kişinin yanında fazla kart taşıma sorununa bir çözüm sunmuştur (Özbey, 2006).

Akıllı kartların hayatımızı kolaylaştırdığı ve pek çok soruna çözüm sunduğu yadsınamaz bir gerçek olsa da, bu kartlar pek çok tehlikeyi ve riski de beraberinde getirmektedir. Kartlara sonradan yüklenebilen yazılımlar çok büyük esneklik sağlamakta, ancak bazı güvenlik tehditlerini de doğurabilmektedir. Kötü amaçlı yazılımlar kartların üzerindeki önemli veriyi bozabilir, değiştirebilir, hassas verinin çalınmasına veya kart üzerindeki diğer uygulamaların hatalı çalışmasına neden olabilir (İnan, 2012).

Akıllı kartlarda, biyometrik özelliklerin kullanımı da mümkündür. Biyometri, insanların fizyolojik ve/veya davranışsal özelliklerine göre otomatik tanınması anlamına gelmektedir. Geleneksel şifreler, büyük ya da küçük harf, sayı ve sembollerin farklı kombinasyonlarından oluşan, genellikle uzun yapılardır. Bununla birlikte söz konusu zihin yorucu özelliklerinin yanında bu tür şifrelerin sıklıkla değiştirilmeyi gerektirmesi yaygın kullanıcı memnuniyetsizliklerine neden olmaktadır. Biyometrik teknolojiler bu tür sorunlar için çözüm üretebilmektedir. (Biometrics, 2004). 21. yüzyılda birçok devlet; ulusal kimlik kartları, sosyal güvenlik kartları, e-pasaportlar, ehliyetler, vb. güvenlik riski yüksek belgeler için biyometrik teknolojileri kullanmaktadır. Biyometrik sistemler aynı zamanda uluslararası terörizm, suç önleme, uyuşturucu kaçakçılığı, kimlik hırsızlığı, bilgisayar ve internet suçları, sınır denetimi, yasadışı göç ve dolandırıcılık gibi sorunların çözümüne yardımcı olmaktadır (Jain vd., 2004). 11 Eylül 2001'de gerçekleşen terör saldırıları sonrasında dünya çapında pek çok ülke, pasaportlarda biyometrik teknolojilerin kullanımı amacıyla gerekli yazılımların üretimine başlamıştır (Gerrit, 2004).

Türkiye'de 14 Mart 2016'da başvuru işlemleri başlatılan akıllı kimlik kartlarının, ilk olarak pilot şehir seçilen Kırıkkale'de dağıtımına başlanması ve akıllı kimlik kartı kullanımının üç yıl içinde ülke geneline yayılması hedeflenmiştir. Proje, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü tarafından yürütülmüş; projede Türk mühendisleri tarafından geliştirilen uygulama ve sistemlerden yararlanılmıştır. Kartlar aynı zamanda seyahat belgesi ve e-imza yerine de kullanılabilecektir (Haber7, 2016; EKDS, 2015).

TÜBİTAK tarafından geliştirilen çipli kimlik kartlarının şifreleme mekanizması ve işletim sistemi olan AKİS'in (Akıllı kart işletim sistemi), taklit, tahrif ve sahtecilik kaynaklı güvenlik risklerini önemli ölçüde azaltması beklenmektedir Biyometrik veri olarak parmak, damar ve el ayası izi kullanılan bu kartların depolama hafızası 1GB'dir. Bahsi geçen veriler şifrelenmiş sayısal karakterler olarak yalnızca veri merkezinde tutulacak ve kart yönetim

sisteminde saklanmayacaktır. Bu veriler oldukça kişisel bilgilerdir ve Türkiye mevzuatında kişisel verilerin korunmasına dair yasa 24 Mart 2016 tarihinde kabul edilmiştir. Ayrıca, Türkiye Cumhuriyeti Anayasası'nın "Özel Hayatın Gizliliği" başlıklı 20 maddesinde de bu duruma değinilmektedir (EKDS, 2015; Ajanshaber, 2015; Resmi Gazete, 2016).

TÜBİTAK tarafından geliştirilen söz konusu sistemde; verilerin alındığı, iletildiği ve işlendiği ağın altyapısı kapalı devre olması ve herhangi açık bir ağa bağlantısı bulunmaması planlanmaktadır Ayrıca çalışmalar kapsamında biyometrik verileri barındırmak için inşa edilen Kişiselleştirme Merkezi Binası, uluslararası askeri standart olan Tempest NATO Zone 2 standartlarına göre inşa edilmiştir ve dış cephesi metal alaşım ile kaplanmıştır. Bunun yanısıra metal filmle kaplanan ve filtrelerle koruma altına alınan kablo ve borular da güvenliği artırmak amacıyla yapılmıştır. Ayrıca, manyetik veri yaymaya karşı izole etmeyi sağlayan Faraday Kafesi de oluşturularak binada elektromanyetik izolasyon sağlanmıştır (EKDS, 2015).

Akıllı kartlardaki güvenlik açıklarından kaynaklanan sorunlar genellikle yargıya intikal etmektedir. Bu sorunun temel kaynaklarından biri de tüm vatandaşlara ait bilgilerin tek bir merkezi biyometrik veri tabanında tutulmasıdır (Roy, 2015).

Fransa'da yapılan bir araştırmanın (Leparisien, 2011) sonuçlarına göre; gerek yeni kimlik arayışında olan suçlular ve gerekse yasadışı göçmenler tarafından biyometrik kimlikler kullanılarak çok sayıda yasa dışı işlem yapıldığı görülmüştür. Ayrıca biyometrik sistemlerin %100 başarı garanti etmemesi sebebiyle de sorunlar yaşanabilmektedir. Bunun bir örneği, 2004 yılında İspanya'nın Madrid şehrinde bombalı terör saldırısında şüpheli çanta üzerinde parmak izinin bulunması sebebiyle tutuklanan ve daha sonra hata yapıldığı fark edilip tazminat teklifiyle serbest bırakılan Brandon Mayfield'in davasıdır. Bu tür olayların başka örnekleri dünya genelinde mevcuttur (Roy, 2015).

En tehlikeli güvenlik problemleri arasında, biyometrik verinin saklandığı veritabanlarına erişim sağlanıp bilgilerin çalınması ve kamuoyu ile paylaşılması yer almaktadır. Örneğin, 2006 yılında İsrail'de 9 milyon kişinin kimlik bilgileri çalınmıştır. Bu tür olaylar beklenmedik felaketlere yol açabilmektedir. Zira teröristlerce yapılan saldırılar veya rehin alma olaylarını gerçekleştirmek için, böylesi bir durum büyük bir fırsat doğuracaktır (Roy, 2015).

Akıllı kartlar ve güvenliği konusunda kapsamlı bir araştırma yapılan bu çalışmanın, ikinci bölümünde akıllı kartlar ve akıllı kart sistemlerinde dikkat edilmesi gereken hususlar belirtilmiş, üçüncü bölümünde bu kartlardaki güvenlik açıkları ve bu açıklar kullanılarak yapılabilecek saldırılar detaylandırılmış, dördüncü bölümde akıllı kartların finansal işlemlerde kullanımı ile ilgili örnekler verilmiş ve beşinci bölümde akıllı kart sistemleri ve güvenliği ile ilgili görüş ve öneriler sunulmuştur.

2. Akıllı Kartlarda Dikkat Edilmesi Gereken Hususlar

Akıllı kartlar, kredi kartı boyutlarında üretilen ve içerisinde işlemci, RAM ve ROM belleği bulunan gömülü bir mikroçipe sahip donanımlardır. Üzerinde manyetik şerit, barkod, temassız radyo frekans vericileri gibi farklı teknolojileri bulundurabilmektedir. Akıllı kartlar; kimlik teşhisi ve denetimi, veri depolama ve çeşitli uygulama hizmetlerinde kullanılabilirler (Ko & Caytiles, 2011).

Akıllı kimlik kartlarında öncelikli olarak alınması gereken önlemler şunlardır (Başak & Bıyıklıoğlu, 2008; Roy, 2015; Xiao & Savastano, 2007):

- Veriler yalnızca açıkça belirtilen meşru bir amaç için ve mutlaka toplanması gerektiği için toplanmalıdır.
- Şahsa ait veriler kişinin rızası dâhilinde alınmalıdır ve bu sırada daha önce belirlenen amaç kişiye açıkça belirtilmelidir.
- Devlet organları ile kişi ve kuruluşlar arasında yapılacak veri transferine kısıtlamalar getirilmelidir.
- Verilerin güvenliği ve gizliliği, alınacak uygun önlemlerle sağlanmalıdır ve kişiler kendi verilerine erişim hakkına sahip olmalı ve gerektiğinde yanlış/eksik verileri düzeltebilmelidir.
- Güvenlik açısından önemli olan verilere toplama sınaması konularak verinin bütünlüğü denetlenmelidir. Herhangi bir olumsuz durumla karşılaşıldığında kart kendini korumaya almalıdır.
- Algoritmaların işlem süreleri sabitlenerek yan kanal analizleri ve zamanlama analizleri ile gizli bilginin açığa çıkarılması önlenmelidir.
- Kritik işlemlere çift kontrol yapısı uygulanıp, sonuçlar karşılaştırılarak hata olmasının önüne geçilmelidir.
- Akıllı kartlarda yonga yüzeyinden değerli verileri okumayı engellemek için etkin kalkan adlı bir mekanizma kullanılmalıdır. Bu mekanizmada yonga yüzeyinde rastgele dizilmiş ince veri yolları bulunmaktadır. Bu mekanizmayla değişken verilerin doğruluğu sağlanmaktadır. Bu yüzeyin aşınması durumunda verilerde hata meydana gelebileceğinden yonga kendini güvene almaktadır.
- Güvenlik açısından akıllı kartlardaki önemli verilerin kopyaları birden fazla formda tutularak verinin değiştirilmesi engellenmelidir.
- Akıllı kart yongalarında, yonganın yüzeyinin kazılarak analiz edilmesini önlemek için önemli bloklar yongaya rastgele yerleştirilmelidir. Ayrıca mikroişlemcinin lazerle kesilmesi gibi saldırılara karşı yonganın üzerine ikinci bir metal tabaka konularak yonganın özelliklerine ulaşılması engellenebilmektedir.

Her ne kadar sahteciliğin tamamen önlenmesi imkânsız olsa da bu riskler, tehditler analiz edilip doğru bir tespit mekanizması ve uygun bir caydırma yöntemi kullanılarak azaltılabilir. Bir bireye ait yeni kaydedilen biyometrik verilerin, halihazırda kaydedilmiş olanlarla eşleştirilmesi işlemi her zaman tümüyle güvenli bir süreç dâhilinde yürütülemeyebilmektedir. Söz konusu risklerin azaltılabilmesi için yanlış eşleştirmelerin dağılımının ve eşleşme mekanizmasının modellenmesi gerekmektedir. Bu sürecin ardından modelin analizi yapılmalı, yanlış verileri engelleyecek yöntemler geliştirilmelidir. (House of Commons Science and Technology Committee, 2006).

2.1. Şifre Kullanımı

İlk akıllı kart uygulamaları basit kimlik kart özelliğindedir. Kart üzerinde kart sahibinin adı ve kart numarası gibi kişisel bilgileri kabartma ile basılmıştır. Taklide karşı koruma

baskıdaki incelikler ile sağlanmaktadır. Günümüzde kart kullanımının artmasıyla alınan önlemler saldırılara karşı yetersiz kalmaktadır (Wrankl, 2016).

Kartın arkasına manyetik bir şerit eklenerek ek bilgiler de karta yüklenmiştir. Karta eklenen bu özellik ile birlikte güvenlik için yeni bir kimlik doğrulama yöntemi ortaya çıkmıştır. Kart kullanıcıları işlem yapmak için kişisel kimlik numarası (PIN) şifrelerini girerek sisteme giriş yapmaktadır. Yüksek güvenlik gerektiren verilere erişim için gereken kişisel kimlik numarası ve kişisel kilit açma anahtarına (PIN ve PUK) uzunluk sınırlaması getirilerek deneme yanılma yöntemiyle tahminleri güçleştirilir. Doğum tarihi, ad, okul ve çocuk adları gibi herkesin tahmin edebileceği basit ifadeler şifrelerde kullanılmamalıdır (Başak & Bıyıklıoğlu, 2008).

2.2. Şifreleme

Şifreleme, verinin güvenliğini sağlamak için kullanılan bir yöntemdir. Bu yöntem her ne kadar donanımlı saldırganlara karşı etkisiz olsa da, en azından kart okuyucuya sahip sıradan bir insanın, kart içerisindeki verilere erişimini önlemiş olacaktır (Gerrit, 2004). Blok şifreleme yöntemini kullanan veri şifreleme standardı algoritması (DES), verileri bir anahtar yardımıyla metin uzunlukları belli olan bloklar halinde şifrelemektedir (İTÜ, 2013). DES algoritmasının zayıflığından dolayı yerine DES şifrelemesinin 3 kere art arda yapılması şeklinde çalışan üçlü veri şifreleme standardı algoritmasının (3DES) kullanılması önerilir (Başak & Bıyıklıoğlu, 2008).

2.3. Biyometrik Tanımlama Sistemi

Kişinin fiziksel ve davranışsal karakteristiklerini tanımlayarak kimlik saptamak için geliştirilmiş otomatik sistemlerdir. Kimlik saptama bireyin özellikleri ile yapıldığı için, şifreli sistemlerde yaşanan kaybetme ve unutma gibi problemlerle karşılaşılmaz. Biyometrik sistemler, kişinin belirli biyolojik karakteristiklerini benzersiz bir koda dönüştürmektedir. Kimlik saptamasında, kişinin anlık gelen özellikleriyle o kişinin daha önce veritabanına kaydedilmiş olan biyometrik özellikleri karşılaştırılır ve kimliğin doğruluğu tespit edilir (Oranlı, 2007).

Biyometrik sistem genel bir kimlik kartının amaçlarına uygun olmalıdır. Sistemde hata oranı %1'i aşmaması gerektiğinden, biyometrik özellik evrensel olmalıdır. Ayrıca veri koruma yasasına göre orantılılık testinden geçirilmelidir. Orantılılık prensiplerine göre kişiye ait biyometrik veriler gerekenden fazla olmamalıdır, bir ortama kalıcı şekilde aktarılmamalıdır ve kişinin rızası dâhilinde alınmalıdır (Gerrit, 2004).

Biyometrik sistemler, doğrulama ve teşhis gibi iki farklı modda çalışmaktadır. Doğrulamada, yeni gelen sorgu talep edilen kimlik şablonlarına uyuyor ve yeterince benziyorsa, kimlik gerçek (doğru) olarak kabul edilmektedir. Teşhiste ise, yeni gelen sorgu veritabanına kayıtlı tüm kullanıcıların bilgileriyle karşılaştırılmaktadır. Sorgu sonucu hangi kullanıcı şablonu en çok benzerlik gösteriyorsa aranan kullanıcı bulunmuş olmaktadır (Nandakumar vd., 2009).

Akıllı kimlik kartlarında yaygın olarak kullanılan biyometrik tanımlayıcılar parmak izi, iris ve yüz verileridir (Gerrit, 2004). Parmak izi verisi diğer fiziksel özelliklere nazaran en güvenilir özelliktir (Jain vd., 1997; Best, 2013). Her birey farklı parmak izine sahiptir ve parmak izleri zamanla değişmez. Parmak izi, kolay erişilebilir ve sistematik bir biçimde sınıflandırılabilir

olmasından dolayı biyometrik sistemlerde yaygın olarak kullanılmaktadır. (Karakülah vd., 2004). Parmak izi tanıma sistemleri; sistem performansı, kullanım kolaylığı, güvenilirliği ve maliyeti nedeniyle, en yaygın olarak kullanılan biyometrik yöntemdir. (Ayyanna, 2007; Sağıroğlu & Özkaya, 2006; Koteswara vd., 2014). Genellikle kampüs, yemekhane ve yurt giriş çıkış kontrollerinde kullanılmaktadır. Parmak izi tanıma giriş çıkış kontrollerinde güvenliği artırsa da, kişi tarafından gün içinde pek çok nesneye dokunulduğundan dolayı, parmak izi buralarda istemsizce bırakılmaktadır. Bu durum ise kişiyi takip etmeyi ve bu parmak izini taklit ederek sistemlere giriş sağlamayı kolaylaştırmaktadır. Parmak izinin taklidi çok zordur fakat imkânsız değildir. Ayrıca bazı kişilerin deri hastalığına yakalanma ve yanma gibi sebeplerden dolayı parmak izi ayrıntılarının bulunmaması da sorun teşkil etmektedir (Gerrit, 2004).

Yüz verisi ile ilgili problem, kişinin izni ve haberi olmaksızın edinilip saklanılabilmesi ve hatta üzerinde değişiklik yapılabilmesidir. Sürekli görünür olduğu için yüz verisinin tercih edilmesi savunulsa da, bu durum verinin elde edilmesini kolaylaştırdığından aslında bir dezavantajdır (Gerrit, 2004).

İris verisi ise kişinin bilgisi olmadan edinilemeyeceğinden dolayı, yüz ve parmak izinin dezavantajını ortadan kaldırmaktadır. Ancak iris verisinden diyabet, hipertansiyon, aşırı alkol ve esrar kullanımı, homoseksüelite gibi sağlık sorunları ve özel veriler elde edilebilmekte ve bu durum ise kişi için bir dezavantaj oluşturabilmektedir (Gerrit, 2004).

Görüldüğü üzere biyometrik verilerin her çeşidinin kendine özel riskleri vardır. Ancak veri güvenliği açısından, iris verilerinin işlenmesine dayanan sistemlerin diğer sistemlere kıyasla daha üstün olduğu söylenebilir. Türkiye'deki akıllı kartlarda kullanılması planlanan biyometrik veriler arasında ise iris bulunmamaktadır (Haber7, 2016).

2.4. Merkezi Veritabanı

Güvenlik risklerini artıran temel konulardan biri de akıllı kartlarda gizlenen verilerin manyetik şeritler üzerinde saklanmasıdır. Gerekli aygıtlara erişimi olan herkes manyetik şerit üzerindeki veriyi okuyabilir, silebilir ya da değiştirebilir. Güvenli kullanım için, okuyucular doğrulama yaparken sürekli merkezle bağlantı kurmalıdır.

Biyometrik kartlar, verilerin merkezi veritabanları yerine yerel depolama birimlerinde saklanacak şekilde tasarlanmalıdır. Birçok ülkede ise verilerin saklanması hususunda merkezi biyometrik veritabanları tercih edilmektedir. Bunun amacı, kişilerin farklı isimlerle birden fazla kimlik edinmelerini engellemek içindir. Ancak merkezi bir veritabanında biyometrik verileri tutuyor olmak olası bir saldırı durumuna karşı büyük bir risk taşımaktadır. Bu sebeple merkezi veritabanı yerine verinin yalnızca kartlarda taşınması önerilse bile bu durum doğrulama işleminin yapılmasına engel teşkil edeceğinden uygulanmamıştır (UK Government Biometrics Working Group (BWG), 2003).

2.5. Özel Uygulamalarda Kullanım

Kimlik kartındaki biyometrik verilerin özel uygulamalarda kullanımı esasen hukuki açıdan sorun teşkil edecektir. Kimlik denetimi yapan kişilerin artması, yetkisiz kişilerin vatandaşların kimlik kartı kullanımını takip edebilmesi ve ifşa edebilmesi gibi durumlar kişisel verilerin mahremiyetini ihlal duurmunu ortaya çıkarabilir. Böyle bir durumda hukuki ve etik

problemler çıkabilmektedir. Çünkü bir kez kişinin verilerine erişim hakkı kazanan biri, kişi hakkında detaylı bilgilere erişebilir ve bu durum kişi için problem oluşturabilir. Ancak yine de zorunlu durumlarda, bu tür bir seçim yapılırken kullanıcıya karar verme fırsatı verilmesi daha uygun olacaktır (TÜBİTAK, 2006; Gerrit, 2004).

2.6. Yedekleme ve Güncelleme Prosedürü

Her biyometrik sistemde, herhangi bir sebepten dolayı hata oluşabileceği ve geçici ya da kalıcı bir süreliğine biyometrik verilere erişimin mümkün olamayabileceği göz önünde bulundurulmalıdır. Uygulanacak yedekleme prosedürleri gecikmeyi engelleyecek nitelikte olmalıdır. Ayrıca kart bileşenleri, kullanıcının bilgisi dışında ortaya çıkan etkenlerden dolayı da zarar görebileceğinden, kart gövdesi sahteciliğe karşı güvenli olmalı ve çipsiz kullanımı mümkün olmalıdır (Gerrit, 2004). Kişilerin biyolojik özelliklerinin zamanla değişmesi sebebiyle biyometrik veri kaydının belirli aralıklarla güncellenmesi de gerekmektedir. Ayrıca vatandaşların kartlarında bulunan evlilik durumu, askerlik, sabıka kaydı gibi verilerin de güncel tutulması gerekmektedir. Bu sebeple, en azından her beş yılda bir kimlik kartı sahibinin kayıtlarının güncellenmesi tavsiye edilmektedir (TÜBİTAK, 2006).

2.7. Donanımsal Anomali Sensör Kullanımı

Akıllı kartlarda anormal durumları sezmek için çok sayıda donanımsal anomali sensörü yer almaktadır. Bu sensörler karta uygulanan gerilim, saat işareti, sıcaklık ve ışık gibi etmenlerin tanımlı alt ve üst limitlerin dışında olduğu anormal bir durum sezdiğinde, kart yongası bu durum ortadan kalkana kadar çalışmasını keserek kendini güvenli duruma alır. Buna reset durumu denmektedir. Bu sensörler sayesinde ultraviyole ışığı kullanarak, elektriksel silinebilir ve programlanabilir salt okunur bellek anlamına gelen EEPROM'un silinmesi ve saat işaretinin kesilmesi gibi saldırılara karşı koruma sağlanmış olur (Xiao & Savastano, 2007).

3. Akıllı Kartlarda Güvenlik Açıkları ve Olası Saldırılar

Akıllı kartlarda bulunan güvenlik açıklarının iyi tespit edilmesi, kartların kullanımının doğuracağı tehditleri ortadan kaldırmak için alınacak önlemlerin belirlenmesi açısından önem arz etmektedir. Çalışmanın bu bölümünde, akıllı kartlarda mevcut bazı güvenlik açıklarından bahsedilmiş, bu kartlara düzenlenebilecek bazı olası saldırılar üzerinde durulmuştur.

Akıllı kartlarda güvenlik dört bileşen ile sağlanmaktadır. Bunlardan ilki fiziksel olarak kartın kendisidir. Diğer bileşenler yonga, işletim sistemi ve kart üzerindeki uygulamalardır. Bir akıllı kartın güvenli olması için bütün bileşenlerin güvenilirliğinin sağlanması gerekir. Aşağıda akıllı kart uygulamalarında sık karşılaşılan güvenlik problemleri maddeler halinde sıralanmıştır. Bu maddeler göz önünde bulundurularak güvenlik ile ilgili önlemler alınmalıdır (Başak & Bıyıklıoğlu, 2008):

- Yonga modülünün temas noktalarına tel iliştirilerek okuyucu ve kart arasındaki veri istenilen şekilde değiştirilebilmektedir.
- Ultraviyole ışığı kullanarak EEPROM silinebilmekte, kartın güvenli durumu bozulabilmektedir.
- Akıllı kartın PIN kontrolü sırasında hata sayacı sıfırlanabilmektedir.

- Saat işareti kesilip elektron ışın test edici ile rasgele erişilebilir hafızanın (RAM) içeriği gözlenebilmektedir.
- Mikroişlemcinin üst tabakaları lazerle kesilerek içyapısı bozulabilmektedir.
- Kriptografik algoritmalarda anahtara bağlı olarak işlem süresi değişebilmektedir. Bu değişimden yararlanarak anahtarlar ortaya çıkabilmektedir.
- Süper bilgisayar kullanılarak deneme yanılma yöntemiyle DES anahtarları ele geçirilebilmektedir.
- Belli mekanizmalar kullanılarak kart işlemcisine hata yaptırılabilmekte ve gerilimdeki değişimler işlemcinin komutları atlamasına ya da yanlış yorumlanmasına sebep olabilmektedir.
- Saat işaretindeki değişimler verinin yanlış okunmasına sebep olabilmektedir.
- Sıcaklıktaki değişimler işlemcide tutarsız davranışlara yol açabilir. İşlemciye yöneltilen lazer ışığı ya da beyaz ışık, devrelerini bozabilmektedir.
- Elektromanyetik değişimler RAM'deki verilerin değişmesine sebep olabilmektedir.
- Kart çalışırken karttan sızan bilgileri inceleyerek, yapılan işlemleri ve gizli verileri açığa çıkarmaya yönelik saldırılar da mevcuttur.

Tablo 1'de akıllı kartların güvenliğine ilişkin yürütülen yazın taramasının bir özeti sunulmuştur.

Tablo 1: Akıllı Kartların Güvenliğine İlişkin Yazın Taraması

Kaynak	Amaç	Sunulan Çözüm
Başak & Bıyıklıoğlu, 2008	Veri Gizliliği	DES algoritmasının yerine 3DES şifreleme algoritmasının kullanılması
UK Government Biometrics Working Group (BWG), 2003	Biyometrik verilerin güvenli depolanması	Verilerin yalnızca kartta ya da yerel merkezlerde depolanması
Biometrics, 2005	Veriye erişimin engellenmesi	Şifrelemenin kullanılması
Gerrit, 2004	Biyometrik tanımlama sisteminin belirlenmesi	Diğer türlere göre daha avantajlı olan iris verisinin kullanılması
Ko & Caytiles, 2011	Fiziksel saldırılara karşı çözüm bulunması	Koruyucu ve çoklu katman kullanımı, boyut küçültme, sensörler
House of Commons Science and Technology Committee, 2006	Güvenlik	Karşılaştırma mekanizmasının modellenmesi
Roy, 2015	Hatanın önlenmesi	Kritik işlemlere çift kontrol yapısı uygulanması
Biometrics, 2004	Akıllı kartlarda yonga yüzeyinden değerli verilerin okunmasının engellenmesi	Etkin kalkan adlı bir mekanizmanın kullanılması

3.1. Tersine Mühendislik

Tersine mühendislik, bir sistemin parçalarına ayrılarak çalışma prensibinin analiz edilmesini içerir. Bir saldırgan da bu şekilde kart üzerinde bulunan çipi gövdesinden ayırarak hafıza bileşenlerine erişebilir. Taramalı elektron mikroskoplar kullanılarak PIN'e, biyometrik verilere ve kişisel bilgilere ulaşılabilir. Ayrıca kart üzerindeki biyometrik şablona erişebilen saldırgan, fiziksel karakteristikle uyuşacak potansiyel görüntü setini azaltabilmektedir (Ko & Caytiles, 2011; Xiao & Savastano, 2007).

3.2. Güç Analizi

Bir yan kanal saldırı türü olan güç analizinde, saldırgan mikrodenetleyiciye fiziksel erişim sağlayarak, harici veri yolunu ve geçerli yoğunluğu kayıt altına alabilmektedir. Bu saldırı türü, cihazın güç tüketimindeki değişiklikleri analiz ederek bilgi edinebilmek amacıyla geliştirilmiştir. Kartlarda, yanlış ya da doğru şifre girildiğinde güç emisyon desenlerinde farklılık oluştuğu saptanmıştır. Bu durum ise kimlik kartlarında güvenliğin kırılmasına sebep olabilmektedir (Xiao & Savastano, 2007).

3.3. Gizli Tarama ve İzleme

Gizli tarama işlemi, kullanıcının rızası ve bilgisi dâhilinde olmadan kimlik kartı üzerindeki elektronik bilgilerin okunmasıdır. Bu durum ICAO'nun yalnızca temel standartlarına uyan, şifreleme kullanmayan pasaportlar için bir tehdit unsurudur. Çünkü kart okuyucuya sahip yankesiciler, teröristler veya adam kaçıranlar bu durumdan fayda sağlayacaklardır. Gizli izleme işlemi ise kart sahibinin hareketlerini takip etmeyi sağlar ve gizli taramaya kıyasla kolaydır. Çünkü sadece çip numarasını okuyabilmek yeterlidir (Xiao & Savastano, 2007).

3.4. Gizli Dinleme

Saldırgan veriyi karttan doğrudan okumak yerine, yetkisiz bir cihaz yardımıyla kart ile okuyucu arasındaki iletişimi dinleyebilir. Çünkü kart meşru bir okuyucu tarafından sorgulandığında da eşsiz bir tanımlayıcı yaymaktadır. Gizli dinleme saldırısı, akıllı kimlik kartlarının güvenliği hususunda en büyük tehdidi oluşturmaktadır. Bu durumun sebepleri arasında, saldırının tamamen pasif olması ve tespitinin imkânsız olması yer almaktadır. Bir diğer sebep ise gizli dinlemenin, gizli taramanın aksine, daha uzak bir mesafeden uygulanabilir olmasıdır. Ayrıca akıllı kimlik kartları seyahat belgesi gibi çeşitli amaçlarla kullanılacağından, farklı ortamlarda gizli dinleme işlemi yapılabilecek ve bu durum saldırganın zayıf nokta bulmasını kolaylaştıracaktır (Xiao & Savastano, 2007).

3.5. Sahtecilik

Biyometrik verilerde sıkça rastlanan sahtecilik olayı genel olarak iki kademede meydana gelmektedir. Bunların ilki kayıtlı şahsa ait biyometrik verinin elde edilmesi, ikincisi ise elde edilen veri üzerinde değişiklikler uygulanmasıdır. Yüz, parmak izi ve iris verileri her ne kadar güvenliğin sağlanması için kullanılsa da, bu verilerin saldırganlar tarafından kolay elde edilebilir olmaları sahteciliğin yolunu açmaktadır (UK Government Biometrics Working Group (BWG), 2003; Biometrics, 2005).

3.6. Diğer Fiziksel Hasarlar

Kimyasal çözücüler, aşındırıcı veya lekeleyici maddelerle karta fiziksel hasarlar verilebilir. Aşındırıcı maddelerle çipteki metal ve silikon katmanları eritilebilir. Lekeleme ise aşındırma hızında değişiklikler yapılan daha gelişmiş bir tekniktir. Bu teknikle ROM hafızalarındaki 1 ve 0'larda değişiklikler yapılabilmektedir (Ko & Caytiles, 2011).

4. Akıllı Kartların Finansal İşlemlerde Kullanımı

Finansal sistemin unsurlarından biri olan ve aracılık faaliyetinde bulunan bankalar tasarruf sahipleri ile yatırımcılar arasında köprü görevi üstlenen önemli kurumlardır. Bu kurumların piyasaya sunduğu finansal araçlar zamanla çeşitlenmiş ve gelişen teknolojinin de katkısıyla bu araçlar hemen herkesin ulaşabileceği kolaylığa erişmiştir. Yakın bir geçmişe kadar banka binasına gitmeyi gerektirecek bir işlem için artık internet ve bilgisayar yeterli olmaktadır. Finans alanındaki yenilikler bununla sınırlı kalmamakta, her geçen gün ortaya konan inovasyon sektörün gelişmesine katkı sağlamaktadır. Örneğin bazı bankalar mobil bankacılık uygulamalarına parmak izi ile girme imkânını sunmaktadırlar (Turkishtimedergi, 2015).

Bu bölümde akıllı kimlik kartlarının kullanım alanlarından biri olan bankacılık uygulamaları üzerinde durulmuştur. Bu uygulama henüz çok yeni olduğu için literatürde kısıtlı miktarda kaynak bulunmaktadır.

Son yıllarda kullanımı yaygınlaşan akıllı kimlik kartları, bir finansal inovasyon örneği olarak gösterilebilir. Örneğin Nijerya'da ulusal biyometrik kimlik kartları banka kartı gibi ATM'lerde ve marketlerde kullanılmaya başlamıştır. Bu kapsamda 167 milyon nüfusa sahip Nijerya'da pilot uygulama olarak 13 milyon kimlik kartı ile banka kartının birleştirilmesi planlanmıştır. Her bir Nijerya vatandaşının demografik ve biyometrik bilgilerini üzerinde yer alan mikroçipte barındıran kimlik kartları, banka kartlarıyla bağdaştırılmıştır. Bu kartlarla, sosyal yardımlar alınabilmekte, ürün ve hizmetler için ödeme yapılabilmekte, ATM'lerde para yatırma ve çekme işlemleri yapılabilmekte ve elektronik ödemelerin yapılabildiği diğer birçok finansal işlemlerde kullanılabilecektir. Kimlik kartları alışveriş merkezlerinde kullanıldığında kasiyerler müşterinin kimliğini hem fotoğraftan hem de çipte bulunan biyometrik bilgilerden doğrulayabilmektedirler. Pilot uygulama başarılı olursa ülkedeki 120 milyon kimlik kartı ile banka kartını birleştirmeyi planlanmaktadır. Fakat kimlik kartı ile banka kartının birleştirilmesinde bilgi güvenliği ile ilgili birçok çekince de bulunmaktadır. Bunlardan en önemlisi bankaların kişilerin ulusal çapta tüm bilgilerine ulaşabilmeleri ihtimalidir (Fastcompany, 2013; CNN, 2014). Dolayısıyla akıllı kimlik kartlarında güvenlik çok önemli bir faktör olarak karşımıza çıkmaktadır.

Akıllı kimlik kartlarıyla ilgili benzer bir uygulama Estonya'da da sunulmaktadır. Ulusal kimlik kartları elektronik ödemelerde kullanılabilmektedir. Estonya vatandaşlarına 15 yaşından itibaren kamu hizmetlerinden yararlanmak ve ticari işlemlerde kullanmak için, ihtiyaç duyulan tüm kişisel bilgilerini ihtiva eden mikroçipli kimlik kartları verilmektedir. Kimlik kartının kullanımı için banka işleminde olduğu gibi bir PIN gerekmektedir. Hükümetin yürüttüğü X-Road adlı dijital altyapıya bağlı ülkedeki bankalar, devlet ve özel firmaların veri tabanlarını devletin kontrolündeki bu altyapı ile birbirine bağlanmaktadır. Ayrıca sağlık kayıtlarını ve

vergi bilgilerini bu kartlarda dosyalama, akıllı telefonlardan hizmet siparişi ve oy kullanma gibi işlemlerde de akıllı kimlik kartları kullanılabilmektedir (Pymnts, 2014).

Anthes (2015) çalışmasında, e-yerleşimcilere kapılarını açtığı için gelecek 10 yıllık sürede Estonya nüfusunun dünya genelinde %600'dan fazla büyüyerek 1,3 milyondan 10 milyona yükseleceğini belirterek, 2015 yılında birçok ulusal elektronik hizmet ve veritabanlarına erişim için dijital kimlik kartları ve dijital imza başvurusunda bulunan e-yerleşimcilere sınırlarını açmıştır. Estonya dışındaki yatırımcıların Estonya'da yatırım yapabilmelerine, iş kurabilmelerine ve Avrupa Birliği'ndeki herhangi bir ülkeyle ticaret yaparken Estonya'yı köprü olarak kullanmaları için bu fikir uygulamaya alınmıştır. 15 yaşından itibaren tüm vatandaşlara verilen kimlik kartlarında yer alan dijital imza ile gayri safi yurtiçi hasılanın %2'si, yani Estonya için 500 milyon dolarlık bir kazanç sağlandığı belirtilmektedir (Anthes, 2015).

Estonya'nın uyguladığı X-Road altyapısında, kişiler kendi verilerini kontrol edebilmektedir. Örneğin bir kişi, elektronik sağlık kayıtlarına belirlediği bir ismin erişimini kısıtlayabilmekte, verilerine kimlerin eriştiği bilgilerini istediği zaman görebilmektedir. Bununla birlikte önemli bir güvenlik tehdidi de bulunmaktadır. Her şeyin kaydı internet üzerinde bulunduğundan dolayı, kişisel bilgilerin çalınması halinde hükümetin yapacak bir şeyi kalmayacaktır. Bu nedenle Estonya e-devlet hizmetini veritabanlarıyla birlikte, Estonya dışında kardeş ülkelerin veri elçiliklerinde bulut üzerine yayma fikri ortaya atılmıştır. Buna rağmen bu uygulamanın bu kardeş ülkelerin veri gizliliğini sağlayıp sağlayamayacağı konusunda tereddüt etmektedir (Anthes, 2015).

Estonya'nın akıllı kartlarda bankacılık ve diğer sektörler ile kamu sektöründeki verileri bir araya getirdiği X-Road altyapısının bir benzerini Finlandiya' da kurulmaya başlanmıştır. Hindistan'da 1,3 milyar vatandaştan alınan biyometrik veriler akıllı kimlik kartlarına yüklenerek kullanılmaya çalışılmış ancak İngiltere'de gizlilik haklarının ihlaline sebep olacağı düşünülerek iptal edilen buna benzer bir projede olduğu gibi, sonucu tartışılmaktadır (Anthes, 2015).

Avrupa'nın dijital geleceğini korumak için görevlendirilen Avrupa Komisyonu başkan yardımcısı Andrus Ansip, akıllı kartların e-hizmetlerde kullanılabilmesi için tüm kişisel bilgilerin ayrı sunucularda barındırıldığını ve devlet dairelerinin bağımsız güvenlik duvarlarının ardında tutulduğunu, sistemin devlet ve banka gibi işletmelerin veri paylaşımı yapabilmesine sadece "bireylerin rızası olursa" izin verdiğini söylemiştir. Bunun yanında bir diğer problem ise, aynı anda birçok kullanıcının sisteme giriş yapması nedeniyle, arıza meydana geldiğinde sistemde dağınıklığın ortaya çıkması ihtimalidir (Pymnts, 2014).

Eaton vd. (2018) yaptığı çalışmada, Danimarka, İsveç ve Norveç'teki devlet ve finans sektörünün birlikte çalışması sonucu ortaya çıkan ulusal elektronik kimlik kartının ülke genelindeki analizi sunulmaktadır. Çalışmada finansal aktörler ile devlet arasında uygulanacak bilgi paylaşımının nasıl olması gerektiği hususuna odaklanılmış, kamu ve özel sektörün bir araya geldiği bankalar gibi özel sektör temsilcilerinin taleplerini iletebilecekleri bir platform oluşturmanın önemi vurgulanmıştır (Eaton vd., 2018). Kişisel bilgilerin gizliliğini sağlayacak devlet idaresindeki merkezi bir altyapı ve bu altyapının güvenliği önem arz etmektedir.

Medaglia vd. (2017) tarafından yürütülen ve ulusal elektronik kimlik kartlarının Danimarka bankacılık sektöründeki kullanımını ele alan bir çalışmada, birincil ve ikincil veri

analizleri yapılmıştır. Bu araştırma kapsamında, Danimarka ulusal e-ID'nin ortaya çıkmasında devlet ve bankacılık sektörleri arasındaki çıkarların uyumlaştırılması, kaynakların birbirine bağlanması ve yönetim modellerinin düzenlenmesi gibi konularda zamanla ortaya çıkabilecek değişimler ve işbirlikçi uygulamaların teorik altyapısı incelenmiştir. Araştırma sonucunda, dijital bilgi altyapısının kurulmasında kamu-özel sektör işbirliğinin sağlanması amacıyla kullanılacak yöntemleri kavramsallaştırmak için bir işlem modeli oluşturulmuştur (Medaglia vd., 2017).

Chemla & Richard 2005 yılında akıllı bir kart ve biyometrik bir profil kullanarak bireyin kimliğini saptamaya dayalı finansal işlemler için güvenlik cihazı, metodu ve sistemi konulu bir patent almışlardır. Dolayısıyla akıllı kartların finansal işlemlerde kullanılması fikri yeni olmamakla birlikte, akıllı kart sınıfına dahil olan akıllı ulusal kimlik kartlarında bu fikrin uygulanmasının dünya genelinde henüz çok yeni olduğu ve bu konuya olan ilginin arttığı gözlenmektedir (Chemla & Richard, 2005).

Birleşik Arap Emirlikleri'nde de vatandaşlara biyometrik ve biyografik detaylarının içerisinde bulunduğu akıllı kimlik kartları verilmektedir. Bu kartlar ülkede birincil kimlik kartı olarak zorunlu kılınmıştır. Hükümet, mevcut kartları gruplayarak bir araya getirmeyi ve bunları yeni akıllı kimlik kartı ile değiştirmeyi amaçlamıştır. Ayrıca bu kartın ülkedeki mevcut elektronik ödeme sistemlerini de destekleyeceği ve geliştireceği düşünülmektedir (Al-Khouri, 2014).

Ruanda'da da benzer şekilde akıllı kimlik kartları yetişkin halkın büyük çoğunluğuna dağıtılmış, bu kimlik kartları ile bankacılıktan sosyal güvenliğe kadar çeşitli hizmetlerde kimlik doğrulama için kullanılmaktadır. Bireysel kaydı modernize etme ve çocuklar için kimlik tanımayı sunma çalışmaları devam etmektedir (Nyamulinda, 2014). Pakistan'da ülkenin en büyük para transfer programından faydalanan şahısları tanıma ve e-ödeme sistemlerinin geliştirilmesinde de biyometrik kimlik kartları kullanılmıştır (Khan, 2014).

Finlandiya'da, 18 yaş ve sonrası tüm Finli vatandaşlara ve daimi ikamet edenlere Finli Elektronik Kimlik Kartı (FINEID) verilmektedir. Bu elektronik kimlik kartı zorunlu değildir. E-Devlet, E-Bankacılık, E-Ticaret hizmetlerinde ve elektronik olarak imza atmak için kullanılmaktadır. TUPAS adlı bir altyapı kullanılarak e-ticarette doğrulama ve online ödeme yapılabilmektedir. Makalede Finlandiya'da kullanılan sistemin yönetimsel detayları kapsamlı olarak sunulmaktadır (Rissanen, 2010).

5. Sonuç

İşletmeler ve resmi kurumlarda yapılan işlemlerin hızlı ve aynı zamanda güvenli bir biçimde onaylanabilmesi 21. yüzyılda finansal süreçlerin temel gereksinimleri arasındadır. Biyometrik teknikler; yazılım ve donanım teknolojilerinin hızlı gelişimi sonrası özellikle pasaport ve kimlik kartı gibi yüksek düzeyde güvenlik riski taşıyan belgelerde yaygın olarak kullanılır hale gelmiştir. Bu durum insanların daha hızlı ve aynı zamanda daha güvenli süreçlerle işlem yapabilmesini sağlamaktadır. Bu tür sistemlerin temel amacı, meşru erişim hakkı olmayan kişilerin sistem erişimlerini engellemektir. Ancak teknik, hukuki ve güvenlikten kaynaklanan

altyapı eksikliklerinin tüm dünyada varlığını devam ettirdiğini, bu nedenle sistemlerin halen kötücül yazılımlara ve fiziksel saldırılara karşı büyük ölçüde savunmasız olduğunu belirtmek gerekir.

Akıllı kartlarda tersine mühendislik, güç analizi, gizli tarama ve izleme, gizli dinleme ve sahtecilik gibi bazı güvenlik açıkları bulunmaktadır. Akıllı kartlarda önlem alabilmek için öncelikle açıkların ne olduğunun bilinmesi gerektiğinden, bu makale kapsamında bu açıkların ne olduğu hakkında bilgiler sunularak alınabilecek önlemler hakkında detaylı bilgiler sunulmuştur. Bu kapsamda dikkat edilmesi gereken birçok husus bulunmaktadır. Çalışma kapsamında, şifre kullanımı, şifreleme, biyometrik tanımlama, merkezi veritabanları, özel uygulamalar, yedekleme ve güncelleme prosedürleri ve donanımsal anomalilerden kaynaklanan güvenlik riskleri mevcut yazın temelinde incelenmiştir.

Yazında, akıllı kart uygulamalarında veri güvenliğinin sağlanması için alınması gereken çok sayıda önlem ele alınmış olmakla birlikte; bunların içerisinde verilerin genel erişime açık saklama birimleri yerine veri gizliliğinin esas alındığı birimlerde saklanması en dikkat çekici öncelik olarak ön plana çıkmaktadır. Buna göre biyometrik kartlar verilerin yerel veritabanlarında saklanmasını sağlayacak şekilde tasarlanmalıdır. Herhangi bir biyometrik sistemde, kötüye kullanımı önlemek için güçlü denetim ve gözetim programları olmalıdır. Ayrıca güvenliği sağlamak için iletişimde uygun protokoller tercih edilmelidir.

Akıllı kart sistemleri yürütülen işlemleri kolaylaştırmakla beraber farklı güvenlik risklerini de beraberinde getirmektedir. Bu nedenle hızla gelişen yazılım ve donanım teknolojilerinin takip edilerek, sistemlerin güvenlik açıklarının hızlı bir şekilde giderilmesi gerekmektedir.

Veri koruma ile ilgili hükümler içeren ulusal ve uluslararası mevzuat bileşenlerinin odaklandığı temel nokta kişisel veri güvenliğidir. Akıllı kartlardan kaynaklanan güvenlik risklerinin kabul edilebilir düzeyin üzerine çıkması durumunda kişisel hak ihlallerinin yaşanması kaçınılmaz olacaktır. Bu nedenle kimlik kartlarının kullanımı da benzer mevzuat bileşenlerinden etkilenmek durumundadır.

14 Mart 2016'da dağıtımına başlanmış olan akıllı kimlik kartlarının Türkiye'deki uygulamasının kısa bir süre içinde ülke çapında yaygınlaştırılması hedeflenmektedir. Bu nedenle bu kartların güvenliğinin sağlanması için pek çok önlem alınmaktadır. Çalışma kapsamında bahsi geçen önlemler birbirleriyle ilişkili ve teorik bir bakış açısıyla sınıflandırılmış; ön plana çıkan konular ile sorunların çözüm yöntemleri mevcut yazın temelinde incelenmiştir. Çalışmada belirtilen yöntemler dikkate alınarak önlemlerin artırılması ve bilgi güvenliğinin sağlanması önem arz etmektedir.

Kaynakça

Ajanshaber. (2015). *Yeni kimlikler ne zaman verilecek*. Erişim Tarihi: 26.02.2016, http://www.ajanshaber.com/yeni-kimlikler-ne-zaman-verilecek-haberi/327952

Al-Khouri, A. M. (2014). Electronic payments: Building the case for a national initiative. *Advances in Social Sciences Research Journal*, 1(3), 176-195.

Anthes, G. (2015). Estonia: A model for e-government. *Communications of the ACM*, 68(6), 18-20.

Ayyanna, K. (2007). *Study of some fingerprint verification algorithms*. (Yayınlanmamış Yüksek Lisans Tezi). Department of Electronics & Communication Engineering National Institute of Technology, Rourkela.

Başak, M., & Bıyıklıoğlu, F. (2008). *Bilgi güvenliği ve akıllı kartlar*. II. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, KKTC, 213-215.

Best. (2013). *Biyometrik güvenlik sistemleri*. Erişim Tarihi: 21.03.2018, http://www.bestdergisi.com.tr/arsiv/yazi/biyometrik-guvenlik-sistemleri

Biometrics. (2004). *Biometric application*. Erişim Tarihi: 18.03.2018, http://www.geocities.ws/hnabhijith/Biometrics.htm#7

Biometrics. (2005). *Liveness detection for iris recognition*. Erişim Tarihi: 21.03.2016, http://www.biometrics.org/bc2005/Bios/RS/Bio%20Toth%20_%20RS.pdf

Chemla, Y., & Richard, C. (2005). *Security device, method and system for financial transactions, based on the identification of an individual using a biometric profile and a smart card*. US Patent.

CNN. (2014). *Branding Nigeria: Mastercard-backed i.d. is also a debit card and a passport*. Erişim Tarihi: 04.03.2018, http://edition.cnn.com/2014/09/25/business/branding-nigeria-mastercard-backed-i-d-/index.html

Eaton, B., Hedman, J., & Medaglia, R. (2018). Three different ways to skin a cat: Financialization in the emergence of national e-id solutions. *Journal of Information Technology*, 33(1), 70-83.

EKDS. (2015). *Yeni kimlikler ilk hangi ilde dağıtılacak*. Erişim Tarihi: 26.02.2016, http://www.ekds.org/node/83

Fastcompany, (2013). *Nigeria's futuristic national id cards are also debit cards*. Erişim Tarihi: 04.03.2018, https://www.fastcompany.com/3009549/nigerias-futuristic-national-id-cards-are-also-debit-cards

Gerrit, H. (2004). *Biometric identity cards: Technical, legal, and policy issues*. ISSE 2004 — Securing Electronic Business Processes, Editors: Sachar Paulus, Norbert Pohlmann, Helmut Reimer, Vieweg+Teubner Verlag, 1-11.

Haber7. (2016). *İşte yeni kimlik kartlarının dağıtım tarihi*. Erişim Tarihi: 01.03.2018, http://ekonomi.haber7.com/ekonomi/haber/1814858-iste-yeni-kimlik-kartlarinin-dagitim-tarihi

House of Commons Science and Technology Committee. (2006). *Identity card technologies: Scientific advice, risk and evidence*. The Government Reply to the Sixth Report from the House of Commons Science and Technology Committee Session, 1-200.

İnan, T. (2012). *Akıllı kart teknolojisi*. Erişim Tarihi: 16.03.2018, https://www.ce.yildiz.edu.tr/personal/tevfik/file/1148/0113841+Mesleki+Terminoloji+II+-+SmartCard.pdf

İTÜ. (2013). *Şifreleme yöntemleri*. Erişim Tarihi: 02.07.2018, https://bidb.itu.edu.tr/eskiler/seyirdefteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri

Jain, A. K., Hong, L., & Bolle, R. (1997). On-line fingerprint verification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(4), 302-314.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4-20.

Karakülah, M., Danacı, M., & Ciritçi, İ. H. (2004). Biyometrik parmak izinin akıllı kartlarla kullanımı ve uygulaması. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 10(4), 13-16.

Khan, G.A. (2014). *Building robust identification systems*. World Bank South-South Learning Forum, Rio de Janeiro, Brazil.

Ko, H., & Caytiles, R. D. (2011). A review of smartcard security issues. *Journal of Security Engineering*, 8(3), 359-370.

Koteswara, R. D. V. N., Kishore, G. S. N., & Vasavi, G. (2014). Adaptive fingerprint enhancement. *International Journal of Future Generation Communication and Networking*, 7(4), 159-170.

Leparisien, (2011). *Plus de 10 % des passeports biométriques seraient des faux*. Erişim Tarihi: 21.03.2018, http://www.leparisien.fr/faits-divers/plus-de-10-des-passeports-biometriques-seraient-des-faux-19-12-2011-1775325.php

Medaglia, R., Hedman, J., & Eaton, B. (2017). *Public-private collaboration in the emergence of a national electronic identification policy: The case of nemid in Denmark*. Proceedings of the 50th Hawaii International Conference on System Sciences, Hawaii, 2782-2791.

Nandakumar, K., Jain, A. K., & Ross, A. (2009). *Fusion in multibiometric ıdentification systems: What about the missing data?*. The 3rd edition of the International Conference on Biometrics (ICB), Alghero, Italy, 743-752.

Nyamulinda, P. (2014). *Experience of Rwanda in implementing a national identification program*. World Bank South-South Learning Forum, Rio de Janeiro, Brazil.

Oranlı, G. (2007). *Radyo frekansıyla tanımlama teknolojisinin uygulanması kararının bulanık analitik hiyerarşi yöntemi ile değerlendirilmesi: Bankacılık sektöründe bir uygulama*. (Yayınlanmamış Yüksek Lisans Tezi). İTÜ Fen Bilimleri Enstitüsü, İstanbul.

Özbey, R. (2006). *Akıllı kart teknolojileri*. Ulusal Elektronik İmza Sempozyumu, Ankara, 49.

Pymnts, (2014). *Estonian national id cards embrace electronic payment capabilities*. Erişim Tarihi: 04.03.2018, https://www.pymnts.com/news/2014/estonian-national-id-cards-embrace-electronic-payment-capabilities

Resmi Gazete. (2016). *Kişisel verilerin korunması kanunu*. Erişim Tarihi: 15.03.2018, http://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf

Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. Bank IDs. *Identity in the Information Society*, 3(1), 175-194.

Roy. (2015). *Saying no to biometrics*. Erişim Tarihi: 20.03.2016, http://www.maurice-info.mu/saying-no-biometrics-guru-dev-teeluckdharry.html

Sağıroğlu, Ş., & Özkaya, N. (2006). Otomatik parmak izi tanıma sistemlerinde kullanılan önişlemler için yeni yaklaşımlar. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 21(1), 11-19.

Turkishtimedergi. (2015). *İşte finansta yılın inovasyonları*. Erişim Tarihi: 04.03.2018, http://www.turkishtimedergi.com/finans/iste-finansta-yilin-inovasyonlari

TÜBİTAK. (2006). *Akıllı kartların kamuda kullanımı*. Ön çalışma raporu.

UK Government Biometrics Working Group (BWG). (2003). *Biometric security concerns*. CESG Technical report.

Wrankl. (2016). *Smart card applications*. Erişim Tarihi: 28.02.2016, http://www.wrankl.de/SCA/SCA.html

Xiao, Q., & Savastano, M. (2007). *An exploration on security and privacy ıssues of biometric smart id cards*. Information Assurance and Security Workshop, West Point, NY, 228-233.