mülkiye dergisi
Araştırma Makalesi

Bankacılıkta Uzaktan Kimlik Tespitinde Karşılaşılan Riskler ve Çözüm Önerileri

Serdal Yıldırım, Fibabanka Ar-Ge Merkezi, İstanbul
ORCID: 0009-0006-9941-081X
E-Posta: Serdal.Yildirim@fibabanka.com.tr

Özet

Dijital bankacılık ve uzaktan bankacılık hizmetlerinin kullanımı giderek artmaktadır ve bankaların teknoloji entegrasyonuna önem vermeleri gerekmektedir. Yeni teknolojilerin sunduğu faydaları fark eden bankalar, tasarruf etme ve müşteri sayısını artırma potansiyeline sahiptir. Teknolojik ilerlemeler ile dijital bankacılık uygulamalarındaki gelişmeler hızlanmıştır ve müşteri deneyimini geliştirmek hedeflenmektedir. Dijital bankacılık ve uzaktan bankacılık hizmetlerinin yaygınlaşması ile fiziksel banka şubelerine olan gereksinim azalırken, müşteri edinimi için farklı yöntemler geliştirilmektedir.

Uzaktan kimlik tespiti, bankacılık ve diğer çevrimiçi hizmetlerde güvenliği sağlamanın temel taşlarından biridir. Ancak, bu süreçteki güvenlik zayıflıkları, kötü niyetli kişilerin kimlik avı gibi suçlar işlemesine olanak tanıyabilir. Yapay zekâ, bu tür tehditlere karşı etkili bir savunma mekanizması sağlayabilir. Ancak, bazı bankalar hala bu teknolojiyi yeterince kullanmamakta veya güvenlik önlemlerini yeterince güçlendirmemektedir. Bu durum, gelecekte Deep Fake gibi gelişmiş sahtekarlık yöntemlerinin ortaya çıkmasına neden olabilir.

Son dönemde Türkiye'de dijital bankacılığın yükselişi, finansal hizmetlere olan erişimde devrim niteliğinde bir değişim sağlamıştır. Bu yeni dijital bankaların kurulması ve uzaktan kimlik doğrulama yöntemlerinin benimsenmesiyle, müşteriler bankacılık işlemlerini kolaylıkla gerçekleştirebilir hale gelmiştir. Geleneksel bankacılık modelinden farklı olarak, dijital bankacılık müşterilere her an her yerden erişim imkânı sunar. Bu durum, müşterilere bağımsızlık ve özgürlük sağlarken, aynı zamanda bankalar için de operasyonel maliyetlerin düşürülmesini sağlar. Fiziksel banka şubelerine olan ihtiyacın azalmasıyla birlikte, bankalar daha verimli bir şekilde hizmet sunabilir ve bu da genellikle maliyetleri azaltır. Bu dijitalleşme trendi, bankaların daha rekabetçi olmasını ve müşterilere daha hızlı ve kullanıcı dostu bir deneyim sunmalarını sağlar. Özetle, Türkiye'deki dijital bankacılık gelişimi, müşterilere daha kolay, hızlı ve esnek bir bankacılık deneyimi sunarken, bankaların da operasyonel verimliliğini artırır ve maliyetleri düşürür. Bu da finansal hizmetlere olan erişimi genişletir ve toplumun finansal katılımını artırır. Ancak uzaktan bankacılık hizmetleri kullanımı yüksek risk taşımaktadır ve bu risklerin yönetilmesi önemlidir. Bankaların güvenlik önlemlerini artırmaları ve yapay zekâ teknolojilerini kullanmaları, uzaktan kimlik tespiti sürecindeki riskleri azaltabilir. Ayrıca, müşteri memnuniyetini ve kullanıcı dostu bir süreci sağlamak da önemlidir. Bankaların, dijital bankacılık ve uzaktan bankacılık hizmetlerine odaklanarak teknoloji entegrasyonunu geliştirmeleri, tasarruf etme ve müşteri sayısını artırma potansiyeline sahiptir. Bu çalışma, bankaların uzaktan kimlik tespiti yöntemlerini güvenli bir şekilde kullanmalarına yardımcı olmayı amaçlamaktadır.

Anahtar Sözcükler: Dijital Bankacılık, Güvenlik, Uzaktan Müşteri Edinimi, Uzaktan Kimlik Tespiti, Yapay Zekâ.

Makale Gönderim Tarihi: 28.11.2023, Makale Kabul Tarihi: 27.02.2024

Identification of Risks Encountered in Remote Identity Verification in Banking and Proposed Solutions

Abstract

The usage of digital banking and remote banking services is on the rise, emphasizing the importance for banks to prioritize technology integration. Banks recognizing the benefits offered by new technologies have the potential to save costs and attract more customers. Technological advancements have accelerated developments in digital banking applications, which aim to enhance the customer experience. As the prevalence of digital banking and remote banking services grows, the need for physical bank branches diminishes, leading to the development of various methods for customer acquisition.

Remote identity verification is crucial for ensuring security in banking and other online services. However, security vulnerabilities within this process may allow malicious individuals to commit crimes such as phishing. Artificial intelligence (AI) can provide an effective defense mechanism against such threats. Nevertheless, some banks still underutilize this technology or fail to sufficiently strengthen their security measures. This may lead to the emergence of advanced fraud methods, such as Deep Fake, in the future.

The recent rise of digital banking in Turkey has revolutionized access to financial services. With the establishment of these new digital banks and the adoption of remote authentication methods, customers can easily conduct banking transactions. Unlike the traditional banking model, digital banking offers customers access to services anytime, anywhere, providing them with independence and freedom. By reducing the need for physical bank branches, banks can deliver services more efficiently, which often reduces costs. This digitalization trend enables banks to be more competitive and offer faster and user-friendly experiences to customers. Overall, the development of digital banking in Turkey not only provides customers with an easier, faster, and more flexible banking experience but also increases operational efficiency and reduces costs for banks. This, in turn, expands access to financial services and enhances financial inclusion within society.

However, the use of remote banking services carries high risks, and managing these risks is crucial. Enhancing security measures and utilizing AI technologies can mitigate the risks associated with remote identity verification. Additionally, prioritizing customer satisfaction and providing a user-friendly process are essential. By focusing on digital banking and remote banking services, banks can improve technology integration, leading to potential cost savings and an increase in customer numbers. This study aims to assist banks in securely deploy remote identity verification methods.

Keywords: Digital Banking, Security, Remote Customer Acquisition, Remote Identity Verification, Artificial Intelligence.

Giriş

Bankalar, müşterilerinin beklenti ve ihtiyaçlarını etkin bir şekilde karşılamak ve toplumun ihtiyaçlarıyla uyumlu adımlar atmak için hizmet sunan kurumlar olarak görev yapmaktadır (Gorgani, 2016). Bu sebeple bankacılık sektörünün, dijital dönüşümlere uyum sağlaması bir zorunluluk hâlidir. Bankacılık sektörü yapısı itibarıyla dijital dönüşümden etkilenen önemli bir aktör olmasının yanında dijital dönüşüme de öncülük etmektedir. Yeni teknolojilerin benimsenmesi müşteri deneyimlerini ve banka satış performanslarını etkilemektedir (Indriasari vd., 2019; Arjun vd., 2021). Bu bağlamda bankacılık sektörü, akıllı sistemlerin popüler olması nedeniyle verimli ve müşteri dostu yeni sistemler geliştirmek için birçok Ar-Ge girişimine yatırım yapmaktadır (Wassan Abdullah, 2020). Dijital bankacılıkta kullanılan güncel teknolojiler; yapay zeka (AI), büyük veri analitiği (BDA), blok zinciri, dijital para birimi, biyometri, bulut bilişim, nesnelerin İnterneti (IoT), açık bankacılık ve kimlik doğrulama olarak sıralanmaktadır (Indriasari vd., 2022).

Ülkemizde, son zamanlarda uzaktan müşteri edinimi gibi finansal teknolojilerle ilgili önemli çalışmalar yapılmış ve bu alanla ilgili düzenlemeler günlük hayatımıza yavaş yavaş girmeye başlamıştır. Mart 2023'te Cumhurbaşkanlığı Finans Ofisi tarafından yayımlanan Türkiye Fintek Rehberi ve Türkiye Fintek Ekosistemi Durum Raporu, ülkedeki bu gelişmelere yön verdiği ve mevzuatsal uyum için gerekli düzenlemelerin yapıldığını göstermektedir (CFO, 2023). Dijitalleşme ve teknolojinin finans sektöründe yaygınlaşmasıyla birlikte, finansal hizmetlerde büyük bir değişim ve dönüşüm süreci yaşanmaktadır. Bu durum, hizmet ağları, iş modelleri ve yapısal düzenlemelerin köklü bir şekilde değişmesine neden olmaktadır. Koronavirüs salgınıyla ortaya çıkan yeni durum da finans sektöründe karar vericilerin sektör düzenlemelerini şekillendirmesine etki etmektedir. Örneğin, devletin 2019-2023 dönemini kapsayan 11. Kalkınma Planı'nda belirtilen 248.7 nolu politika tedbiri doğrultusunda, finansal kuruluşlar müşterileriyle gerçekleştirdikleri işlemlerde "fiziki belge" ve "elle atılan imza" kullanımını azaltma amacıyla aksiyonlar almaktadır ve bu süreç devam etmektedir (SBB, 2019).

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından 01.04.2021 tarihi 31441 Resmî Gazete'de yayınlanan Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik yayımlanarak bankalar tarafından yeni müşteri kazanımında kullanılabilecek uzaktan kimlik tespiti yöntemleri belirlemiştir. Söz konusu süreç Mali Suçları Araştırma Kurulunca 30 Nisan 2021 tarihli ve 31470 sayılı Resmi Gazete'de yayımlanan 19 sıra nolu tebliğin yayımlanması ile

desteklenmiş ve böylelikle yazılı şekil şartına tabi sözleşmeler de dâhil olmak üzere, bankalar ile müşterileri arasındaki sözleşme ilişkilerinin elektronik ortamda kurulabilmesine ve uzaktan kimlik tespiti yapılabilmesine imkân tanınmış, diğer ülke uygulamalarında olduğu gibi şubesiz bankacılık modelinin altyapısının kurulmasına yönelik önemli bir adım atılmıştır (RG, 30.04.2021-31470). 2021 Yılı Ekonomik Reform Paketine uygun olarak uzaktan müşteri edinimi süreci Türkiye Cumhuriyeti Merkez Bankası (TCMB) tarafından Ödeme ve Elektronik Para Kuruluşlarını, Sermaye Piyasası Kurulu (SPK) tarafından sermaye piyasası kurumlarını ve BDDK tarafından finansal kuruluşları da kapsar şekilde genişletilmiştir (HMB, 2021). Son olarak BDDK tarafından 29.12.2021 tarihinde yayımlanan Dijital Bankaların Faaliyet Esasları ile Servis Modeli Bankacılığı Hakkında Yönetmelik (DBY) ile de Fidor, Nubank, Monzo, WeBank, Tandem, N26, Revolut gibi şube olmaksızın sadece dijital ortamda hizmet verecek Neobank uygulamalarına imkân veren dijital bankacılığın yasal altyapısını hazırlamıştır (RG, 29.12.2021-31704). Video bankacılık olarak adlandırılan uzaktan müşteri edinim uygulamaları sadece müşteri edinim ile sınırlandırılmamış; uzaktan sözleşme ilişkisi kurulması, finansal ve finansal olmayan işlemlerin gerçekleştirilmesinde doğrulama yöntemleri olarak da kullanılmaya başlanmıştır. Öyle ki video bankacılık; dijital ve servis modeli bankacılığın ana dayanağı olmuş ve kullanım alanı sadece müşteri edinim ile sınırlanmayarak finansal ve finansal olmayan işlemlerin gerçekleştirilmesi amacı ile de kullanılmaya başlanması ve kullanımının tüm finansal sistemde yaygınlaşması nedeni ile yaratacağı risk de büyümüştür.

BDDK tarafından yayımlanan Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik sürecin güvenliğinin sağlanması için bilgi teknolojileri tarafından uygulanan kontroller ile müşteri temsilcisi tarafından yapılacak ek kontroller koyarak sisteme yeterli bir güvence sağlamaya çalışmıştır (RG, 30.04.2021-31470). Ancak yapay zekânın sağlayacağı ilave güvenliğe değinilmemiş; teknolojik olarak 'yakın alan iletişimi' (NFC) kullanılarak aktif ve pasif doğrulamanın yapılması, biyometrik yüz karşılaştırılması ile kişinin canlılığını tespit edici yöntemlerden bahis olunmakla yetinilmiştir. İşbu hâl ile dijital bankacılık süreci yapay zekânın yaratacağı ilave korumadan mahrum kalmıştır. Oysaki Deep Fake teknolojisinin bazı kötü niyetli kişiler tarafından uzaktan müşteri edinim sürecinde ve finansal ve finansal olmayan işlemlerin gerçekleştirilmesinde banka ve müşterisini dolandırmak amaçlı kullanılma ihtimali yakın gelecekte büyük bir tehlike yaratacak niteliktedir.

Bankalar ve diğer kuruluşlar, bilişim teknolojilerini modern koşullara uygun

olarak dönüştürmektedir. Bu yöntemle bankaların sağladığı idari ve kamu hizmetleri elektronik biçimde sunulmaktadır (Sova vd., 2021). Dijital bankacılık, gelişen teknolojik trendleri kullanarak etkili, hızlı ve kullanıcı dostu bankacılık işlemlerinin gerçekleştirilmesini sağlayan bir kavramdır (Indriasari vd., 2022). Juniper Research tarafından yapılan infografik araştırmasına göre, dünya genelinde dijital bankacılık ve uzaktan bankacılık hizmetlerinin kullanıcı sayısı 2020'de 2,4 milyar olarak kaydedilmiştir ve 2024'te %54'lük bir artışla 3,6 milyara yükseleceği öngörülmektedir (Juniper Research, 2020). Bu sebeple dijital bankacılık ürünlerinin ve sektörün teknoloji entegrasyonunun önemi de gün geçtikçe artmaktadır.

Bankalar, yapay zekâ teknolojilerini kullanarak inovatif bankacılık hizmetleri sunarak hızlı bir şekilde büyümeye devam etmektedir. Son yıllarda, FinTech şirketleri ve yapay zekâ alanında meydana gelen hızlı teknolojik ilerlemeler, bankacılık sektörünün hizmet sunumunu tamamen farklı bir seviyeye taşımıştır (Beybur, 2021). Örneğin dijital bankacılık hizmetlerinin geleneksel bankacılık hizmetlerinin yerine geçmesiyle bankalar hizmet yelpazelerini genişletilerek müşteri sayılarını önemli ölçüde artırma şansı elde etmiştir (Toshtemirovich Mamadiyarov, 2021). Yeni teknolojilerin sunduğu potansiyel faydaların farkında olan Amerika Birleşik Devletleri'ndeki bankaların neredeyse %80'i, 2023 yılına kadar yaklaşık 447 milyar dolar tasarruf etmeyi beklemektedir (Digalaki, 2022). Bu teknolojiler, bankacılık kanallarında (örneğin; otomatik bankamatikler, çevrim içi bankacılık, mobil bankacılık), hizmetlerde (örneğin; çek görüntüleme, ses tanıma, sohbet robotları) ve çözümlerde (örneğin; AI yatırım danışmanları ve AI kredi seçicileri) yenilikçi uygulamalara yol açmaktadır (Fares vd., 2022). 2019 yılında COVID-19 pandemisinin yayılmasını önlemek için akıllı dijital bankacılık uygulamalarındaki gelişmeler hızlanmıştır. Bu teknolojiler ile müşteri deneyimlerini geliştirmek ve insan etkileşimini azaltmak hedeflenmektedir (Indriasari vd., 2022). Fiziksel banka şubelerine olan gereksinimin zamanla azalacağı öngörüsü ile müşteri edinimi için farklı yöntemler geliştirilmiştir (Dağıdır Çakan vd., 2022).

Son zamanlarda ülkemizde de dijital bankalar kurulmaya başlanmış (1 dijital mevduat bankası ve 3 dijital katılım bankası) ve uzaktan kimlik tespiti yöntemlerine ve elektronik ortamda sözleşme ilişkisinin kurulmasına imkân veren düzenlemeler tüzel kişileri de kapsar şekilde hayata geçirilmeye başlanmıştır. Uzaktan müşteri edinimi ve bu süreçte yapılan uzaktan sözleşme ilişkisi kurulması dijital ve servis modeli bankacılığının temeli olmuştur. Bu dijital düzenlemelerden biri olarak uzaktan kimlik tespitinin yapılması ve sözleşme kurulmasının mümkün olması ile fiziksel varlığa gerek duyulmadan

uzaktan kimlik doğrulaması ile müşteri edinilmesi ve müşterilerine hizmet alma imkânı sağlanmıştır. Bu uygulama ile bankalar, müşterilerin bankayı bizzat ziyaretine gerek kalmaması gerçeğinden hareketle müşterilere bankacılık hizmeti sunar (Belov ve Zagumennov, 2019; Sova vd., 2021). Bu hizmet birçok avantajı beraberinde getirmiştir. Gelişmiş ülkelerde, otopark problemi ve yaşam temposunun yüksekliği sebebi ile banka ofislerine ziyaretler engellenebilmektedir. Dijitalleşmenin getirdiği bir avantajla bu sistem uzaktan yürütülebilir hale getirilmiştir. Ayrıca uzaktan kimlik tespiti yöntemleriyle banka giderleri azaltılmakta ve finansal hizmetlere erişilebilirlik artmaktadır (Ezrokh, 2020). Öte yandan Koronavirüs Pandemisi gibi beklenmedik uzun vadeli karantinalar, bankaları ve müşterilerini çevrim içi çalışmaya zorlamıştır. Bu sebeple bankalarda dijital altyapılar ve dijital ekonominin geliştirilmesi gerekliliği doğmuştur (Sova vd., 2021). Bu uygulamalar müşteriler için yüksek derecede bağımsızlık ve özgürlük sağlar (Korobov, 2017). Uzaktan kimlik doğrulama yöntemleri, kullanıcı deneyimini iyileştirebilir, uluslararası hizmetlerin geliştirilmesine katkıda bulunabilir ve fiziksel olarak banka içerisinde bulunmanın neden olduğu gereksiz sağlık risklerinden kaçınmayı sağlayabilir (ENISA, 2021).

Bankalar için yeni bankacılık ürün ve hizmetleri, ekonomik büyüme ve rekabet gücü sağlamada önemli bir araç olsa da uzaktan bankacılık hizmetlerinin kullanımı, çevrim dışı hizmetlere göre daha yüksek risk taşıdığından, risk faktörü son derece önemlidir (Mamadiyarov, 2021). Cardiff Üniversitesi'nden Cohen, risklerin azaltılmasının uzaktan bankacılık işlemlerinin yürütülmesinde pozitif bir ilişki olduğunu tespit etmiştir (Koenig-Lewiset vd., 2010). Bu durumda bankacılıkta kullanılan uzaktan kimlik tespiti yöntemlerinin sahip olduğu risklerin yönetilmesi zorunluluğu doğar. Bu nedenle, bu alanda yapılacak araştırmalar, günümüzün en acil konularından biridir.

Bu çalışmada; öncelikle uzaktan bankacılık hizmetlerinin müşteriler için öneminin vurgulanması, nüfusun kimlik tespiti başta olmak üzere uzaktan bankacılık hizmetleri konusunda bilgi eksikliği gibi olumsuz faktörlerin ortadan kaldırılması, bankacılıkta kullanılan uzaktan kimlik tespiti yöntemlerinin sahip olduğu risklerin belirlenmesi ile süreç boyunca sahip olunan risklerin literatüre dayalı olarak tespit edilmesi hedeflenmektedir. Bu makale, kullanılan yöntemlere yönelik risklerin tespiti, risk yönetimini sağlamak için gerekli altyapının oluşturulması ve risk yönetiminin gerçekleştirilmesi için uygulanacak yönetim planının yapılandırılması sürecine yardımcı olacak literatür bilgisini içermektedir.

Yapılan literatür taraması, aşağıdaki araştırma sonuçlarına yanıt bulmayı hedeflemiştir.

- Bankacılıkta kullanılan uzaktan kimlik tespiti yöntemlerinde Türkiye ve dünyadaki güncel durum nedir?
- Bankalar, bankacılıkta kullanılan uzaktan kimlik tespiti yöntemlerinde ne gibi risklerle karşılaşmaktadır?
- Karşılaşılan riskler için çözüm önerileri nelerdir?

Çalışmanın geri kalanı şu şekilde yapılandırılmıştır: 2. bölüm olan literatür taraması bölümü, bankacılık sektöründe dijitalleşmenin dâhil olduğu ve bir anlamda uzaktan kimlik tespiti yöntemlerine ilişkin çalışmaları inceler. 3. Bölümde bankacılıkta kullanılan uzaktan kimlik tespiti yöntemleri ele alınmıştır. 4. bölüm, süreçlere dair riskleri literatür aracılığı ile tespit eder. 5. bölümde tespit edilen risklere yönelik risk yönetimi önerileri yer almaktadır. Son olarak 6. bölüm, çalışmaya dair bulguları ve sonuç bölümünü içermektedir.

Literatür Taraması

Bankacılık sektöründe dijital teknolojilerin ve uzaktan kimlik tespiti yöntemlerinin literatürde ele alındığı bir dizi çalışma bulunmaktadır. Uzaktan kimlik tespiti (digital onboarding), banka müşterisi olmak için banka şubesine gitme, uzun sözleşmeleri okuma ve el ile imzalama gibi zorunlulukları ortadan kaldıran bir sistemdir (Dağıdır Çakan vd., 2022). Bu alanda yapılan araştırmalar, bankacılık sektörünün dijital dönüşümünü anlamak, müşteri deneyimini iyileştirmek, operasyonel verimliliği artırmak ve güvenlik önlemlerini güçlendirmek gibi amaçlarla gerçekleştirilmektedir. Kimlik doğrulama, gerçek veya tüzel kişinin kimliğine dayanan güvenin temel olduğu her türlü durum için önemlidir (ENISA, 2021). Özellikle mobil bankacılık, internet bankacılığı, yapay zekâ, büyük veri analitiği ve biyometrik kimlik doğrulama gibi konular ve bu alanlardaki risk yönetimi, literatürde önemli bir araştırma alanı olmuştur. Bu çalışmalar, bankacılık sektöründeki dijital teknolojilerin ve uzaktan kimlik tespiti yöntemlerinin etkin kullanımının incelenmesini sağlamakta ve sektörün gelecekteki yönünü belirlemede önemli bir rol oynamaktadır.

Korobov, teknolojinin gelişimi ile dönüşen bankacılık sektörünü ve oluşan yeni bankacılık kültürünü ele almıştır (Korobov, 2017). Indriasari vd. (2022), dijital banka teknolojisinin bankaların işlerini desteklemek ve deneyimleri iyileştirmek için geleneksel bankacılığın geliştirilmesi için kullanılması gerektiğini ifade etmektedir. Stoiko, BankID gibi uzaktan dijital uygulamalar ile yerel finans piyasası katılımcıları için hizmet sunma prosedürünün basitleştiğini ve yenilikçi

hizmetlerin oluşturulması, mevcut durumun iyileştirilmesi için uygun koşulların sağlanabileceğini ifade etmiştir (Stoiko, 2020).
İnternet, bankacılık ve alışveriş işlemlerinde yoğun olarak kullanılmasına rağmen, araştırmalar internetin güvenli olmadığını göstermektedir. İnternet, kimlik avı, kimlik sahtekârlığı, bilgisayar korsanlığı gibi tehditlere maruz kalmaktadır. Bankacılık ve finansal işlemlerdeki gelişmiş teknolojilerin kullanımı arttıkça, saldırganlar da gizli verilere erişmek için daha gelişmiş teknikler kullanmaktadır (Sheshasaayee ve Sumathy, 2017). Bu gibi durumların ele alındığı çalışmalara ek olarak Zadeh ve Barati, en güvenilir biyometrik yöntemlerden biri olarak üç boyutlu yüz tanıma ve bir yazılım içerisinde yer alan tek seferlik bir parola içeren bir sistem önermiştir (Zadeh ve Barati, 2019).

Ezrokh, Rus bankacılık sisteminde uzaktan kimlik doğrulama uygulamalarının sorunlarını çözebilmek için ilgili alandaki uluslararası deneyimin incelenmesi, Rus bankalar ve müşterileri arasındaki uzaktan kimlik doğrulama uygulamalarına karşı olan düşük motivasyonun temel nedenlerinin analiz edilmesi, bu sorunların formülize edilmesi ve yapılandırılması, devlet politikalarındaki sorunlu alanları incelemek, siber suç önleme faaliyetlerini incelemek, tespit ettikleri sorunların çözümlerine gerekçe sağlamak ve orta ve uzun vadede uzaktan kimlik tespiti yapılmasını sağlayan sistemin geliştirilmesi amacı ile dijitalleşmenin genel risklerini belirlemek üzerine çalışmıştır (Ezrokh, 2020). Shamah, bankaların kimlik hizmeti sağlayıcısı olarak hangi rollere sahip olduğunu açıklarken ulusal e-ID yapılarını tanıtan bir çalışma yapmıştır (Shamah, 2018). Keleş ve Demirel (2020), uzaktan müşteri kabulünde yüz tanıma ile Türkiye Cumhuriyeti Kimlik Kartı (TCKK) kimlik doğrulamasının kullanımı üzerine yaptıkları çalışmada yüz tanıma oranını iyileştirmek için renkli yüz görüntüsünün alınmasını sağlayan 'yakın alan iletişimi' (NFC) özelliğini incelemiştir. Toshtemirovich Mamadiyarov (2021), Özbekistan'daki bankacılık ve finans siteminde uygulanan yeni teknolojilerin avantajlarını ele almıştır.

Öte yandan uzaktan müşteri edinimi, sürdürülebilirlik açısından da kıymetli bir yöntem olarak ele alınmıştır. Dağıdır Çakan vd. (2022)'nin çalışmasında, vaka örneği olarak uzaktan müşteri kazanımları üzerinden yapılan hesaplamada, 733.111 adet müşteri için toplam 274 bin ağaç değerinde kâğıt tasarrufu yapıldığı tespit edilmiştir. Ayrıca müşterilerin bankaya gitmesinin gerekmemesi ile yakıt tasarrufu ve banka işlem süreçlerinin kısalması ile de zaman tasarrufu sağlanabilmektedir.*Bankacılıkta Kullanılan Uzaktan Kimlik Tespiti Yöntemleri*
Bankacılık sektörü, sıkı regülasyona tabi olan bir sektördür ve sürekli olarak yeni yaklaşımlar ve teknolojilerin hızla benimsenmesiyle regülasyon faaliyetleri ön planda olmaya devam etmektedir (Balkan, 2021). Elektronik tanımlama

yöntemlerinin etkinliği, kamu ve özel sektörde sunulan hizmetlerde tek ve güvenilir bir kimlik doğrulama yöntemi kullanılmasını amaçlamaktadır. Bu sayede kullanıcılar, farklı hizmetlere erişmek için farklı kimlik doğrulama yöntemleri kullanmak yerine, tek bir yöntemle tüm hizmetlere erişebilirler. Bu, kullanıcıların deneyimini kolaylaştırırken, hizmet sağlayıcılar açısından da daha verimli bir işlem süreci sağlar ve güvenliği artırır (Teemu, 2010). Uzaktan kimlik doğrulama kabiliyeti, elektronik işlemlerin olasılığını artırır ve ayrıca işlemde yer alan tarafların kimliklerinin geçerliliğini temin eder (ENISA, 2021). Uzaktan kimlik doğrulama süreci aşamaları Şekil 1'de gösterilmektedir.

Şekil 1. Uzaktan Kimlik Doğrulama Süreçleri

(**Kaynak:** ENISA, 2021. (Yazar tarafından uyarlanmıştır.))

Uzaktan kimlik teşhisi yöntemleri 6 başlık altında ele alınmaktadır. Bunlar: operatör ile yerinde kimlik tespiti, operatör ile video destekli operatör ile kimlik tespiti, uzaktan otomatik kimlik tespiti, elektronik tanımlama araçları ile kimlik tespiti, sertifika tabanlı kimlik tespiti ve kombine yöntemlerdir (ENISA, 2021).

Operatör ile yerinde kimlik tespiti: Operatör ile yerinde kimlik tespiti, operatörün talep ettiği belgelerin banka müşterisi tarafından ibraz edilmesi ve bu belgelerin yüz yüze doğrulama süreci ile onaylanmasını içerir. Video destekli operatör ile kimlik tespiti: Bu yöntemde banka temsilcileri/ operatörler, başvuru sahipleri/banka müşterileri ile çeşitli talimatlara dayalı olarak bir kimlik belirleme süreci yürütürler. Bu süreçte delillerin toplanması, akıllı mobil cihazlar aracılığı ile yapılır. Uzaktan otomatik kimlik tespiti: Bu yöntemde gerçek zamanlı etkileşim olmaksızın yazılım sistemleri tarafından otomatik olarak bir kimlik tespiti yapılmaktadır. Elektronik tanımlama araçları ile kimlik tespiti: Bu

yöntemde kimlik doğrulama süreçleri elektronik tanımlama süreçlerine bağlı olarak iletilebilir. Sertifika tabanlı kimlik tespiti: Bu yöntemde elektronik imzalar gibi bir güvenilir sertifikaya sahip sistemler kullanılır ve kullanıcı bilgileri o sertifikadan çekilir. Ayrıca elektronik imzalar, günlerce sürebilen bir süreci tek bir oturuma sığdırarak zamandan ve enerjiden tasarruf sağlar (Dağıdır Çakan vd., 2022). Kombine yöntemler: Uzaktan kimlik doğrulama yöntemleri, bir diğeri ile birlikte de kullanılabilmektedir. Bu şekilde elde edilen çoklu kullanımlar kombine yöntemlere tabidir.

Uzaktan kimlik tespitinin yapılmasını sağlayan bu yöntemler, bankaların veri tabanlarında yer alan müşteri bilgilerinde bulunan yüz görüntüsü ve ses gibi biyometrik kişisel verilerin müşteri temsilcileri ve çeşitli yazılımlar aracılığı ile teyit edilerek uzaktan yürütülen ve banka müşterilerinin finansal hizmet almalarını sağlayan sistemlerden oluşmaktadır. Bu sistem içerisinde farklı teknolojilerin kullanımı mevcuttur. Bu teknolojiler aşağıdaki gibidir:

Parmak İzi Teknolojisi: Parmak izi teknolojisi, cep telefonlarının güvenliğini artırmak için kullanılabilen ve aynı zamanda cep telefonu kullanıcılarına son derece kolaylık sağlayan bir teknolojidir (Gao vd., 2014). Bu teknoloji kullanıcılarını parmak izlerinden tespit etmektedir. El Kimliği Teknolojisi: Bu teknoloji, avuç içi damarlarının benzersiz bir haritasını çıkarabilir ve kızılötesi sinyallerin kişinin hemoglobinine emilme biçimine göre kullanıcılarını tanımlayabilir (Zadeh ve Barati, 2019). İris Tarayıcı: Iris desenleri kişiye özel ve kopyalanması neredeyse imkânsız olduğundan iris kimlik doğrulama teknolojisi, elektronik cihazları güvende tutmanın ve bilgileri gizli tutmanın en güvenli yollarından biridir. Ancak belirtmek gerekir ki parlak ışık altında veya kullanıcıların güneş gözlüğü takmaları gibi durumlarda tarayıcının performansı zayıflayabilmektedir (Zadeh ve Barati, 2019). Yüz Tanıma Teknolojisi: Bu teknoloji (Face ID) tasarlanırken şapkalar, eşarplar, gözlükler, kontakt lensler ve birçok farklı güneş gözlüğü ile uyumlu hale getirilmiştir. Dahası iç mekânlarda, dış mekânlarda ve hatta karanlık ortamlarda bile kullanılabilecek şekilde tasarlanmıştır (Apple, 2023). Biyometrik Kimlik Doğrulama: Biyometrik kimlik doğrulama veya kısaca biyometri, bir bireyin yüz, parmak izi, el geometrisi, iris, tuş vuruşu, imza, ses vb. gibi geleneksel kimlik doğrulama yöntemlerine göre birçok avantaj sunar. Biyometrik özellikler unutulamaz veya kaybedilemez, bu nedenle şifreler gibi unutulma veya kaybolma riski yoktur. Biyometrik özelliklerin kopyalanması, paylaşılması ve dağıtılması zordur, bu nedenle şifrelerin ortaya çıkmasına benzer riskler taşımamaktadır. Kimliği doğrulanan kişinin, kimlik doğrulama sırasında hazır bulunması gerektiği için, dolandırıcılık yapan kullanıcılar şifreleri paylaştıklarını inkâr edemez. Ancak biyometri oluşturmak daha zor olabilir. Bu

durum ise daha fazla zaman, para, deneyim ve erişim ayrıcalıkları gerektirir. Ayrıca, bir kullanıcının biyometrik özellikleri kullanarak dijital içeriğe eriştiğini reddetmesi pek olası değildir (Jain vd., 2006).

Bankacılıkta kullanılan uzaktan kimlik tespiti yöntemleri, ülkelerin kendi yasa ve kanunlarına dayalı olarak farklılık göstermektedir. Bu bağlamda bir sonraki bölümde dünyadaki örnekler ve Türkiye'deki durum ele alınmıştır.

i) Dünyada Bankacılıkta Kullanılan Uzaktan Kimlik Tespiti YöntemleriDünya çapında bankacılıkta kullanılan uzaktan kimlik tespiti yöntemleri, kullanıcıların kimliklerini doğrulamayı ve güvenli bir şekilde finansal işlemlerini gerçekleştirmeyi amaçlayan teknolojilerdir. Bu teknolojiler ülkelere ve bölgelere göre değişiklik göstermektedir.

Dünyadaki en büyük biyometrik şablon deposu olan Hindistan Benzersiz Kimlik Kurumu (UIDAI), 2009'dan bu yana 1 milyardan fazla müşteriye ait biyometrik veriyi toplamıştır (Banerjee, 2015). Ayrıca Hindistan'da benimsenen Aadhaar tabanlı kimlik doğrulama sistemi, sosyal yardım gibi hizmetlerden faydalanmayı kolaylaştırdığı için yaygın olarak kullanılmaktadır. Günde ortalama 70 milyon işlem yapılmaktadır (Teknomers, 2023). Ancak bu uygulamalar biyometrik verilerin yanında parmak izi uygulamasının dâhil olduğu bir denetleme mekanizmasına sahiptir. Bazı çevrim içi bankalar, kişisel kimlik doğrulaması için sağlam ve güvenli bir biyometrik teknoloji mekanizması kullanarak sistemlerini korumak için ekstra önlemler almaktadır (Jama vd., 2019).

Rusya'da Merkez Bankasının inisiyatifi ile ülkenin finans ve kredi sisteminin etkinliğini ve tüketici memnuniyet düzeyini artırmak amacı ile bankaların müşterilerin uzaktan biyometrik kimlik tanımlaması yapmalarını sağlayan bir kurum kurulmuştur (Ezrokh, 2020).

İsveç'te bankacılık hizmetlerini görüntülü kimlik onayı ile gerçekleştiren bir platform geliştirilmiştir. Bu sisteme göre müşteri dijital kimliğini BankID uygulaması aracılığıyla kullanır. Dijital kimlik kartı bu uygulamada görüntülenir ve kullanıcıdan onay istenir. Dijital kimlik kartının görüntüledikleri müşterinin görüntüsü, ismi, kimlik bilgileri, güvenlik ayrıntıları, dijital kimlik kartını doğrulayan bir mobil karekoddur. Son aşamada bankalar ya da konu olan şirketler müşterinin uygulamasında yer alan kodu tarayarak onay alır. İsveç'te görsel doğrulamada kullanılan güvenlik ayrıntıları şu şekildedir: Müşteri, görüntüsü oluştuktan sonra ekrandaki bir düğmeye basmaya yönlendirilir.

Bu aşamada düğmenin bulunduğu yerdeki görüntü bulanıklaşır ve bir ses duyulur. Doğrulayıcı, kullandığı yazılımlar ile sahte bir hareketsiz görüntü kullanılıp kullanılmadığını denetler (Bankid, 2023). İsveç, Norveç, Finlandiya ve Danimarka'da elektronik kimlik belirleme sistemlerinin kullanımında iyi örnekler bulunmaktadır. Örneğin burada bankacılık çözümleri bölgeye hâkimdir ve milyonlarca kullanıcının erişimine açıktır (Sova vd., 2021).

Avusturya Finansal Piyasa Otoritesi (FMA), görüntülü kimlik tespiti yapma prosedürünü Ocak 2017'de kabul etmiştir. Buna göre müşteri kendi görüntüsünün yanında, kimliğinin ön ve arka yüzüne ait çözünürlüğü yüksek bir görseli iletmekle yükümlüdür (FMA, 2017). İsviçre Finansal Piyasa Denetleme Otoritesi (FINMA), bankalara bireysel olarak yapılan müşteri ziyaretlerinin yerini tutacak bir çevrim içi sistemi ilk kez 2016'da tanıtmıştır. Buna göre bir telekonferans köprüsü aracılığı ile banka çalışanları ve banka müşterileri arasında iletişim sağlanmaktadır. Banka müşterilerinden talep edilen, banka temsilcileri tarafından yöneltilen çeşitli soruları yanıtlamaları, kimlik belgelerini ve diğer belgeleri sunmalarıdır (FINMA, 2016).

Güney Kore'de kullanılan sistem, müşterilerin hâlihazırda bir hesap sahibi olmaları koşulu ile görüntülü kimlik onayı işlemlerine izin vermektedir. Ayrıca diğer ülkelerden farklı olarak kullandıkları blok zinciri teknolojisi ile çalınan kişisel verilerin kullanımını önleyebilmektedir (Etnews, 2018). Çin'deki Kamu Güvenliği Bakanlığı, yüz tanıma teknolojisini ülkedeki diğer sistemlere entegre ederek akıllı telefonlar ile kimlik doğrulamasının önünü açmıştır (Khan, 2018). Pakistan, herhangi bir banka şubesini ziyaret etmeye gerek kalmaksızın müşteri kabulü sağlayan ve %100 yüz biyometrisi kullanan bir sistemden faydalanmaktadır (Ullah, 2022).
Endonezya menşeli bir banka olan Mayapada, OneConnect ile yapmış olduğu ortaklıkta banka müşterilerinin kimliklerinin gerçekliklerinin doğrulanmasında yapay zekâ ve güçlendirilmiş elektronik müşteri tanı teknolojisi kullanacaktır. Ayrıca sahte saldırıların önlenmesinde yüz canlılığı algılama teknolojisi uygulanmaktadır (OneConnect, 2021).

Özbekistan'da uzaktan bankacılık hizmetlerinin kullanımı yaygın değildir. Çünkü banka müşterilerinin finansal okuryazarlığı düşüktür. Ayrıca ülke genelinde internet hız ve kalitesinin düşüklüğü de bu durumda etkilidir (Mamadiyarov, 2020). Ayrıca nüfus ve bankacılık hizmetlerinin uzaktan organizasyonunda birçok problemle karşılaşıldığından bankaların tüm hizmetleri müşterilere iletilememiştir (Mamadiyarov, 2021).

Bu bilgiler ışığında ülkelere göre bankacılıkta kullanılan uzaktan kimlik teşhisi yöntemleri, Tablo 1'de gösterilmektedir.

***Tablo 1**. Ülkelere göre bankacılıkta kullanılan uzaktan kimlik teşhisi yöntemleri*

Uzaktan kimlik teşhisi yöntemleri	**Ülkeler**
Video destekli operatör ile kimlik tespiti	Almanya, Avustralya, Belçika, Bulgaristan, Endonezya, Fransa, Hindistan, İsviçre, İtalya, Güney Kore, Lüksemburg, Pakistan, Polonya, Portekiz, Türkiye, Yunanistan
Uzaktan otomatik kimlik tespiti	Bulgaristan, Estonya, Yunanistan, Norveç
Kombine yöntemler ile kimlik tespiti	Fransa, İspanya
Diğer	Avusturya, Finlandiya, Letonya, Litvanya, Hollanda, Romanya, İsveç, Birleşik Krallık

Kaynak: Yazar tarafından derlenmiştir.

ii) Türkiye'de Bankacılıkta Kullanılan Uzaktan Kimlik Tespiti Yöntemleri

Türkiye'deki bankalarda kullanılan uzaktan kimlik tespitinin geçmişi uzaktan yapılan sözleşmelerin önünü açan kanuna dayanmaktadır. 26.06.2020 tarihli ve 31167 sayılı Resmî Gazete'de yayımlanan 7247 sayılı Kanun'un 10. maddesinde belirtildiği üzere, "Sözleşme, yazılı olarak veya elektronik ortamda kurulur. Elektronik ortamda kurulacak sözleşmelerde, başvuru sahibinin kimliğinin doğrulanmasına imkân verecek şekilde, Kurum tarafından belirlenecek yöntemler kullanılır ve bunlara ilişkin usul ve esaslar Kurum tarafından belirlenir." (RG, 26.06.2020-31167). Bu madde ile sözleşmelerde elektronik ortamda yapılan kimlik doğrulamasının kullanılmasının önü açılmıştır. Sonrasında 24.02.2021 tarihli ve 31405 sayılı Resmî Gazete'de yayımlanan 3580 sayılı Cumhurbaşkanı Kararı Madde 5'te belirtilen ve yönetmeliğe eklenecek olan 6/A maddesinde gerçek kişilerde uzaktan kimlik tespitinde müşteriler ile yüz yüze gelinmeksizin kimlik doğrulanmasına imkân verilen uzaktan kimlik tespiti yöntemlerinin kullanılabileceği belirtilmiştir (RG, 24.02.2021-31405 (Mükerrer)). Bu karar ile ise, banka temsilcileri ve müşteriler arasında yüz yüze gelmeksizin bir iletişim kurulabileceği ve bu şekilde kimlik doğrulaması yapılabileceği açığa çıkmıştır.

Bu düzenlemeler doğrultusunda 01.04.2021 tarihli Resmi Gazete'de yayımlanan "Bankalar Tarafından Kullanılan Uzaktan Kimlik Doğrulama Yöntemleri ve Elektronik Ortamda Sözleşme Kurma Yönetmeliği" ile BDDK kendisine kanun ile verilen düzenleme yapma yetkisini kullanarak bankaların uzaktan müşteri

edinme ve sözleşme kurmasına imkân sağlamıştır. BDDK bu Yönetmelik ile uzaktan müşteri edinmenin şekli ve teknik kısımlarına da yer vermiştir. Böylece bankaların uzun zamandır beklediği müşteri kimlik tespitini uzaktan yapabilme konusundaki bir eşik, yenilikçi bir sistem kullanılarak aşılmıştır. Bankalar bu düzenlemeyle müşteri temsilcisi ile kişinin, fiziksel olarak aynı ortamda bulunmasına gerek olmadan, çevrim içi olarak görüntülü görüşmesi ve birbiriyle iletişim kurarak müşteri edinebilme imkânına kavuşmuş ilave olarak bu görüşmenin devamında sözleşme kurabilme imkânını da edinebilmiştir. Türkiye'de bankacılıkta kullanılan uzaktan kimlik tespiti öncelikle gerçek kişiler, gerçek kişi ticari işletmeler için başlamış ve 25 Mayıs 2023 tarih ve 32201 sayılı Resmî Gazete'de Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik ile de ticaret siciline kayıtlı tüzel kişileri de kapsayacak şekilde genişletilmiştir.

Söz konusu düzenleme uyarınca uzaktan müşteri edinim sürecin kişi tarafından başlatılması, bilgi teknolojileri tarafından uygulanan kontroller ile devam ettirilmesi ve müşteri temsilcisi tarafından yapılacak onaylama ve ek kontroller ile tamamlanması şeklinde tasarlanmıştır. Edinim süreci özetle aşağıdaki gibidir.

- Önceden doldurulmuş bir elektronik form aracılığıyla, uzaktan kimlik tespiti sürecinin işletildiği banka uygulaması üzerinden kişinin başvurusu alınır, bu başvuru işlemi görüntülü görüşme öncesinde gerçekleştirilir.
- Suistimal olasılığını azaltmak için, uzaktan kimlik tespiti işlemleri için belirli bir müşteri temsilcisine atanacak kişilerin tahmin edilebilir durumları önlemek amacıyla uygun mekanizmalar sağlanır.
- Görüntülü görüşme öncesinde müşteri temsilcisi tarafından sorulacak asgari sorular belirlenir ve bu soruların sırası ve türü değişebilir.
- Görüntülü görüşme aşaması, uzaktan kimlik tespiti sürecinde gerçek zamanlı ve kesintisiz olarak yapılır. Müşteri temsilcisi ile kişi arasındaki görsel ve işitsel iletişim yeterli düzeyde gizlilik ve bütünlük sağlar. Bu amaçla, görüşme uçtan uca güvenli iletişimle gerçekleştirilir.
- Uzaktan kimlik tespiti sürecinde, kişiye yalnızca kimlik tespiti işlemi için geçerli olan merkezi olarak üretilmiş SMS OTP (Tek Kullanımlık Şifre) iletilir. Kişi, iletilen SMS OTP'yi çevrim içi olarak uygulama arayüzü üzerinden geri gönderir.

Uzaktan kimlik tespiti sürecinde beyaz ışık altında görsel olarak ayırt edilebilen güvenlik ögelerine, fotoğraf ve imzaya sahip olan kimlik belgesi kullanılır. Bu kimlik belgesi şu an için yeni TC kimlik kartıdır. Bu kimlik belgesinin doğrulanması, bu sürecin en önemli risk yönetim sürecidir.

- Yakın Alan İletişimi (NFC Teknolojisi) Kullanılan Yöntem

Yakın alan iletişimi (NFC) kullanarak, kimlik belgesinin yongasındaki kimlik bilgilerinin doğrulanması, kimlik belgesi üzerindeki bilgilerle kişinin kimliğinin tespit edilmesini mümkün kılar. Söz konusu doğrulama;

• Kimlik belgesi, belgenin verildiği yetkili makam tarafından verilmiş olup, belgenin temassız yongasındaki bilgilerin değiştirilmediği şekilde kullanılır.
• Kimlik belgesinin temassız yongası üzerindeki anahtarların kopyalanarak oluşturulmadığı kontrol edilerek gerçekleştirilir.

Kimlik tespit aşamasına ek olarak uzaktan kimlik tespitinin görüntülü görüşme aşamasında kişinin canlılığını tespit edici yöntemler kullanılır. Her geçen gün yeni teknolojiler ile bu oran yükseltilerek sistem daha güvenli hale getirilmeye çalışılmaktadır (iBeta, 2023).

- Yakın Alan İletişimi (NFC Teknolojisi) Kullanılmayan Yöntem

Yakın alan iletişimi kullanılmayan yöntem güvenlik açısından daha zayıf bir koruma sağlamaktadır. NFC teknolojisinin sağladığı aktif ve pasif doğrulamadan muaf olunduğu gibi yüz tanıma için kullanılan fotoğrafa kimlik yongasından elde edilen fotoğraf olmayıp kimlikte görsel olarak var olan fotoğraf ile yapılmaktadır. NFC teknolojisinin korumasının eksikliğini düzenleyici otorite, aşağıdaki ilave kontrollerle gidermeye çalışmıştır.

• Kimlik belgesindeki dört görsel güvenlik unsuru, şekil ve içerik açısından doğrulanır.
• Sadece görsel güvenlik unsurları doğrulandığında, bir banka kişinin kendi hesabından yapılan ilk finansal işlemi, müşterinin tanınmasıyla ilgili kuralların uygulandığı başka bir bankadaki kişiyle sürekli iş ilişkisi kurmadan önce zorunlu kılar.
• Kimlik belgesindeki fotoğrafın biyometrik karşılaştırması yapılır.

Yukarıda yapılan kontroller sonrası müşteri temsilcisi tarafından görüntülü görüşme aşamasında ilave kontroller yapılarak süreç tamamlanır.

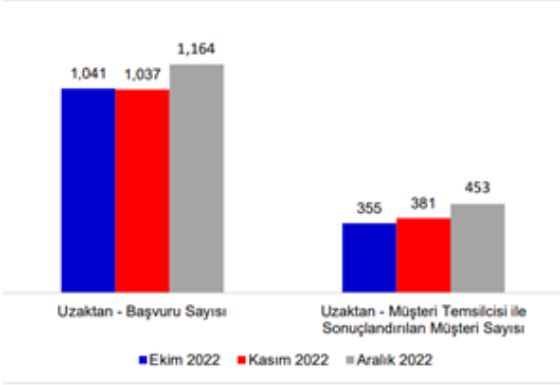
NFC teknolojisi kullanılmayan süreçlerde ilave kontroller konulsa da dahi NFC kullanılan süreçler daha güvenlidir. Uzaktan müşteri ediniminde temel alınan yeni TC kimlik kartının sağladığı bu teknik imkândan yararlanılmayan ancak bankaların müşteri teminine yardımcı olmak amacı ile oluşturulan NFC'siz sürecin dijital bankacılık hedeflemesinde zayıf bir alan olarak görülmektedir.

Yönetmelik, "Banka sahte yüz teknolojisine dair riskleri önlemeye yönelik

ilave tedbirler alır" hükmünü içermektedir. Ancak cari olarak ülkemizdeki hiçbir banka Deep Fake teknolojisinin yaratacağı tahrifata hazır değildir. Deep Fake teknolojisinin bazı kötü niyetli kişiler tarafından uzaktan müşteri edinim sürecinde ve video bankacılığı görüntülü görüşme aşamasında bankayı dolandırmak amaçlı olarak kullanılma ihtimali kuvvetle muhtemeldir. İşbu yüzden bankalar yapay zekânın video bankacılık sürecinde kullanarak Deep Fake'nin yaratacağı tahrifatı başka bir yapay zekâ ile tespit ederek kendilerini ve müşterilerini finansal ve reputasyonel risklere karşı korumaya şimdiden başlamalıdır.

Türkiye Bankalar Birliği (TBB)'nin Aralık 2022 dönemi itibarıyla 16 banka verisinden oluşan tablosuna aşağıda yer verilmiştir.

Tablo 2: Uzaktan Müşteri Edinimi (Bin Kişi)



Kaynak: (TBB, 2023)

Aralık 2022 itibarıyla uzaktan başvuru sayısı 1 milyon 164 bin olmuştur. Müşteri temsilcisi ile sonuçlandırılan uzaktan müşteri edinimi 453 bindir. Bankaların video bankacılık yolu ile yapılan başvurulan sadece %39'unun başarılı olduğu görülmektedir. Başarısız olunma sebepleri ise teknolojik nedenlere (akıllı cihazların işletim sisteminin süreci desteklememesi, teknolojik okuryazarlığın eksik olması, NFC'nin aktive edilip kullanılamaması vs.)dayanmaktadır. Tablo 2'de görüldüğü üzere, uzaktan kimlik tespiti yönteminin kabul gördüğü ve giderek daha fazla insanın bu yöntemi tercih ettiği görülmektedir.
Mayıs 2021'den Aralık 2022'e kadarki süreçte, uzaktan müşteri edinimi başvuruları genel olarak artan eğilimdedir (Tablo 3). Bu amaçla yapılan ve sonuçlanan başvuru adetlerinde ve kabul oranlarında artış gözlenmektedir. Mayıs 2021'de 278 bin olan başvurunun %25'i müşteri edinimi ile sonuçlanır

iken; Aralık 2022'de başvuru sayısı 1 milyon 164 bini geçmiş ve başvurunun müşteri edinime dönüşüm oranı da %39'a yükselmiştir.

Şekil 3: Bankaların Uzaktan Müşteri Edinimi (Bin Kişi)

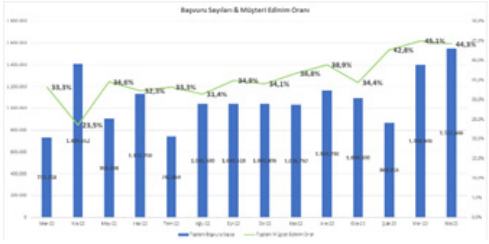
	Uzaktan - Başvuru Sayısı	Uzaktan - Müşteri Temsilcisi ile Sonuçlandırılan Müşteri Sayısı
Mayıs 2021	278,053	69,760
Haziran 2021	228,303	63,829
Temmuz 2021	234,948	61,092
Ağustos 2021	273,959	73,712
Eylül 2021	370,838	100,476
Ekim 2021	467,139	117,233
Kasım 2021	686,183	137,787
Aralık 2021	537,821	147,615
Ocak 2022	406,629	113,692
Şubat 2022	454,657	136,212
Mart 2022	733,258	244,015
Nisan 2022	1,409,652	331,771
Mayıs 2022	906,998	313,497
Haziran 2022	1,132,700	365,542
Temmuz 2022	742,869	247,234
Ağustos 2022	1,041,907	327,647
Eylül 2022	1,043,518	364,703
Ekim 2022	1,041,496	355,178
Kasım 2022	1,036,792	381,051
Aralık 2022	1,164,296	452,952

** Gerçek müşteri edinimleridir.*

Kaynak: (TBB, 2021)

Gerek başvuru adetindeki artışın gerekse de müşteri edinimindeki oransal artışın sebeplerini; -uzaktan müşteri edinim sürecinin daha bilinir olmasına, teknolojik okuryazarlığın artmasına ve sisteme uyumlu akıllı cihazların artmasına bağlanabilir. Öyle ki Nisan 2023 itibarı ile başvuru adeti 1,5 milyonu aşmış ve toplam başvuruların müşteriye dönüşüm oranı %44'ü geçmiştir (Şekil 4).

Şekil 4: Uzaktan Bankacılık Başvuru ve Müşteri Edinimi İstatistikleri



Kaynak: (Türedi, 2023)

Bankacılıkta Kullanılan Uzaktan Kimlik Tespiti Yöntemlerinin Riskleri

Uzaktan müşteri edinim süreci dijital finansal sistemde sadece uzaktan müşteri edinimi amacı ile kullanılmamakta aynı zamanda elektronik bankacılık kanallarının kullanılması için gerekli olan iki faktörlü doğrulama unsurlarının belirlenmesi ve değiştirilmesi ile müşterilerin finansal ve finansal olmayan işlemlerinin gerçekleştirilmesinde de kullanılmaktadır. İşbu yüzden uzaktan kimlik tespit yönteminde görüntülü bankacılık kanalının taşıdığı riskleri bilmek ve suistimale kapalı bir görüntülü bankacılık hizmetinin müşterilerin erişimine sunmak dijital finansal sistemin daha güvenilir çalışmasını sağlayarak dijital bankacılığın gelişmesine katkı sağlayacaktır.

i) Operasyonel Riskler

Bankacılıkta kullanılan uzaktan kimlik tespiti yöntemleri, müşterilerin bankacılık işlemlerini kolaylaştırırken aynı zamanda operasyonel riskler de içerir. Bu riskler teknik ekipman eksikliği, hatalı işlemler, güvenlik zafiyetleri, yetersiz kontroller, müşteri reddi, insan hatası gibi riskleri içerir.

- Uzaktan kimlik doğrulama süreçlerinin karmaşıklığı, müşterilerin süreci anlamasını engeller ve süreci dolandırıcılığa açık hale getirir. Bu risk, müşteri kaybına da yol açabilir. Ayrıca bu süreçte kullanılan mobil uygulamanın kullanıcı dostu olması da önemlidir (Dağıdır Çakan vd., 2022). Müşteri memnuniyetinin her koşulda sağlanması gereklidir. Ancak uzaktan kimlik tespiti süreçleri, banka müşterileri için zaman alıcı ve karmaşık süreçler içerebileceğinden onları sıkabilmektedir. Gereksiz kontrol noktaları süreci güvenli kılar iken kullanıcı dostu olmayan bir ortam yaratması nedeni ile de müşteri kaybının ana gerekçesi olabilmektedir.
- Uzaktan kimlik tespiti yöntemlerini müteakip işlemlerin yüz yüze gerçekleşmesi durumunda yüz yüze bir biçimde imza alınmasının gerekliliği, dijital dönüşüm süreci ve alınan kararların vizyonu ile çelişmektedir. Bu sebeple geleneksel bankalar için dezavantajlı koşullar oluşması riski meydana gelmektedir (Balkan, 2021).
- Uzaktan kimlik tespiti onayı bir müşteri temsilcisi aracılığı ile yapıldığında sürecin onaylama aşamasının bir insan inisiyatifinde yer alması sebebi ile bu denetim mekanizması bilinçli ya da bilinçsiz insan hatası riski içermektedir.
- Elektronik imzalar ile yapılan kimlik doğrulama süreçlerinde nitelikli elektronik imzaların mühür ve sertifikaları birbirinden farklı Nitelikli Güven Hizmet Sağlayıcısı (QRSP) tarafından düzenlendiğinde imzaların kullanımı mümkün olmaz. Bu sebeple sertifika yayıncılarının aynı olması gerekmektedir. Bu da süreçte aksamalara sebep olur (ENISA, 2021).
- Uzaktan kimlik belirleme süreçlerinde taraflar birbirleri ile yüz yüze görüşme

yapmadıklarından, tüketicinin tanınmasını sağlayabilecek yöntemler yeterince güvenli olmadığından sınırlıdır (Dağıdır Çakan vd., 2022). İş ve meslek bilgisi ile gelirin kaynağı konusunda sadece beyan ile yetinilmekte ve doğrulanması mümkün olamamaktadır. Geleneksel bankacılık yerinde ziyaret güvencesinden mahrum bir yapıdır. İşbu hali ile suç gelirlerinin aklanması ve terörün finansmanının önlenmesi tedbirleri karşısında geleneksel bankacılığa göre daha zayıf bir ortam sunmaktadır.

- Kişisel Verilerin Korunması Kanunu (KVKK), Türkiye'deki bankacılık sektöründe kişisel verilerin korunmasını ve işlenmesini düzenleyen önemli bir yasal düzenlemedir. Uzaktan kimlik tespiti yöntemleri, KVKK'nın etkisi altında olduğu için veri güvenilirliği, veri işleme amaçlarına uyum, veri saklama süresi, veri paylaşımı, müşteri bilinçlendirme, denetim ve hukuki uyum süreçleri olmak üzere birçok konuda riskler ortaya çıkabilir.
- Teknolojik okuryazarlığın düşük olması nedeni ile süreç tamamlanamamakta, kaynak israfına neden olunmaktadır.
- Kullanılan sistemler genellikle bankalar tarafından dışardan alınan hizmetler olduğundan bankalar dışa bağımlı durumdadır. Bu dışa bağımlılık ile hizmet sağlayan firmaların sayıca azlığı sürdürülebilirlik açısından bankaların önündeki en önemli operasyonel risk olarak durmaktadır.

ii) Teknik Riskler

Uzaktan kimlik tespiti yöntemleri, bankacılık ve diğer sektörlerde kimlik doğrulama süreçlerinin dijitalleştirilmesi ve kolaylaştırılması için kullanılan önemli araçlardır. Ancak, bu yöntemlerin kullanımıyla birlikte bazı teknik riskler ortaya çıkabilmektedir.

- Bilgisayar programları ile denetlenen kimlik bilgileri %100 doğruluğa sahip değildir. %0,1 ihtimalle de olsa hatalı çıkarım yapılması ihtimali mevcuttur. Örneğin Amazon'un yüz tanıma sisteminde bilgisayarlar, platforma yüklenen 25.000 suçlu fotoğrafı arasından 28 tanesinin mevcut kongre üyelerinden biri olduğu sonucuna varmıştır (Hollister, 2018).
- Kimlik doğrulaması yapılırken farklı ortamlar ve farklı ışıklar kullanılır. Yeterli ışığa sahip olmayan ortamlarda yapılan kimlik doğrulaması, eksik bilgilerin istismar edilebilmesi riskini taşımaktadır. Örneğin kimliklerin kimi özellikleri yalnızca UV ışığında görülebilir. Bu sebeple bazı verilerin işlenmesi konusu probleme yol açabilir.
- Süreçlerin yürütülmesinde kullanılan yazılımların kullanışlılığı önemlidir. Yazılımların uygun biçimde test edilmesi, geliştiricilerin sunduğu garantiler vb. konularda yeterli şeffaflığın olmayışı, bankalar ve potansiyel müşteriler açısından proje güvenini azaltıcı etki sağlamaktadır (Ezrokh, 2020).

• Videolu görüşmelere dair kanıtların saklanması hususu da önem taşımaktadır. Bazı bankalar bu belgeleri dâhili olarak saklarken bazıları dâhili ve harici olmak üzere iki türlü depolama biçimi ile saklamışlardır (ENISA, 2021). Bu depolama yöntemlerinin de kendilerine ait riskler taşıdıkları bilinmektedir.

iii) Güvenlik Riskleri

Uzaktan kimlik tespiti yöntemlerinin yaygınlaşmasıyla birlikte, güvenlik riskleri de artmaktadır. Bu yöntemlerde kullanılan dijital platformlar, kişisel ve hassas verilerin paylaşılmasını gerektirir. Mevcut kimlik doğrulama yöntemleri, kullanıcı odaklı olmadığından kullanıcıların güvenliğini tehlikeye atmaktadır (Jama vd., 2019).

• 15.03.2020 tarihli ve 31069 sayılı Resmî Gazete'de bu hassas veriler "Kimlik doğrulamada kullanılan veriler başta olmak üzere; müşteriye ait olan, çeşitli sebeplerle bankaca muhafaza edilen ve üçüncü kişilerce ele geçirilmesi halinde, bu kişilerin müşteri olan kişilerle ayırt edilebilme mekanizmalarının zarar göreceği ve dolandırıcılık ya da müşteriler adına sahte işlem yapılmasına imkân verebilecek nitelikteki veriler" olarak tanımlanmıştır (RG, 15.03.2020 -31069). Bu bağlamda uzaktan kimlik tespiti yöntemlerinin yaşatacağı herhangi bir sızma olayında kişilere ait hassas bilgilerin de çeşitli sahte işlemler için kullanılabileceği riski açıktır.

• Bankalar tarafından oluşturulan biyometrik müşteri tanımlama veri tabanlarının siber güvenlikleri şüphelidir (Ezrokh, 2020). Mobil bankacılıkta meydana gelen yazılım güvenliği açıkları, kullanıcıların bilgisayar korsanları tarafından saldırıya uğrayabilecekleri ve varlıklarının çalınabileceği endişelerine yol açmaktadır (Zadeh ve Barati, 2019). Kuruluşlar, artan sayıda potansiyel saldırılara maruz kalmaktadır ve bu saldırılar arasında "Kimlik Avı, İstenmeyen Posta, Casus Yazılım ve Kötü Amaçlı Yazılımlar" gibi tehditler yer almaktadır (Jama vd., 2019).

• Uzaktan otomatik kimlik tespiti yöntemlerinde çeşitli yazılım saldırıları riski mevcuttur. Örneğin bir DeepFake (sahte görüntü çakıştırma) saldırısına karşı bankalar son derece zayıf durumdadır (Aydin vd., 2023).

• Biyometrik sahtekârlık ya da sahte parmak izi kullanılabilir (ENISA, 2021).

• Son olarak verilerin yer aldığı veri tabanlarına yetkisiz erişim riski, kullanıcıların ve bankaların güvenliklerine zarar verebilir.

iv) İtibar Riskleri

Uzaktan kimlik tespiti yöntemlerinin kullanımı, tüm süreçleriyle bankaların itibar riskleriyle karşılaşabileceği önemli bir alanı kapsamaktadır. Bankalar bazı riskler sebebi ile itibarlarını ciddi şekilde zedeleme potansiyeline sahiptir.

• Bir müşterinin kimliği yanlışlıkla doğrulanırsa veya bir güvenlik açığı nedeniyle müşteri verileri kaybolursa, müşterilerin güveni sarsılabilir ve bankanın itibarı zarar görebilir. Bu durum, müşteri kaybı, itibar kaybı ve hukuki sonuçlar gibi olumsuz etkilerle sonuçlanabilir.
• Sınırlı kaynağa sahip yerel bankaların dijital gelişmeleri yakalayamaması sebebi ile rekabet edebilme ihtimallerinin azalması riski söz konusudur.
• Sadece Dijital Bankacılık lisansı olan bankalar için bu husus, varlık-yokluk sorunu haline gelebilecektir. Dijital güvenliğini koruyamamış bir dijital bankanın sistemden çıkması günler içinde olabilecektir. Öyle ki sadece likidite riski ABD'nin 14. büyük bankası olan First Republic Bank, JP Morgan'a devredilmek zorunda kalınmıştır.

v) Yasal Riskler

Uzaktan kimlik tespiti yöntemlerinin kullanımıyla birlikte, yasal riskler de dikkate alınması gereken önemli bir konudur.

• Bu süreçler, kişisel verilerin paylaşımını içerdiğinden verilerin yetkisiz kullanılması riski söz konusudur.
• Bazı ülkeler, bankaların kendi içlerinde geliştirmiş olduğu uzaktan kimlik tespiti yöntemlerinin kullanılması için gerekli yasal düzenlemelere sahip olmayabilir. Aynı zamanda bu kullanımlar çeşitli düzenlemeler ile sınırlandırılmış olabilir. Bu sebeple bankaların farklı yasal düzenlemelere uymak zorunda kaldığı ve uluslararası operasyonlarda dikkate alması gereken bir risk ortaya çıkar.
• Uzaktan kimlik tespiti yapılırken kullanılan biyometrik belirleme işlemleri video kaydı ile saklanmamaktadır (Ezrokh, 2020). Bu durumda yaşanacak sahtekârlık girişimleri sonrasında meydana gelen dava süreçlerinde mahkeme için bir kanıt oluşturmak zorlaşmaktadır. Bu sebeple verilerin kaydedilmemesinin getirmiş olduğu bir risk söz konusudur.
• Teknolojik ilerlemeler ve uygulama deneyimleri göz önünde bulundurularak, uzaktan kimlik tespit süreci, güvenlik ihlallerinin tespit edilmesi veya gerçekleşmesi durumunda, ilgili mevzuatta değişiklik yapılması, bankanın potansiyel dolandırıcılık veya sahtecilik eylemlerinden haberdar olması, kullanılan uzaktan kimlik tespiti yönteminin zayıflıklarının ortaya çıkması gibi durumlarla ilgili olarak da gözden geçirilir ve güncellenir. Yeterli güvenlik önlemlerinin alınmaması veya yetersiz bulunması, idari yaptırım riski oluşturabilir.

vi) Finansal Riskler

Yenilikçi yaklaşımların beraberinde getirdiği finansal riskler de göz ardı edilemez.

• İlk yatırım maliyeti, bankacılık süreçlerinin dijitalleşmesi için önemli bir gider kaynağıdır. Süreçlerin yeni olması nedeni ile tecrübe alanının sektördeki yetersizliği birlikte çalışacağı harici firmaları seçiminde bankaları hataya yöneltebilecektir. Bu durum finansal risklere sebep olabilecektir.
• Kullanılacak yazılımın teknolojik altyapının gelişmişliğine bağlı olarak ortaya çıkan maliyet, bankalar için maddi risk yaratabilmektedir. Çoğunca kullanılan sistemler bankalar tarafından dışarıdan alınan outsource hizmetler olduğundan bankaların maliyet belirleyici yönü zayıf kalmaktadır.
• Uzaktan kimlik tespiti uygulamaları, bankalara aylık olarak bağlantı maliyeti çıkarmaktadır (Belov ve Zagumennov, 2019).
• Önceki bölümlerde de ele alınan dolandırıcılık, kimlik hırsızlığı ve diğer güvenlik tehditleri, bankaların ve müşterilerin finansal varlıklarını potansiyel olarak tehlikeye atabilir. Çünkü özellikle internet aracılığı ile gerçekleştirilen işlemler kötü niyetli taraflar için caziptir ve parasal kayıplara neden olabilecek saldırıları çeker (Jama vd., 2019).

Bankacılıkta kullanılan uzaktan kimlik tespiti yöntemlerine ilişkin risklerin sıralandığı özet bilgi, Tablo 2'de ifade edilmiştir.

Tablo 2. Özet bilgi tablosu

Riskler	**Kaynak**
Operasyonel Riskler	Balkan, 2021; ENISA, 2021; Dağıdır Çakan vd., 2022
Teknik Riskler	Velioğlu vd., 2019; Hollister, 2018; Ezrokh, 2020; ENISA, 2021; Sova vd., 2021
Güvenlik Riskleri	Yang, 2010; Sheshasaayee ve Sumathy, 2017; Jama vd., 2019; Zadeh ve Barati, 2019; Ezrokh, 2020; ENISA, 2021
İtibar Riskleri	Ezrokh, 2020; ENISA, 2021; Sova vd., 2021
Yasal Riskler	Balkan, 2021; ENISA, 2021; Indriasari vd., 2022
Finansal Riskler	Belov ve Zagumennov, 2019; Jama vd., 2019; ENISA, 2021; Sova vd., 2021; Surane, 2021

Kaynak: (Yazar tarafından derlenmiştir.)

Risk Yönetimi Planları ve Çözüm Önerileri

Uzaktan kimlik tespiti yöntemlerine ilişkin riskler 6 başlık altında incelenmiş olsa da literatüre göre bu risklerin en çok ele alınanı güvenlik riskleri olmuştur. Bu bölümde güvenlik riskleri başta olmak üzere bazı çözüm önerileri sunulmaktadır. Bankalar ve banka temsilcilerinin perspektifinden bakıldığında, sorumlulara

önemli görevler düşmektedir. Araştırma verilerine göre uzaktan müşteri kabulü prosedürlerinin sağlanması için gerekli olan akıllı telefon ve çipli kimlik gereksinimleri herkesçe karşılanamamaktadır. Bu durumda herkesin erişimini kolaylaştırmak adına erişilemeyen potansiyel müşteriler için bir yönetim planı yapılması gerekmektedir. Ayrıca elektronik tanımlama hizmeti sağlayıcılarının alması gereken bir dizi önlem vardır. Bunlar: kişisel verileri korumak ve kayıp, imha, sızıntı risklerine karşı güvenlik sağlamak için teknik önlemlerin alınmasıdır (Sova vd., 2021). ENISA'nın yapmış olduğu bankacılık araştırmasına dâhil olan bir bankanın müşteri kimliği tanımlamasında bir insan operatörü olmasına rağmen süreçteki risk analizleri teknoloji altyapılı onay mekanizmalarınca yapılmaktadır (ENISA, 2021).

Banka yazılımlarının süreç içerisinde aldığı rol büyüktür. Süreçlerde yaşanan gecikmelerin önlenmesi için iyileştirilmesi gerekmektedir. Böylece zamandan tasarruf sağlanır. Dijital kimlik şemalarının benimsenmesi ile banka müşterileri çevrim içi hizmetler ile ilgili yaşadıkları deneyimde ciddi ve olumlu sonuçlar sağlar ve bu dönüşüm bankalara ve finansal kurumlara değişim için öncü olma fırsatı verir (Sova vd., 2021). Ek olarak, yazılımlarda çeşitli iyileştirmeler yapılabilir (Jama vd., 2019). Uzaktan kimlik tespiti için doğrulama alanları arttırılabilir. Optik okuyucu ile edinilen bilgilerin algoritmik çözümlemesi yapılarak kullanılan kimliğin sahte olma ihtimali azaltılabilir. Barkodların doğrulukları kimlik doğrulama süreçlerine dâhil edilebilir.

Bankaların uzaktan kimlik tespitinin müşteri edinim dışında finansal ve finansal olmayan işlemlerin gerçekleştirilmesinde de kullanıldığı için müşteri edinimde kullanılmayan ancak edinim sonrası müşteri tarafından belirlenen unsurları finansal ve finansal olmayan işlemlerde kimlik tespitinde ek unsur olarak kullanılması uzaktan işlemleri daha güvenli hale getirecektir.

Bir sistemdeki güvenlik açığının istismar edilmesi; bir varlığın gizliliğinin, bütünlüğünün ve kullanılabilirliğinin kaybı dâhil olmak üzere çeşitli sonuçlara neden olabilir. Bankacılık veri merkezleri gibi büyük müşteri verisi depolayan kuruluşlar için, siber fiziksel saldırıları azaltmak için kesin önlemler almak önemlidir. Bu önlemler, güvenlik unsurlarının kolayca ayarlanmasını sağlamalıdır (Jama vd., 2019). Zadeh ve Barati, günümüzde parmak izi biyometrik sensörünün yaygın olarak kullanıldığına rağmen, bu sensörü kullanmaktan memnun değiller ve yüz tanıma biyometrik sensörlerinin daha düşük hata oranı, daha yüksek güvenlik seviyesi ve daha düşük saldırı riski sunması nedeniyle tercih edilmesi gerektiğini önermiştir (Zadeh ve Barati, 2019). Yüz eşleştirme algoritması, derin sinir ağlarındaki en son gelişmeleri kullanarak, en yüksek güvence düzeyiyle

eşleştirme performansını sağlamakta yardımcı olabilir. Bazı bankalar, müşteri kimlik doğrulamasında ekstra bir güvenlik katmanı sağlamak için "Güvenli Anahtar" sistemini kullanmaktadır. Bu sistem, kullanıcı adı ve PIN numarası yerine, kullanıcının oturum açmak için kişisel bir "Güvenli Anahtar" cihazına sahip olmasını gerektirir. Bu sayede internet bankacılığı dolandırıcılığına karşı daha fazla koruma sağlanır (Jama vd., 2019). Mesaj Kimlik Doğrulama Kodları (MAC'ler), veri bütünlüğünü ve kaynağın orijinalliğini sağlamak için kullanılan kriptografik hash fonksiyonlarıdır. Oturum anahtarlarına dayanan bu algoritmalar, verilerin kasıtlı veya kazara değiştirilmesini kontrol etmek için kullanılır (Jama vd., 2019). Velioğlu vd. (2019), internetle aktarılan verilerin güvenli iletimi için hesaba dayalı adresleme (hashing) yöntemini önermiştir. Bu şekilde veriler okunamayacak ve tahmin edilemeyecek şekilde sıfırlanmaktadır (Velioğlu vd., 2019). Uzaktan kimlik doğrulama yöntemleri, kombineli olarak kullanılarak bazı güvenlik risklerinin yönetilmesine katkı sağlayabilir. Örneğin, güvenlik için otomatik süreçler bir insan operatör desteği aracılığı ile güçlendirilebilir (ENISA, 2021). BDDK tarafından yapılan uzaktan müşteri edinim süreci de son aşamada bir insan müdahalesi ile sonlanmaktadır. Sürecin tamamen dijital olması desteklenmemiştir.

Uzaktan bankacılık uygulamalarında kullanılan en yaygın sistem "Tek Seferlik Şifre" (one time password) uygulamasıdır. Bu uygulamada kullanıcıların sistemde kayıtlı olan cep telefonlarına bir şifre gönderilir. Ancak bu sistem, çeşitli saldırılara karşı savunmasızdır. SMS ile gönderilen OTP ya da doğrulama kodunun, aynı mobil cihazda yüklü diğer uygulamalar tarafından okunmayacağı ve bu uygulamalar tarafından üçüncü bir tarafa iletilmeyeceği garanti edilemez. Ayrıca, mobil cihaz üzerindeki "SMS Mesajlaşma Uygulaması" bankanın kontrolünde olmadığı için müşteriye SMS ile gönderilen OTP ya da doğrulama kodunun bütünlüğü veya güvenilirliği konusunda yeterli güvence sağlanamayabilir. Bu nedenle, SMS OTP'nin yönlendirme riskini ortadan kaldırmak için SIM OTP gibi çözüm yöntemleri kullanılabilir (HMB, 2021). SIM OTP ile iletilen mesaj SIM kartın tetiklenmesi ile kullanıcıya gittiği için telefon işletim sistemine gönderilmeden ekranda belirir ve başka bir numaraya yönlendirilemez. Bu durumda SIM kart kopyalama veya numara yönlendirme yoluyla yapılan dolandırıcılık olayını sıfıra indirir. Sheshasaayee ve Sumathy (2017) de bu sorunu önleyebilmek için hafif bir kriptografi ile tek seferlik şifrenin bulunduğu metni gizleyerek sistemi daha güvenli hale getirmeyi hedeflemiştir.

Biyometri, insan vücudu bilgilerini ölçen ve analiz eden bir teknolojidir. Bu bilgiler arasında DNA, parmak izleri, retinalar ve irisler, ses kalıpları, yüz kalıpları ve el ölçümleri gibi veriler bulunur. Bu verilerin analizi, kullanıcının kimliğini

doğrulamak için kullanılır. Biyometrik kimlik doğrulama, kurumsal düzeyde, kamu güvenliği ve elektronik cihaz uygulamalarında yaygın olarak kullanılmaktadır. Biyometrik kullanımı, güvenlik açısından kolaylık sağlamıştır (Jama vd., 2019). Kimlik hırsızlığı riskini azaltmak için, biyometrik veriler genellikle kullanıcıdan alındıktan hemen sonra şifrelenir. Veri tabanında depolanan eşleşme noktaları, sayısal değere dönüştüren bir algoritma kullanılarak işlenir. Daha sonra değer, taranan biyometrik bilgilerle karşılaştırılır ve değerin onaylanıp onaylanmadığı doğrulanır. Bu işlem, biyometrik kimlik doğrulamanın güvenliğini sağlamak için gereklidir (Yang, 2010). Ayrıca görüntülü görüşme yönteminde kullanıcılardan bazı ek kanıtlar talep edilebilir. Örneğin operatör, SMS ile gönderilen bir kodu talep ederek kontrol sağlayabilir (ENISA, 2021). Ülkemiz uygulaması da bu yönde olup SMS OTP doğrulaması müşteri edinim sürecinde kullanılmaktadır.

Paydaşların uzaktan kimlik doğrulama çözümlerinin yeterli güvenilirliğe sahip olduğuna ikna edilmesi gereken durumlarda, daha fazla verinin daha uzun süre saklanması gerekebilir (ENISA, 2021). Bu noktada alınması gereken önlem, depolama olanaklarının değerlendirilmesidir. Ek olarak uzaktan yapılan kimlik tespitlerinde kişisel kimlik verilerinin yalnızca veri işleme amacı ile kullanıldığına emin olunmalıdır (Sova vd., 2021). Literatür göstermektedir ki, belli bir uzaktan kimlik doğrulaması yöntemini kullanırken onun zayıflığını kapatan bir diğer yöntemden de destek alınabilir. Böylece oluşturulan kombine yöntem ile güvenlik riskleri azaltılabilir.

İnternet/mobil bankacılığında gerçekleştirilen tüm işlemlerin cazip bir hedef olması nedeniyle, parasal kayıpları önlemek veya kabul edilebilir bir düzeyde güvence altına almak için gerekli tedbirler alınmalıdır (Jama vd., 2019). Banka operatörleri, sistemlerindeki güvenlik açıklarını belirlemek için kullandıkları kimlik doğrulama yöntemiyle ilgili bir boşluk (gap) analizi yapmalıdır. Bilinen unsurların sosyal mühendislik yolu ile kolayca elde edilebilir olması, SMS OTP'nin yukarıda belirttiğimiz zafiyeti nedeni ile biyometrik veriler internet ve mobil bankacılıkta güvenlik sağlayıcı unsur olarak devreye alınmalı ve bankalar tarafından geliştirilmelidir.

Bankalar, KVKK'nin getirdiği risklere karşı etkin bir şekilde korunmak için çeşitli önlemler alabilir. Veri güvenliği için güçlü şifreleme yöntemleri, güvenlik duvarları ve sıkı erişim kontrolü gibi teknolojik önlemler alınmalıdır. Veri işleme amaçlarına uyumlu erişim yetkileri sağlanmalıdır. Yetkisiz erişimler engellenmeli, erişimlerin log kayıtları ile takibi sağlanmalıdır. Müşteri bilinçlendirme ve onay süreçleri önemlidir, bu nedenle müşterilere veri işleme faaliyetleri hakkında şeffaf ve anlaşılır bilgiler sağlanmalıdır. Denetimler düzenli olarak yapılmalı ve

veri ihlâl durumlarında derhâl bildirim yapılmalıdır. Bankaların KVKK'ye uyumlu politikalar ve prosedürler geliştirmesi, personel eğitimleri düzenlemesi ve hukuki danışmanlık alması önemlidir. Kişisel verilerin işlenmesini içeren kimlik doğrulama sürecinde, ilgili hukuki süreçlere dikkat edilmesi gerekmektedir. Bu veriler, kişileri, grupları veya toplulukları etkileyebilecek içeriklere sahip olabilir, bu nedenle bankacılık şirketleri her senaryo için risk planlaması yapmalıdır. Ayrıca uluslararası veri transferi de dâhil çeşitli verilerin alınması, korunması ve işlenmesi ile ilgili Kişisel Verilerin Korunması Kanunu ve bu kanuna ilişkin maddeler düzenlenmelidir. Bankacılık sektörü başta olmak üzere müşteri gizliliğinin önemsenmesi gerektiği ve hassas verilerin korunması gerektiği çeşitli sektörlerde bu hususstaki düzenlemelerin daha ayrıntılı ve açık bir şekilde ifade edilmesi gerekmektedir.

Literatür taramasında görülmektedir ki, bankalar, müşteri tanımlamasında farklı yöntem ve araçlar kullanmaktadır. Bu noktada Metaverse gibi sanal ekosistemler, bankacılık işletmeleri için bir fırsat olabileceğinden firmalar tarafından değerlendirilmelidir (Indriasari vd., 2022).

Öte yandan yeni bir finansal anlayışın ve blok zincir teknolojisine dayalı uygulamaların gelişmesi, geleneksel bankaları ve şubelerini kullanmayan yapılarla rekabet etmek için bankaların strateji geliştirmelerini zorunlu kılar. Bu durumda, düzenlemelerin önemi daha da artar(Balkan, 2021).

Bulgular ve Sonuç

Dünyada bankacılığın konvansiyonel bankacılıktan dijital bankacılığa doğru yol aldığı bu geçiş sürecinde ise hibrit bankacılık modeli ile bankacılığın devam edeceği anlaşılmaktadır. Bu dönüşümü hem teknolojik gelişmeler hem kullanıcıların bankacılık beklentisinin dijitale evrilmesi hem de dijital bankacılığın maliyet tasarrufu özendirmektedir. Türkiye'de de değişim bu yönde olup mevzuat altyapısı hazırlanmış Dijital Bankaların Faaliyet Esasları ile Servis Modeli Bankacılığı Hakkında Yönetmelik ile dijital bankacılığın önü açılmıştır. Hâlihazırda 1 mevduat ve 3 katılım bankası dijital bankacılık lisansını almıştır.

Şubesiz bankacılığın iyi tasarlanması oldukça önemlidir. Bu sistemin kullanıcı dostu bir yapı olmasının yanında güvenli dijital bir banka yapısının kurulması da bir o kadar önemlidir. Şubesiz bankacılık modellerinin kart kopyalama, sosyal mühendislik, dolandırıcılık yazılımları ile yarattığı mağduriyetler ortadadır. BDDK'nin Bilgi Sistemleri ve Elektronik Bankacılık Yönetmeliği'nin kimlik doğrulama ve işlem güvenliği tedbirleri, riski azaltsa da mağduriyetleri gidememiştir. Bunun önemli sebeplerinden birisi de Yönetmeliğin önerdiği iki faktörlü doğrulama modelinde

bankaların biyometrik veri doğrulama seçeneğini uygulamaya koymakta gecikmeleridir. Bilinen unsurların sosyal mühendislik yolu ile kolayca elde edilebilir olması, SMS ile gönderilen doğrulama kodunun, aynı mobil cihaz üzerinde yüklü diğer uygulamalar tarafından okunabilmesi ve bu uygulamalar tarafından üçüncü bir tarafa yönlendirilebilmesi, SIM Kartın kopyalanabilmesi, mobil cihaz üzerindeki SMS mesajlaşma uygulamasının bankanın kendi kontrolünde olan bir mobil uygulama niteliğinde de bulunmaması nedeni ile 2 faktörlü doğrulamanın önemli sacayağı olan müşteriye SMS ile gösterilecek doğrulama kodunun bütünlüğü ya da güvenilirliği şüphelidir ki pratikte oluşan dolandırıcılık vakaları da bu şüpheyi doğrulamaktadır.

Yukarıda ifade olunan riskin bertaraf edilebilmesi için bizim önerimiz BDDK'nin Bilgi Sistemleri ve Elektronik Bankacılık Yönetmeliği ile Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik ile altını çizdiği biyometrik verilerin uzaktan kimlik tespitinde hem müşteri edinim aşamasında hem de finansal ve finansal olmayan işlemlerde kullanılmasıdır. İnternet ve mobil bankacılığında işlemi yapan kişinin gerçekten hesap sahibi müşteri olup olmadığının tespiti için login aşamasında 2 faktörlü doğrulamalara ek olarak aşağıdaki ilave doğrulamaların sağlanmasıdır.

- Uzaktan Kimlik Tespiti Yöntemlerine İlişkin Yönetmelik'te ifade olunan 'yakın alan iletişimi'nin kimlik kartına uygulanarak kimliğin doğrulanması,
- Doğrulanan kimlikten alınan resim ile yüz doğrulamasının sağlanması ve
- Müşterinin canlılık testine tabi tutulması

Bu güçlü doğrulama en azından müşterinin büyük bir kısmı Türk vatandaşları olan bankalarca uygulanması sosyal mühendislik, SIM kart kopyalama, SMS yönlendirme gibi vakalara son verecektir.

Yukarıda ifade edildiği üzere Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik (UKTY) müşteri ediniminde 'yakın alan iletişimi'nin başarısız olması durumunda müşteri edinimini optik okuma ve ilk finansal işlemin müşteriye ait başka bir bankadan yapılması ile mümkün hale getirmiştir. Ancak biz bu uygulamanın kimlik kartlarının bünyesinde bulunan güvenlik unsurlarını atlaması, yüz tanımanın kimlikteki optik okuyucu ile edinilen resim (dolandırıcı kendi resmini yapıştırabilir) ile özçekim ile çekilen fotoğrafın karşılaştırması nedeni ile güvence sağlamaması nedeni ile terk edilmesi gerektiği düşüncesindeyiz.

Uzaktan kimlik tespitinin en önemli adımlarından birisi de canlılık testidir. Bankalardan risk emniyeti açısından canlılık testi ve benzer şekilde sürecin önemli sacayağı olan yüz tanıma oranlarını kabul edilebilir bir güvenlik oranına çekmesi beklenmelidir. İşbu açıdan uzaktan kimlik tespit sürecinde işlem doğruluk yüzdesini artırmak bakımından bankalar, süreçlerini sürekli test etmeli sonuçlara göre kullanılan teknolojiyi geliştirmeli, değiştirmeli ya da eşik değerlerini artırmalıdır.

Elektronik Bankacılık Hizmetlerinde Ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasında Kimlik Doğrulama ve İşlem Güvenliği İçin Sağlanması Gereken Kriterler Hakkında Taslak Genelge (2022/2) uyarınca, Bankacılık Düzenleme ve Denetleme Kurumunun gözetimi ve denetimi altında olan diğer kuruluşlara ve DBY kapsamındaki arayüz sağlayıcılara başvurarak bankalar, Kurum gözetimi ve denetimi altındaki diğer kuruluşlar ve arayüz sağlayıcılarına ürün ve hizmet sunabilmek için kurumdan izin almakla yükümlüdür. Taslağın bu hali ile yayımlanmasını olumlu buluyoruz. Önerilen, BDDK'nin lisanslama sunarken firmaların kimlik doğrulamada kullandıkları teknolojilerin ve algoritmaları analiz ederek her bir firma için asgari eşik değerler belirlemesi ve uygulanmasını zorunlu tutmasıdır. Mesela, A firmasının algoritma zenginliğine göre yüz tanıma eşik değerini %70 belirler iken diğer bir firma için %90 belirlemesidir. Firmalar teknolojilerini ve yazılımlarını geliştirdikçe BDDK'den eşik değerlerini yükseltmelerini isteyebileceklerdir.

Uzaktan müşteri edinimlerinde karşılaşılacak diğer bir risk Deep Fake (DF)'tir. DF olarak bilinen yapay zekâ teknolojisi kullanılarak sahte görüntü ve ayırt edilmesi çok güç ses benzerlikleri yaratılmaktadır. DF teknolojisi, bir kişinin yüzünü ve sesini başka bir kişinin yüzüne ve sesine yerleştirmeyi başarabilmekte olup ayırt edilmesi zor bir benzerlikle bunu sunabilmektedir. Uzaktan müşteri ediniminin son evresi, müşteri temsilcisi tarafından müşterinin görüntülü karşılanması bazı ilave doğrulamalar ile sürecin tamamlanmasıdır. Ancak DF teknolojisi müşteri temsilcisini atlatabilecek becerilere sahiptir. İşbu yüzden bankalar, DF riskinin farkına varıp uzaktan kimlik tespitinde görüntülü görüşme ile işlemi sonlandırdığı uygulamalarına yapay zekâ dedektörleri kurarak DF'nin başka bir yapay zekâ ile yakalanmasını sağlayıp bu riskin oluşmasını önlemelidir.

Türk bankacılık sisteminde uzaktan kimlik tespiti yöntemlerinin kullanılıyor olması şüphesiz doğru bir adımdır. Bu teknolojik adımlar ile daha çok kişinin finansal sistem ile tanışması ve daha ucuz hizmet alması sağlanabilir. Ancak bu sistemlerin gerçek potansiyellerine ulaşılabilmesi için işleyişteki tüm risk kalemlerinin detaylı bir analizi gerekmektedir. Bankalar bu sürecin sebep

olacağı güvenlik açıkları ya da müşteri kayıpları gibi riskleri önceden fark edip önüne geçemezse sektörde devamlılıklarını riske atacaklardır. Denetleyici kurumlar da bu riski görüp özellikle dijital zafiyetleri tespit edecek birikime sahip istihdamı sağlamalı, bu alandaki bilgi birikimini artırmalıdır. Ek olarak banka kullanıcılarının dijital ortamdaki okuryazarlığın artırılması ile bankacılık sektörünün teknolojik gelişmelere ayak uydurması sağlanmalıdır. Bu amaçla bankalar:

- Bankacılık sistemlerinin dijitalleşme özellikli altyapısı en yeni teknolojiye uygun olarak güncellenmelidir.
- Bankacılık sektöründeki iş esnekliği sağlanmalı,
- Başta uzaktan bankacılık hizmetleri olmak üzere tüm hizmetler için gerekli personelin yetiştirilmesi sağlanmalı,
- Dijital yeni ürün ve hizmetler geliştirilmeli,
- Kullanıcı dostu sistemler ve ürünler geliştirilirken güvenlik riski ihmal edilmemelidir. Amaç, dijital bankacılık ürünleri sunan banka olmak değil dijital güvenli banka olmaktır.
- Konvansiyonel risk yönetimine teknolojik risk yönetimini eklenmelidir.

Uzaktan kimlik tespiti yöntemlerine ilişkin risklerin analiz edildiği bu çalışma, güvenlik risklerinin en önemli konu olduğunu ortaya koymaktadır. Bankalar ve banka temsilcileri, uzaktan müşteri kabulü süreçlerinde önemli sorumluluklar üstlenmektedir. Ancak, akıllı telefon ve çipli kimlik gibi gereksinimlerin karşılanamaması, erişilemeyen potansiyel müşteriler için bir yönetim planının oluşturulmasını gerektirmektedir. Elektronik tanımlama hizmeti sağlayıcıları, kişisel verilerin korunması ve güvenlik sağlanması için teknik önlemler almalıdır. Banka yazılımlarının iyileştirilmesi ve güçlendirilmesi, süreçlerdeki gecikmelerin önlenmesine yardımcı olacaktır.

Bu çalışmanın ana kazanımı, son teknoloji dijital bankacılık teknolojisi trendlerinden biri olan uzaktan kimlik tespiti yöntemlerine ilişkin riskleri tespit ederek dijital bankacılık mimarisi ve akıllı dijital bankacılık uygulamalarına katkıda bulunmak, riskli noktaları belirlemek ve risk azaltıcı tedbirlere katkı sağlamaktır. Uzaktan kimlik tespiti yöntemlerinin kullanım alanlarına ilave güvenlik seviyeleri önerilerek daha güvenli bir dijital bankacılık oluşumuna katkı sağlanmaya çalışılmıştır.

Kaynakça

Alomaliye (2023). Uzaktan ve Şubeden Müşteri Edinimi İstatistikleri. https://www.alomaliye.com/2023/04/11/uzaktan-ve-subeden-musteri-edinimi-istatistikleri-mart-2023/. Son erişim tarihi, 15.11.2023.

Arjun R vd. (2021). Developing banking intelligence in emerging markets: Systematic review and agenda. *Int. J. Inf. Manag.* Data Insights, vol. 1, no. 2, p. 100002, 2021.

Apple (2023). iPhone veya iPad Pro'nuzda Face ID'yi kullanma. Erişim: 16.05.2023. https://support.apple.com/tr-tr/HT208109. Son erişim tarihi, 15.11.2023.

Aydin M vd. (2023). A Fusion-Based Deep Neural Networks Approach for Face Liveness Detection. *International Conference on Innovations in Intelligent Systems and Applications (INISTA)*, 20-23 September 2023. 10.1109/INISTA59065.2023.10310519.

Balkan H (2021). Dijital (Şubesiz) Bankaların Regülasyonu. *Bankacılar Dergisi*, Sayı (Vol. 118). https://orcid.org/0000-0001-8032-9866.

Banerjee S (2015). From cash to digital transfers in India: The story so far. *Customer-Centricity for Financial Inclusion brief*. Washington, DC, World Bank, pp.1–4.

Bankid (2023). Digital ID card in BankID. Erişim: 25.04.2023. https://www.bankid.com/en/foretag/digital-id-card. Son erişim tarihi, 15.11.2023.

Belov A V ve Zagumennov P D (2019). Designing Algorithms for Evaluating the Effectiveness of Remote Banking Systems. *Journal of Accounting and Finance* (Vol. 19, Issue 9).

Beybur M (2021). Şubesiz Dijital Bankacılık ve Türk Bankacılık Sektörü İçin Öneriler. *Ankara Hacı Bayram Veli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi.* 24/1 (2022) 286-303.

Chajkina E V vd. (2018). Innovative technologies as a factor of competition in the Russian banking market. Nauchnyi vestnik: 7nansy, banki, investitsii, no.4, pp.114–121.

CFO (2023). Türkiye Fintek Ekosistemi Durum Raporu. https://www.cbfo.gov.tr/turkiye-fintek-ekosistemi-durum-raporu. Son erişim tarihi, 20.06.2023.

Dağıdır Çakan C vd. (2022). A New Approach in Banking Branchless (Digital) Banking and Customer Acquisition: Case Study of Kuveytturk Bank*. Finans Ekonomi ve Sosyal Araştırmalar Dergisi*. Year 2022, Volume: 7 Issue: 1, 177 - 192, 31.03.2022. https://doi.org/10.29106/fesa.1059930.

Digalaki E (2022). The impact of artificial intelligence in the banking sector & how AI is being used in 2022. https:// www. businessinsider. com/ ai- in- banki ng- report? r= US& IR=T.

ENISA (The European Union Agency for Cybersecurity) (2021). Remote ID Proofing -Analysis of Methods to Carry Out Identity Proofing Remotely. Erişim: 12.05.2023. https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing

Etnews (2018). Woori Bank to Be the first South Korean Commercial Bank to Launch a PC Version of Bank Sign. Erişim: 25.04.2023. http://english.etnews.com/20181008200002.

Ezrokh Y S (2020). Problems of establishing the practice of remote identification of

clients in the Russian banking system (economic aspects). Vestnik Sankt-Peterburgskogo Universiteta. Ekonomika. 36 (2), 266–286. https://doi.org/10.21638/spbu05.2020.205.

Fares O H vd. (2022). Utilization of artificial intelligence in the banking sector: a systematic literature review. *Journal of Financial Services Marketing*. https://doi.org/10.1057/s41264-022-00176-7.

FINMA (Swiss Financial Market Supervisory Authority) (2016). Circular 2016/7 Video and Online Identification: Due diligence requirements for client onboarding via digital channels. https://www.finma.ch/en/~/media/finma/dokumente/rundschreiben-archiv/2016/rs-16-07/finma-rs-2016-07.pdf?la=en. Son erişim tarihi, 25.04.2023.

FMA (Regulation of the Financial Market Authority) (2017). Online Identification Regulation. https://www.fma.gv.at/download.php?d=2665. Son erişim tarihi, 25.04.2023.

Gao M vd. (2014). Fingerprint sensors in mobile devices. Paper presented at the 2014 *9th IEEE Conference on Industrial Electronics and Applications*.

Gorgani G (2016). The effect of e-banking on bank customers' deposits. *International Journal of Humanities and Cultural Studies (IJHCS).* ISSN 2356-5926, 1(1), 2231-2246.

HMB (Türkiye Cumhuriyeti Hazine ve Maliye Bakanlığı) (2021). *Ekonomi Reformları*. https://ms.hmb.gov.tr/uploads/2021/03/Ekonomik-Reformlar-Kitapcigi.pdf. Son erişim tarihi, 20.05.2023.

Hollister S (2018). Amazon facial recognition mistakenly confused 28 Congressmen with known criminals. https://www.cnet.com/news/privacy/amazon-facial-recognition-thinks-28-congressmen-look-like-known-criminals-at-default-settings/.

iBeta (2023). ISO 30107-3 Presentation Attack Detection Test Methodology And Confirmation Letters. https://www.ibeta.com/iso-30107-3-presentation-attack-detection-confirmation-letters/. Son erişim tarihi, 20.08.2023.

Indriasari E vd. (2019). Digital Banking Transformation: Application of Artificial Intelligence and Big Data Analytics for Leveraging Customer Experience in the Indonesia Banking Sector," in *Proceedings - 2019 8th International Congress on Advanced Applied Informatics*, IIAI-AAI 2019, 2019, pp. 863–868.

Indriasari E vd. (2022). Intelligent Digital Banking Technology and Architecture: A Systematic Literature Review. *International Journal of Interactive Mobile Technologies*, 16(19), 98–117. https://doi.org/10.3991/ijim.v16i19.30993.

Jain A K vd. (2006). Biometrics: a tool for information security. *IEEE transactions on informaion forensics and security*, 1(2), 125-143.

Jama A Y vd. (2019). Cyber physical security protection in online authentication mechanisms for banking systems. Advances in Intelligent Systems and Computing, 857,

1021–1031. https://doi.org/10.1007/978-3-030-01177-2_74.

Juniper Research. (2020). Digital Banking Users to Reach 2 Billion This Year, Representing Nearly 40% of Global Adult Population. www.juniperresearch.com/press/digital-banking-users-to-reach-2-billion. Son erişim tarihi, 29.04.2023.

Keleş M K ve Demirel Ş (2020). Republic of Turkey Identity Card (TCKK): Banking Use Case in Authentication & Customer Onboarding. ACM International Conference Proceeding Series, 35–40. https://doi.org/10.1145/3397125.3397126

Kemp S (2021). Digital 2021: The Latest Insights Into the State of Digital. Erişim: 13.05.2023. https://wearesocial.com/uk/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital/.

Khan A (2018). National Identity Card: Opportunities and Threats. *Journal of Asian Research*, vol.2, no.2, pp.77–85.

Koenig-Lewis N vd. (2010). Predicting young consumers' take up of Mobile Banking Services. *International Journal of Bank Marketing*, 28(5), 410–432. https://doi.org/10.1108/02652321011064917.

Korobov Y (2017). Global Banking: Transformation, Innovation & Competition. Paper presented, in Proceedings of the SHS Web of Conferences. *Innovative Economic Symposium 2017*, 19 October 2017, (IES2017), Czech Republic, 39, 01012.

Kozlova N P ve Ustinova E V (2019). Digitization of the banking sector: trends and cases of development of the Russian market. *Ekonomika. Biznes. Banki*, no.1, pp.18–34.

Mamadiyarov Z (2020). Prospects For The Development Of Remote Banking Services In The Context Of Bank Transformation. *The American Journal of Applied Sciences*, 02(07), 108–118. https://doi.org/10.37547/tajas/Volume02Issue07-18

Mamadiyarov Z (2021). Analysis of factors affecting remote banking services in the process of bank transformation in Uzbekistan. *Financial and Credit Activity: Problems of Theory and Practice*, 1(36), 14–26. https://doi.org/10.18371/fcaptp.v1i36.227607

NTV (2022). 10 kişiden 8'i çipli kimlik karta geçti. https://www.ntv.com.tr/turkiye/10-kisiden-8i-cipli-kimlik-karta-gecti,7VG7ZGeJYEOat0-HsHZMRQ. Son erişim tarihi, 13.05.2023.

NVİ (Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü). TC Kimlik Kartı (Online Access). https://www.nvi.gov.tr/tc-kimlik-karti. Son erişim tarihi, 20.05.2023.

OneConnect (2021). OneConnect Announces Partnership with Indonesia-based Bank Mayapada, to Enable Digital Onboarding through a Comprehensive Suite of Innovative Solutions. https://www.prnewswire.com/news-releases/oneconnect-announces-partnership-with-indonesia-based-bank-mayapada-to-enable-digital-onboarding-through-a-comprehensive-suite-of-innovative-solutions-301417400.html. Son erişim

tarihi, 20.08.2023.

RG (Resmî Gazete) (2020). Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (2020, 15 Mart*). Resmî Gazete* (Sayı: 31069). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm

RG (Resmî Gazete) (2020). Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun (2020, 18 Haziran). *Resmî Gazete* (Sayı: 31167). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2020/06/20200626-1.htm

RG (Resmî Gazete) (2021). Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik (2021, 24 Şubat). *Resmî Gazete* (Sayı: 31405). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2021/02/20210224M2-3.pdf

RG (Resmî Gazete) (2021). Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik (2021, 1 Nisan). *Resmî Gazete* (Sayı: 31441). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2021/04/20210401-7.htm.

RG (Resmî Gazete) (2021). Mali Suçları Araştırma Kurulu Genel Tebliği (2021, 30 Nisan). *Resmî Gazete* (Sayı: 31470). Erişim adresi: https://resmigazete.gov.tr/30.04.2021.

RG (Resmî Gazete) (2021). Dijital Bankaların Faaliyet Esasları ile Servis Modeli Bankacılığı Hakkında Yönetmelik (2021, 29 Aralık). *Resmî Gazete* (Sayı: 31704). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2021/12/20211229-6.htm.

Sardana V ve Singhania S (2018). Digital technology in the realm of banking: A review of literature. *International Journal of Research in Finance and Management*, 1(2): 28-32. https://www.allfinancejournal.com/article/view/12/1-2-8.

SBB (Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı) (2019). On Birinci Kalkınma Planı (2019-2023). https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf. Son erişim tarihi, 20.06.2023.

Shamah J (2018). The role of financial institutions in delivering identity-as-a-service for governments, *Web Fraud Prevention and Online Authentication Market Guide 2017/2018*, Thursday 8 March 2018.

Sheshasaayee A ve Sumathy D. (2017). A Framework to Enhance Security for OTP SMS in E-Banking Environment Using Cryptography and Text Steganography. *Proceedings of the International Conference on Data Engineering and Communication Technology, Advances in IntelligentSystems and Computing*, 469.

Sova O vd. (2021). Development of remote identification the enterprises by digital technologies. *SHS Web of Conferences*, 120, 02004. https://doi.org/10.1051/shsconf/202112002004

Stoiko O (2020). The problems of economy, 2(44), 356-364.

Surane J (2021). Developers Are the New Bankers': Wells Fargo Analysts Predict Wave of Job Cut. Erişim: 13.05.2023. https://www.bloomberg.com/news/articles/2021-09-28/-developers-are-the-new-bankers-mayo-predicts-wave-of-job-cuts

TBB (Türkiye Bankalar Birliği) (2021). Uzaktan ve Şubeden Müşteri Edinimi İstatistikleri. Türkiye Bankalar Birliği: https://www.tbb.org.tr/tr/banka-ve-sektor-bilgileri/istatistiki-raporlar/Uzaktan_ve_Subeden_Musteri_Edinimi_Istatistikleri/6154. Son erişim tarihi, 29.08.2023.

TBB (Türkiye Bankalar Birliği) (2023). Uzaktan ve Şubeden Müşteri Edinimi İstatistikleri. Türkiye Bankalar Birliği: https://www.tbb.org.tr/tr/bankacilik/banka-ve-sektor-bilgileri/istatistiki-raporlar/59. Son erişim tarihi, 29.08.2023.

Teemu R (2010). Electronic identity in Finland: ID cards vs. bank IDs, IDIS (2010) 3:175–194, DOI 10.1007/s12394-010-0049-8

Teknomers (2023). UIDAI, sağlam parmak izi tabanlı Aadhaar kimlik doğrulaması için yeni güvenlik mekanizmasını kullanıma sunuyor. https://teknomers.com/2023/02/28/uidai-saglam-parmak-izi-tabanli-aadhaar-kimlik-dogrulamasi-icin-yeni-guvenlik-mekanizmasini-kullanima-sunuyor/. Son erişim tarihi, 25.04.2023.

Toshtemirovich Mamadiyarov Z (2021). Risk Management In the Remote Provision of Banking Services In The Conditions of Digital Transformation of Banks. *ACM International Conference Proceeding Series*, 311–317. https://doi.org/10.1145/3508072.3508119.

Türedi D C (2023). Uzaktan Bankacılık Başvuru ve Müşteri Edinimi İstatistikleri. *Fibabanka*.

Ullah M (2022). Khushhali Microfinance Bank begins digital account onboarding. https://dnd.com.pk/khushhali-microfinance-bank-begins-digital-account-onboarding/261469.

Velioğlu S vd. (2019). A New Approach to Cryptographic Hashing: Color Hidden Hash Algorithm. *Proceeding of 2019 International Conference on Digitalization (ICD).*

Wassan Abdullah A (2020). Digital payment and banking adoption research in Gulf countries: A systematic literature review, *Int. J. Inf. Manage*., 2020.

Yang JC (2010). Biometrics verification techniques combining with digital signature for multimodalbiometrics payment system. *In: 2010 International Conference on Management ofe-Commerce and e-Government*.

Zadeh M J ve Barati H (2019). Security improvement in mobile baking using hybrid authentication. *ACM International Conference Proceeding Series*, 198–201. https://doi.org/10.1145/3369114.3369151.