İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

DOKUNMA DİNAMİĞİ İLE MOBİL KULLANICILAR İÇİN KİMLİK DOĞRULAMA

YÜKSEK LİSANS TEZİ

Rıdvan ÖZGÜVENİR

Bilişim Uygulamaları Anabilim Dalı

Bilgi ve Haberleşme Mühendisliği Programı

HAZİRAN 2019

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

DOKUNMA DİNAMİĞİ İLE MOBİL KULLANICILAR İÇİN KİMLİK DOĞRULAMA

YÜKSEK LİSANS TEZİ

Rıdvan ÖZGÜVENİR
(708151031)

Bilişim Uygulamaları Anabilim Dalı

Bilgi ve Haberleşme Mühendisliği Programı

Tez Danışmanı: Prof. Dr. M. Oğuzhan KÜLEKCİ

HAZİRAN 2019

İTÜ, Bilişim Enstitüsü'nün 708151031 numaralı Yüksek Lisans Öğrencisi Rıdvan ÖZGÜVENİR, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "DOKUNMA DİNAMİĞİ İLE MOBİL KULLANICILAR İÇİN KİMLİK DOĞRULAMA" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Prof. Dr. M. Oğuzhan KÜLEKCİ** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Doç. Dr. Gökhan BİLGİN** Yıldız Teknik Üniversitesi	.....
	Dr. Öğr. Üyesi Sefer BADAY İstanbul Teknik Üniversitesi	.....

Teslim Tarihi : 03 Mayıs 2019
Savunma Tarihi : 13 Haziran 2019

Aileme,

ÖNSÖZ

Yüksek lisans eğitimim süresince değerli bilgi ve tecrübelerini benimle paylaşan, vizyonuyla bana yol gösteren, hiçbir zaman desteğini esirgemeden değerli vaktini sabırla bana ayıran danışmanım Prof. Dr. Muhammed Oğuzhan Külekci'ye, beni asla yalnız bırakmayan en değerli varlığım aileme, özellikle de eğitim hayatımın ilkokuldan bugüne kadar her döneminde üstün bilgi ve becerileri ile bana önce örnek daha sonra destek olan ablam Kübra'ya ve beni destekleyen tüm arkadaşlarıma teşekkür ederim.

Haziran 2019

Rıdvan ÖZGÜVENİR
Bilgisayar Mühendisi

İÇİNDEKİLER

Sayfa

KISALTMALAR

ATM : Automated Teller Machine
DNA : Deoksiribo Nükleik Asit
EER : Equal Error Rate
FAR : False Acceptance Rate
FRR : False Reject Rate
ID : Identification Number
IP : Internet Protocol
KVKK : Kişisel Verileri Koruma Kanunu
LAN : Local Area Network
MFA : Multi-Factor Authentication
OTP : One Time Password
PC : Personal Computer
PIN : Personal Identification Number
RAID : Redundant Array of Independent Disks
SFA : Single Factor Authentication
TCKN : Türkiye Cumhuriyeti Kimlik Numarası
2FA : Second Factor Authentication

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

DOKUNMA DİNAMİĞİ İLE MOBİL KULLANICILAR İÇİN KİMLİK DOĞRULAMA

ÖZET

Hızla gelişen teknoloji ile birlikte bilgisayarlar insan hayatının çok önemli birer parçası haline gelmiştir. Daha ergonomik, taşınabilir bilgisayarların, yüksek işlem gücüne sahip donanım ve yazılımların geliştirilmesi, internete daha hızlı ve kolay erişim yardımıyla çevrimiçi ortamlar insanların günlük eylemlerinin sanal ortamlara taşınmasını sağlamıştır. Günümüzde bankacılıktan alışverişe, resmi kurumlardaki işlemlerden ticarete kadar birçok eylem, geliştirilen uygulamalar aracılığıyla mobil cihazlardan kolaylıkla gerçekleştirilebilmektedir. İnsan hayatını oldukça kolaylaştıran bu gelişmeler beraberinde birtakım güvenlik problemlerini de getirmektedir. Bu noktada, kullanıcı tanımlama ve kimlik doğrulama, bilgi güvenliği ve gizlilik kavramları hem bireyler hem de kurumlar için önemli hale gelmektedir. Buna karşılık, bilgi güvenliği ve bilinci konusu hızla gelişen bu yeniliklerin hızını yakalayamamıştır. İnsanlar bahsedilen tüm bu hizmetlerden yararlanabilmek için hassas kişisel verilerini çevrimiçi dünya ile paylaşmaktadır. Bu bilgilerin güvenliği için, kullandığımız bu cihazlarda kullanıcı bilgilerinin güvenliğini sağlayan şifrelemeden parmak izi tanımaya kadar geleneksel ve modern birçok kimlik doğrulama yöntemi kullanılmaktadır. Bugün en çok kullanılan kimlik doğrulama yöntemi olan şifrelemenin, saldırganlar tarafından kolayca kırılabilen ve tek başına bilgi güvenliğini sağlayamayan bir yöntem haline gelmesi, artık daha güvenilir yöntemlere ihtiyaç olduğunu ortaya çıkarmıştır. Ayrıca, insanların da bilgi güvenliği konusundaki bilinci bu gelişmelerdeki hıza paralel hızla gelişmemiştir. Günümüzde insanlar farklı sayıda çevrimiçi ortamda aktif olduğu için bu sistemlerde kullandıkları şifreleri daha kolay hatırlayabilmek adına birbirine çok benzeyen hatta aynı şifreleri hem bankacılık gibi yüksek güvenlik gerektiren sistemlere hem de güvensiz bir sosyal medya platformuna verebilmektedirler.

Teknolojideki gelişmeler yetersiz kalan kimlik doğrulama yöntemlerini güçlendirecek, gelişmiş güvenlik ve kimlik doğrulama sistemlerinin ortaya çıkmasını sağlamıştır. Bu yöntemlerden birisi olan biyometrik kimlik doğrulama yöntemi, insanların fiziksel ve davranışsal ayırt edici özelliklerini kullanarak onları tanıma ve doğrulama yapmayı amaçlamaktadır. Bugün dokunmatik ekranlı mobil cihazların giderek yaygınlaşmasıyla ile insan bilgisayar etkileşimi farklı bir boyuta taşınmış ve bu etkileşim ortaya oldukça değerli ve hassas olan dokunma verilerini çıkarmıştır. İnsanların dokunmatik cihazlarla girdiği etkileşim sırasındaki dokunma davranışları, bireylerin ayırt edici birer özelliği olarak kabul edilmiş ve kimlik doğrulama yöntemi olarak kullanılmaya başlanmıştır.

Bu çalışmada da, dokunma dinamiği ile davranışsal biyometrik kimlik doğrulama yöntemini ele alan bir model tasarlanmış ve bu modelle bir mobil uygulama geliştirilerek dokunma dinamiklerinden kullanıcı doğrulama ve anomali tespiti yapılabileceği ortaya konmaya çalışılmıştır. Çalışmanın ilk bölümünde gelişen insan

bilgisayar etkileşimi ve mobil cihazların insan hayatındaki giderek artan yeri ele alınmış, sonrasında çalışma kapsamında geliştirilen kişiye özel klavyelerin test edildiği uygulamanın temelinde yer alan kullanıcı öğrenme davranışını etkileyen öğrenme yöntemleri açıklanmıştır. Üçüncü bölümde, gelişen dijital dünyada bilgi güvenliğinin önemi ve farklı teknikler kullanılarak yapılan saldırılar sonucu oluşan güvenlik açıkları incelenmiştir, bu güvenlik açıklarına karşı kullanılan ve en yaygın güvenlik önlemi olan kullanıcı kimlik doğrulama ayrı bir başlıkta incelenerek, biyometrik kimlik doğrulama yöntemleri tek tek incelenmiştir. Beşinci bölümde ise literatürdeki benzer çalışmalara yer verilmiştir.

Tez çalışması kapsamında, kullanıcıların dokunma dinamiğini esas alan bir biyometrik kimlik doğrulama uygulaması geliştirilmiştir. Geliştirilen mobil uygulama ile çalışma için kullanıcılardan dokunma dinamiği verilerinin toplanabileceği bir ara yüz sağlanmıştır. Dokunma süreleri, dokunma alanı, dokunma basıncı ve cihaz tutuş pozisyonunun öznitelik olarak değerlendirildiği uygulama ile hem dokunma dinamiği verileri hem de kullanıcılara özel üretilen ve onlara farkında olmadan pasif bir şekilde öğrenme yöntemi olan örtük öğrenme ile öğretilen numerik klavyeler kullanılarak kimlik doğrulama yapılmaya çalışılmıştır.

Geliştirilen uygulama toplam 30 denek katılımıyla test edilmiş, ardından tanımlanan kullanıcılardan ayrı ayrı doğrulama denemeleri yapılması istenmiştir. Katılımcılardan, kendilerine özel 0'dan 9'a rakamların yerleri rastgele dağıtılarak oluşturulan numerik klavyeden belirlenen 6 karakterli rakam dizilerini başarı bir şekilde girmeleri istenmiştir. Ayrıca, yanlış kabul oranının ölçülebilmesi için sistemde tanımlı olmayan 5 kullanıcıdan, daha önceden tanımlanmış kullanıcılar yerine giriş yapmaları istenmiştir. Yapılan deneylere katılan kullanıcılara, deney sonrası birer anket yapılmış ve genel kullanıcı davranışı analiz edilerek tez çalışması kapsamında geliştirilen model ile ilgili çıkarımlar yapılmıştır. Bu deneyler sonucunda, yanlış red oranı (FRR) 0.16, yanlış kabul oranı (FAR) 0.28, eş hata oranı (EER) 0.22 elde edilmiştir.

MOBILE USER AUTHENTICATION USING TOUCH DYNAMICS

SUMMARY

With the rapidly growing technology, computers have become an indispensable part of the human life in today's world where open access is provided to almost every point of the world via internet. Development of portable and more ergonomic PC's, hardware and software which have more powerful processors, faster and easier access to the internet enabled individuals to perform many daily activities in online platforms. For instance, today many transactions from banking to shopping can be carried easily out through applications in mobile devices. In order to perform such activities, systems require some sensitive information, such as bank account information, citizenship number to be shared. Although these activities which are carried by users in online platform make human life easier, they have raised the concerns of information security as sensitive information is required. Thus, the protection and safe storage of information became an essential problem. In this context, privacy, user identification and authentication have become an important concept both for individuals and organizations as sensitive information is required in order to benefit from all these internet facilities.

There are various different traditional and modern authentication methods to secure users' sensitive information and to detect the abnormal cases in information system: encryption, finger print recognition etc. Today, encryption is the most widely used authentication method, but due to the fact that information security attacks are becoming prevalent, this method can easily be cracked by attackers and cannot provide the security by itself. This situation revealed the necessity for more reliable and secure methods. Furthermore, awareness of people about information security has not grown as rapidly as up technology. For example, users can set similar or the same passwords to remember easily for both a banking application which includes their very sensitive data and a social media application that has less secure level.

With the improvements in the technology, new authentication methods have emerged that will strengthen the inadequate and less secure authentication methods. Biometric authentication method is one of these methods which identifies the individuality of the person in a distinctive way and carries them physically or behaviorally, are highly resistant to the possible attacks compared to encryption. Today, with the increasing widespread use of touch screen mobile devices, human computer interaction has become more significant, and this interaction enabled to collect a very valuable data of users such as touch dynamics. The touch behavior during the interaction of people with touch devices has been accepted as a distinctive feature within the context of behavioral biometric authentication method. Behavioral biometry which is also considered as an effective and cheap authentication method can be used without requiring any additional hardware.

The purpose of this thesis is to demonstrate the possible use of behavioral biometric authentication as a safe and effective method of user authentication to identify

possible anomalous behavior or unauthorized access in a system or as a second factor authentication to distinguish the behavior of a legitimate user from the behavior of fraudulent user. Today, many users prefer traditional security methods to log any system in, they prefer using the same or similar password when they log on. This situation brings many security vulnerabilities. In the context of the thesis, it is tried to demonstrate behavioral biometric data as an efficient, alternative and cost-effective solution using the implicit learning method of an adaptive numerical keyboard which is specially created by using touch dynamics values in mobile devices.

In the first part of the thesis, human computer interaction is presented. Human's active interaction with the computers has also contributed to the emergence of new areas of research. In terms of user identification and verification, characteristics of the interaction with computers are considered as distinctive features. The devices which are developed in accordance with the demands of people can be used as an authentication method by analyzing the collected data through monitoring how people use these devices.

In the following section, psychology of learning is presented. Two types of learning methods are examined and compared: Explicit learning and implicit learning. Explicit learning can briefly be defined as intentionally learning, this process is realized as a result of an intent. Implicit learning is defined as learning of the fact without being aware of what they learned. It differs from explicit learning in terms of awareness. Implicit learning method in which the individuals learned an adaptive personalized keyboard via Touch Dynamics application developed within the context of the thesis is discussed with examples from daily life.

In the third section, concept of the information security and vulnerabilities are examined. Information security is considered as protection and safe storage of sensitive information. Even though there has been various improvements in the field of information security, users are still suffering from security attacks because of security vulnerabilities. Speed of development in information security solutions is not equal with improvements of technology. This difference between information security solutions and technology leads to many security vulnerabilities. In this thesis, firstly information security issue, which is gaining more and more importance with developing technology, has been analyzed together with security vulnerabilities and possible security attack techniques. Then, information security attacks such as social engineering, spyware, brute force are presented with examples.

In the fourth section, user authentication is discussed in detail. User authentication is a process which is based on verifying a user while accessing a system using their information. User authentication methods are divided into three: Knowledge based, object-based and biometric based authentication. The biometric methods include physical and behavioral authentications. Physical authentication method covers using individual's unique physical features, such as retina, to distinguish from others with the help of technological devices. On the other hand, behavioral biometrics utilizes unique behavioral features of users such as touch dynamics. In comparison with physical methods, behavioral ones are cost efficient and can easily be collected. Touch dynamics can be defined as users' unique touch behaviors while using touch screen devices. The application which is developed in the thesis focused on touch dynamics which is a one of behavioral biometric based authentications. First, the authentication methods are examined. All these methods are covered, in particular the touch dynamics which is also used for the application developed in the context of

the thesis, as a behavioral authentication method is analyzed with details. In the fifth part, similar researched on keystroke dynamics and touch dynamics are examined.

In the last section of the thesis, a biometric authentication application which is named as "Touch Dynamics" is based on the users' touch dynamics has been developed. This developed mobile application provides an interface which enables to collect touch dynamics data from users. In this application, touch areas, touch durations that differences between touch and release times, touch pressure and device hold positions are considered as features; it has been tried to authenticate the users with numerical keyboards, which are specially generated for the users and taught by implicit learning. This mentioned keyboards are randomly created with the help of shuffling positions of the numbers on the keyboard from 0 to 9 for each different users. Participants are asked to correctly typed 6-digit numbers using these specialized numeric keyboards. In training stage, each user had completed 30 trials to collect touch dynamics data for identification. These collected data are utilized to perform user's score through statistical methods at the decision making step. In verification stage, the developed application was tested with the participation of the total 30 users and then it was requested to perform separate verification experiments from the identified users. In addition, 5 users who are not defined in the system are requested to log in instead of previously defined users in order to measure the false acceptance rate. At the end of the experiment, a survey was conducted and user behavior was generally analyzed within the scope of developed model in order to deduce. As a result of experiments, False Reject Rate (FRR) was obtained as 0.16, False Acceptance Rate (FAR) as 0.28 and Equal Error Rate (EER) as 0.22.

1. GİRİŞ

Gelişen internet dünyası bireylerin yaşantısını kolaylaştırmak için farklı dijital deneyimleri birbiriyle entegre hale getirerek çevrimiçi platformlarda paylaşılan kişisel veri hacmini giderek arttırmıştır. Çevrimiçi platformları kullanan, internete erişimi olan kullanıcı sayısının her gün katlanarak artmasıyla bugün kullanıcıların hassas bilgileri farklı sistemlerle paylaşılır hale gelmiştir. Bilgisayarların taşınabilir hale gelmesi insanların mobil cihazlar ile çevrimiçi ortamda geçirdiği sürelerin artması sonucu insan bilgisayar etkileşimi farklı bir boyuta taşınmıştır. Bilgi sistemlerindeki bu gelişmeler ile paylaşılan hassas bilgilerin artması, beraberinde birçok güvenlik sorununu getirmiş ve bilgi güvenliği kavramını ortaya çıkarmıştır. Ancak, teknolojinin gelişme hızını, insanların bilgi güvenliği konusundaki bilinçlenme hızı ve bilgi güvenliği sistemlerindeki gelişmeler yakalayamamıştır. Bu nedenle, bilgi güvenliği alanında araştırma ve çalışmalar yapılarak farklı teknikler geliştirilmeye devam etmektedir.

Gelişen bilgi sistemleri ve artan güvenlik riskleri, dünyamızda kimlik hırsızlığı ve hassas verilerin ele geçirilerek ifşa edilmesinin yaygınlaşmasına sebep olmaktadır. Kullanıcı kimlik doğrulama işlemleri için standart bir araç olan geleneksel şifreleme yöntemleri kullanıcıların bilgi güvenliğini sağlama konusunda artık tek başına yetersiz kalmaktadır. Geleneksel parolalara dayanan kimlik doğrulama yöntemleri hala en yaygın kullanılan yöntem olmasına rağmen, düşük bir güvenlik düzeyi sunar ve kimlik hırsızlığı için kullanılan birden fazla saldırıya açıktır. Şifreler tarafından ortaya çıkan güvenlik açıklarını ortadan kaldırmak ve bilgi güvenliğini en etkin şekilde sağlamak için, insanın ayırt edici fizyolojik ve davranışsal özelliklerini temel alan biyometrik teknolojilere dayanan güvenlik stratejileri geliştirilmeye başlanmıştır.

Bugün dünyada giderek yaygınlaşan, dijital güvenlikten sınır güvenliğine kadar kullanılan, biyometrik teknolojiler artık, bireylerin kim olduğunu doğrulamak, bilinmeyen kişilerin kimliklerini tespit etmek ve çok daha fazlasını yapmak için kullanılmaktadır. Dijital dünyada öne çıkan kullanım alanı ise bilgi güvenliğinin

sağlanması için kullanılan biyometrik kimlik doğrulama yöntemleridir. Bu yöntemler, parmak izi tanıma, retina tanıma gibi kişileri fizyolojik olarak diğerlerinden ayırt etmeye yarayan fiziksel özellikler olabildiği gibi; imza, yürüyüş şekli, tuşlama ve dokunma dinamikleri gibi davranışsal özellikler de olabilmektedir. Bugün davranışsal biyometrik kimlik doğrulama yöntemleri, fiziksel kimlik doğrulama yöntemlerine kıyasla maliyeti düşük ve kullanışlı olduğu için, insan ekosisteminde her düzeyde giderek daha fazla uygulanabilir hale gelmektedir.

Mobil platformların hızlı bir şekilde benimsenmesi, mobil cihazlardaki uygulama ve bu uygulamalar aracılığıyla paylaşılan hassas veri çeşitliliğini artırmıştır. Örneğin, cep telefonları bugün insan yaşamının ayrılmaz bir parçası haline gelmiş, kullanıcının dijital kimliğini elinde tuttuğu ve güçlü bir kimlik doğrulama sistemi gerektiren cihazlardır. Bununla birlikte, günümüzde dokunmatik ekranlı mobil cihazlar, mobil pazarda daha büyük paya sahiptir. Bu cihazlar sayesinde, insanlar bankacılık işlemlerinden alışverişe, resmi işlemlerden sosyal medyaya kadar birçok ihtiyacını hızlıca giderebilir hale gelmiş, bir parmak hareketi ile istenilen anda ulaşılabilen ve verilerin paylaşılabileceği sanal ortamlar oluşmuştur. Kullanıcılar birçok kişisel ve hassas verilerini bu cihazlar aracılığıyla çevrimiçi dünya ile paylaşırlar. Bu noktada, bu sistemlere girişte ve işlemler sırasında, meşru kullanıcıların kimliklerini doğrulamak ve sahtekar kimlikleri tespit ederek kişisel bilgilerin korunmasını sağlamak önem arz etmektedir.

Mevcut dokunmatik ekranlı donanımların gittikçe artan çeşitli özellikleri sayesinde, kullanıcılar kredi kartı numarası, TCKN gibi birçok hassas bilgisini paylaşır hale gelmiştir. Bugün bu hassas bilgiler, saldırganlar tarafından gerek teknik gerek sosyal yöntemlerle ele geçirilmesi istenen cazip hedefler haline gelmiştir. Bu problemin önlenmesi için dokunmatik ekranlı mobil cihazlarda akıllı kullanıcı kimlik doğrulama mekanizmalarının geliştirilmesi ihtiyacı ortaya çıkmıştır. Geliştirilmesi gereken mekanizmanın hem kimlik doğrulamayı gerçekleştirebilmesi hem de sürekli doğrulama ile olası bir anomaliyi tespit edebilmesi hedeflenmektedir.

Bu tezin amacı, bir sistemde olası anormal bir davranışı veya davetsiz bir misafiri gerek sisteme girişte gerekse ikinci faktör kimlik doğrulama olarak sistem içerisinde tespit edip meşru bir kullanıcının davranışını, bu istenmeyen kullanıcının davranışından ayırt edecek davranışsal biyometrik kimlik doğrulama yönteminin, güvenli ve etkili bir kimlik doğrulama yöntemi olarak kullanılabilirliğini

göstermektir. Bugün birçok kullanıcı geleneksel güvenlik yöntemlerini kullanan sistemlere giriş yaparken, birbirine benzeyen hatta aynı şifreleri tekrar tekrar kullanmaktadır. Örneğin, kullanıcılar bankacılık için kullandığı şifrelerini çok daha güvensiz bir sisteme kayıt olurken de kullanabilmektedir. Bu da beraberinde birçok güvenlik sorununu getirmektedir. Bu tez kapsamında, bu yöntemlere alternatif olarak kullanıcıların ayırt edici davranışsal biyometrik verilerinden, mobil cihazlarla geçirilen süre düşünüldüğünde, en çok ve maliyetsiz şekilde veri toplanabilecek dokunma dinamiği değerleri kullanılarak, onlara özel üretilen adaptif bir numerik klavyenin örtük öğrenme yöntemi yardımıyla öğretilmesiyle, davranışsal biyometrik verilerin kullanıcı kimlik doğrulamada etkin birer çözüm olarak kullanılabileceği gösterilmeye çalışılmaktadır.

Altı ana bölümden oluşan bu tezde, ilk olarak insan bilgisayar etkileşimi incelenmiştir, ikinci bölümde ise geliştirilen uygulamada kullanılan klavyenin kullanıcılar tarafından istemsizce öğrenilmesinden yola çıkarak öğrenme psikolojisi ve örtük öğrenme yöntemi ele alınmıştır. Üçüncü bölümde uygulamanın temelini oluşturan bilgi güvenliği kavramına odaklanılmış ve güvenlik açıkları farklı tekniklerin kullanıldığı saldırı tipleriyle ele alınmıştır. Dördüncü bölümde, güvenlik tedbirlerinden kimlik doğrulama yöntemi incelenerek, günümüzdeki türleri açıklanarak incelenmiştir; beşinci bölümde literatür taraması sonucunda bulunan benzer çalışmalar hakkında bilgi verilmiştir; son bölümde ise geliştirilen çözüm için tasarlanan model ve bu modelden geliştirilen adaptif uygulama detaylı olarak incelenmiş, yapılan deneyler ve bu deneylerin sonuçları analiz edilerek davranışsal biyometrik kimlik doğrulama yöntemi araştırılmıştır.

2. İNSAN BİLGİSAYAR ETKİLEŞİMİ

İnsan bilgisayar etkileşimi, insanlar ve bilgisayarlar arasındaki ilişki ve etkileşimi inceleyen, yalnızca bilgisayar bilimlerinin değil endüstri, eğitim, antropoloji, sosyoloji gibi bilimlerin ortak fayda sağladığı disiplinler arası bir bilim dalıdır.

Bilgisayarlar hesaplamalara yardımcı olduğu için, gerek bilim insanları gerekse büyük endüstri firmaları tarafından ilk zamanlardan beri kullanılmaktadır. İlk zamanlarda devasa boyutlarda ama çok az işlem gücüne sahip bilgisayarlar giderek daha az yer kaplayan ama çok daha büyük işlem gücüne sahip olan donanımlar halini almıştır. Bilgisayarlar, 1960'larda ilk kişisel bilgisayarın üretimi, 1980 ve sonrasında da kişisel bilgisayarların giderek popülerleşmesi ile hemen herkesin hayatına dokunmaya başlamıştır. Bilgisayarların giderek gelişmesi ve kişiselleşmesi, bilim insanlarını onların daha kullanılabilir ve fonksiyonel olmaları için çalışmalar yapmaya itmiştir. Giderek daha kullanılabilir hale gelen ve mobilleşen bilgisayarlar ile internetin de hızla yaygınlaşması, kablosuz olarak kolay ve hızlı erişilebilir olması aracılığıyla insan bilgisayar etkileşimi önemli bir bilim alanı haline gelmiştir.

Günümüzde arabalardan evlere, cep telefonlarından çamaşır makinelerine kadar birçok donanım, bilgi işlem yapabilen, akıllı bilgisayarlar haline gelmiştir. Doğal olarak rutin hayatlarında bu bilgisayarla etkileşime giren insanların bu sistemleri anlaması, onlara doğru komutlar vermesi, aldığı tepkileri kolayca anlayabilmesi gerekmektedir. Bu noktada, giderek hayatımızın içine giren bilgisayarların tasarımı sırasında, yalnızca teknik ve fonksiyonel ihtiyaçları değil, aynı zamanda hitap ettiği kullanıcı kitlesinin kullanım ihtiyaçları da göz önüne alınmalıdır. Kullanılabilirlik olarak tanımladığımız bu özellik, insanların ürünleri daha kolay anlayıp, kolay kullanabilmeleri ve ürünlerden en fazla verim alabilmelerini sağlamak demektir. Bu nedenle, insan bilgisayar etkileşiminden bahsedilirken, hayatın hemen her alanında kullanılan, insanın ihtiyaçlarına göre şekillenen teknolojiler bu bilimin önemini göstermektedir.

İnsanların bu kadar aktif olarak bilgisayarlarla olan iletişimi, yeni araştırma alanlarının çıkmasına da katkı sağlamıştır. İnsanların kimlik tespiti ve

doğrulamasının yapılmasında, bilgisayarlarla girdiği etkileşimdeki özellikleri birer ayırt edici nitelik olarak kabul edilmeye başlanmıştır. İnsanların ihtiyaçlarına göre ergonomisi şekillenen cihazlar ve bu cihazları insanların kullanma stilleri izlenerek toplanan veriler analiz edilerek, kimlik doğrulama yöntemi olarak kullanılabilmektedir.

İnsan bilgisayar etkileşiminden ve kullanılabilirlikten söz edilirken adaptif sistemlere de değinmek gerekmektedir. Adaptif sistemler, ortama ve kullanıcısına göre davranışını değiştirebilen sistemlere denir. Kullanıcısının seviyesine göre değişebilen uygulamalar, ortam koşullarına göre uyarlanabilen sistemler örnek olarak verilebilir. Günümüzde akıllı cihazlarda bulunan sensörler ile sürekli veri toplama imkanı sağlanmakta, bu sayede de öğrenebilen ve uyarlanabilen sistemler geliştirilebilmektedir.

Tez çalışması kapsamında geliştirilen uygulamada kullanıcılara birbirinden farklı numerik birer klavye üretilerek, bu klavye öğretilmektedir. Kişiye özel üretilen bu klavyeler adaptif birer tasarım örneği sayılabilir.

3. ÖĞRENME PSİKOLOJİSİ

Öğrenme davranış bilimi, evrim teorisi, davranışsal ekoloji ve bilgisayar bilimleri gibi birçok disiplinde araştırmaların ana odak noktasıdır. Öğrenmenin tanımı her ne kadar bu disiplinler içinde ve arasında farklılaşsa da öğrenme genel olarak deneyim sonucu ortaya çıkan insan davranışındaki nispeten kalıcı bir değişiklik olarak tanımlanmaktadır [1]. Bu değişiklik gitar çalmayı öğrenmek gibi olumlu bir davranış değişikliği olabilirken aynı zamanda yüksekten korkmayı öğrenmek gibi olumsuz bir davranış değişikliği de olabilir. Öğrenme psikolojisi, insanların nasıl öğrendikleri ve çevreleriyle nasıl etkileşime girdiği ile ilgili bir dizi konuya odaklanmaktadır. Bir öğrenmenin gerçekleşmesi için üç unsur ele alınmaktadır: Kişinin davranışında bir değişiklik olmalı, bu değişiklikler kalıcı bir etki yaratmalı ve bu değişiklik kişilerin etrafındakilerle girdiği etkileşimin sonucu olmalıdır [2]. Örneğin yaşlanma sonucunda ortaya çıkan davranış değişiklikleri yukarıda belirtilen üç unsura göre incelendiğinde öğrenme olarak kabul edilmez.

Öğrenme eylemi davranışçılara ve diğer kuramcılara göre farklı yöntemler aracılığıyla gerçekleşmektedir. Frensch & Runger, psikolojideki öğrenme yöntemlerini ikiye ayırırlar: Açık öğrenme ve örtük öğrenme [3]. Bu bölümde açık ve örtük öğrenme yöntemleri ele alınmakta, tez kapsamında geliştirilen uygulamada bulunan adaptif numerik klavyelerin öğretilme adımının bu yöntemle ilişkisinden bahsedilmektedir.

3.1 Açık Öğrenme

Açık öğrenme, öğrenmeye yönelik bilinçli bir karar ve öğrenme çabası hakkında net bir farkındalığın olduğu öğrenme yöntemidir. Ellis'e göre, bu öğrenme yöntemi bir yapı arayışında olan bireylerin bir hipotez oluşturup onu test ettiği bilinçli bir süreçtir; bu süreçte kavramlar, kurallar, prensipler ve kalıplar doğrudan öğrenenlere sunulur ve onlardan aktif olarak bu yapıyı aramaları istenir [4]. İnsanlar genellikle belirli bir olguyu açıklayan basit hipotezler oluşturmaya çalıştıkları için açık öğrenme hataya karşı daha az toleranslıdır. Açıklanmaya çalışılan olgular istikrar

gösterdiğinde ve değişkenler arasındaki ilişkiler belirgin olduğunda, basit hipotez tezleri doğru olabilir, ama bu ilişkiler daha az belirgin olduğunda hipotezlerin test edilmesi çok verimli olmaz [5]. Açık öğrenmeye bir öğretmenin öğrencilerine Matematik dersinde bir konu anlatması ya da bir kişinin yemek kitabından bakarak pişirmek istediği yemeğin tarifini öğrenmesi örnek olabilir.

3.2 Örtük Öğrenme

Genellikle farkında olmadan öğrenme olarak tanımlanan örtük öğrenme kuramcılar tarafından farklı şekilde tanımlanmaktadır. Berry ve Dienes örtük öğrenmeyi her yönüyle ele alarak şu şekilde açıklamıştır: Bir birey yeni bilgileri elde etme niyeti olmadan, farkında olmadan elde ediyorsa ve bu şekilde ortaya çıkan bilgiyi ifade etmekte zorlanıyorsa, gerçekleşen öğrenme örtüktür [6]. Bu noktada, örtük öğrenme tamamen bilince dayanan açık öğrenmeden ayrılmaktadır. Örtük öğrenme, kişinin ortamdaki belirli düzenlere karşı duyarlı hale geldiği süreçtir. Düzenleri öğrenmeye çalışmadan, birilerinin bu düzenleri öğrendiğini bilmeden bilinçsizce gerçekleşmektedir. Günlük hayatta edinilen deneyimler, örtük öğrenmenin her yerde ortaya çıkan bir kavram olduğunu göstermektedir. Gerçek hayatta örtük öğrenme, bir anadil ve ikinci dili öğrenme, kategori hazırlama, kavram öğrenme, okuma-yazma öğrenme gibi fiziksel dünya ve sosyal beceriler hakkında bilgi kazanımlarını içeren temel bir süreçtir. Bisiklete binmeyi öğrenmek, çubuk kullanarak yemek yemek ya da araba kullanmak günlük hayatta örtük öğrenme kategorisinde sınıflandırılan aktivitelerdir. Bunlar bireylerin sözlü olarak tarif etmekte zorlandıkları karmaşık motor becerilerde ustalaşmayı içermektedir. Bireylerin bilişsel süreçleri raporlama yeteneği ve bu süreçleri içeren davranışları arasındaki ayrışmalar sadece bu eylemlerle sınırlı değildir, bu ayrışmalar aynı zamanda üst düzey bilişe kadar uzanmaktadır. Buna örnek olarak, ana dilini konuşan bireylerin çoğu zaman konuşurken uyguladıkları dilbilgisi kurallarını ifade edememeleri verilebilir.

Örtük öğrenme araştırmaları temel olarak üç deneysel paradigmaya odaklanmaktadır: Yapay gramerler, dizi öğrenme ve karmaşık sistemlerin kontrolü [7]. Bu paradigmaların her birinde yapılan çalışmalar, katılımcıların bilginin tam olarak ne olduğunu bilmeden, bu karmaşık bilgiyi çeşitli görevler için kullanmayı öğrenebileceklerini göstermektedir. Bu paradigmalardan en eskisi ve bugün hala en çok araştırma yapılmaya devam eden yapay dilbilgisi öğrenimidir. Bu alanda yapılan

ilk deney Reber tarafından 1967 yılında gerçekleşmiştir. Reber'in bu öncü deneyler dizisinde, katılımcılardan sonlu dilbilgisi kuralları tarafından üretilen bir harf dizisini ezberlemeleri istenir. Yapılan denemeler üzerine katılımcılar, dilbilgisi kurallarına uyan dizileri ezberlemenin rastgele dizileri ezberlemeye kıyasla daha kolay olduğunu belirtirler. Ayrıca katılımcılar, her deneme sonrasında birtakım dilbilgisi bilgileri edindiklerini belirterek dilbilgisi kurallarına uyan ve uymayan dizileri tesadüfen değil bilerek ayırt edebilir hale gelirler. Her ne kadar katılımcıların dilbilgisi kuralları hakkında bilgi edinerek davranışları belirlense de deney sonucunda farkında olmadan öğrendikleri bu dilbilgisi kurallarını ifade etmekte zorlanırlar. Dizileri sınıflandırma ve bu sınıflandırma için gerekli kuralların sözlü ifadeleri arasındaki ayrımı Reber örtük öğrenme olarak açıklamaktadır [8].

İkinci paradigma olan dizi öğrenme paradigması da öğrenme eylemini deneylerle açıklayan bir diğer yöntemdir. Paradigmanın ilk çalışmaları Nissen ve Bullemer tarafından 1987 yılında gerçekleştirilmiştir, bu iki kuramcının yaptıkları deneyde, katılımcılardan sıralı olarak yapılandırılmış ve tipik olarak olayların görsel sıralarını oluşturan her bir elemente tepki göstermeleri istenir. Her denemede, katılımcılar bilgisayar ekranında çeşitli konumlardan birinde bir uyarıcı görür ve onlardan ilgili tuşa mümkün olduğunca hızlı ve doğru bir şekilde basmaları istenir. Onlar için bilinmeyen, art arda uyaranların dizisi yinelenen bir modeli izler ve sonlu dilbilgisi gibi ardışık uyaranlar arasında izin verilen geçişleri açıklayan bir dizi kural tarafından yönetilmektedir. Yapılandırılmış denemelere maruz kalan katılımcıların, rastgele bir denemeye maruz kalanlara göre tepki verme süreleri daha hızlıdır. Bu nedenle, kalıp bilgileri sonucunda cevaplarını daha iyi bir şekilde hazırlayabilmektedirler. Her ne kadar yapılandırılmış denemelere tepki verme hızları fazla olsa da, katılımcılar farkında olmadan öğrendikleri kalıpları sözlü bir ifade ile tarif etmekte zorlanırlar [9].

Üçüncü paradigma olan dinamik sistemlerin kontrolünde, deneyin katılımcıları giriş değişkenlerinde oynama yaparak bir çıkış değişkenini kontrol etmek için bilgisayarla etkileşimini öğrenmeleridir. Örneğin, katılımcılar işlenen hammadde miktarı gibi değişkenleri manipüle ederek benzetilmiş bir şeker fabrikasının üretimini belli bir sınır çerçevesinde tutmayı öğrenirler. Yine, bunu girdi değişkenlerini çıktılarla ilişkilendirmek için bilgisayarın karmaşık formülünün farkında olmadan yaparlar

[10]. Tüm bu deneysel paradigmalarda katılımcılar, altta yatan yapının farkında olmadan karmaşık bilgiyi kullanmayı öğrenirler.

Örtük ve açık öğrenmenin sonucu olarak ortaya çıkan bilgi birçok önemli konuda farklılık göstermektedir. Bilinen bir fark, açık bilginin sözlü ifade edilme şekli örtük bilgiye göre çok daha kolaydır. Örneğin, kimya dersi için ezberlediğimiz periyodik tablo hakkında konuşmak oldukça kolaydır, fakat bir çay bardağını almak için kullandığımız belirli hareketleri açıklamamız oldukça zordur. Sonuç olarak, açık bilgi bilinenleri başkasına iletme yeteneği konusunda önemli bir rol oynamaktadır. Buna bağlı olarak, örtük bilginin açık bilgiden çok daha belirgin bir şekilde kendini duygusal tepkilerle göstermesi muhtemeldir. Aynı zamanda örtük bilgi, açık bilgiden çok daha farklı bir biçimde dağıtılabilir ve genellikle ortamdaki işaretlerle otomatik olarak tetiklenir.

Günlük hayattan birçok örnekle açıklanabilen örtük öğrenme yöntemi tez kapsamında geliştirilen uygulamanın arka planını oluşturmaktır. Geliştirilen mobil uygulamada; katılımcılara özel, rakamların yerleri rastgele değişen numerik klavyeler üretilmiş, her bir katılımcıdan hedeflenen 6 karakterli rakam dizilerini sürekli olarak girmesi istenerek, katılımcıların bu klavyeleri farkında olmadan öğrenmeleri incelenmiştir. Katılımcıların rakamları farkında olmadan doğru bir şekilde tuşlayarak öğrenmesi de örtük öğrenme yöntemine uygulamalı bir örnek olmuştur.

4. BİLGİ GÜVENLİĞİ VE GÜVENLİK AÇIKLARI

Teknolojinin yaygın kullanımıyla beraber bilgi ve bilginin doğru koşullarda saklanması ve en etkili yöntemlerle korunması için farkındalık yaratılması konusu giderek önem kazanmaktadır. Günümüz bilgi toplumunda değerli bir varlık olarak kabul edilen bilgiyi saklamak ve korumak için "Bilgi Güvenliği" kavramı ortaya çıkarak farkındalık konusunda kritik adımlar atılmaya devam etmektedir.

4.1 Bilgi Güvenliği

Bilgi güvenliği ilk etapta sadece bilgiyi saklamak ve korumak ile ilgili gözükse de, Ulusal Standartlar ve Teknoloji Enstitüsü tarafından bilgi güvenliği "bilgi ve bilgi sistemlerinin yetkisiz erişim, kullanım, açıklama, aksaklık, değişiklik veya imhadan korunması" olarak tanımlanmaktadır [11].

Bilgi güvenliği kavramı üç temel prensip üzerine kuruludur: Gizlilik, Bütünlük ve Kullanılabilirlik. Bilgi güvenliğinin sağlanması için bu üç prensibin aynı anda gerçekleşmesi gerekmektedir. Gizlilik, hassas bilgilere yalnızca yetkili bir kişi tarafından erişilmesini ve sahip olma yetkisi bulunmayan kişilerden uzak tutulmasını sağlar [12]. Gizlilik ilkesi parolalar, kullanıcı adları, erişim kontrol listeleri ve şifreleme gibi güvenlik yöntemleri kullanılarak uygulanmaktadır. Bilginin istenmeyen kişiler tarafından ele geçirilmesi halinde oluşacak zararın derecesine göre sınıflandırılması yaygındır ve sonrasında güvenlik önemleri bu sınıflandırmaya göre uygulanmaktadır. Bilgi güvenliğinin bütünlük prensibine göre, bilgilerin orijinal amaçlarına uygun bir şekilde güvenliği sağlanmalıdır. Bilgiyi alacak olan kişi sadece bilgiyi oluşturan kişinin istediği bilgiye sahip olmalıdır, bilgiler sadece yetkili kişiler tarafından düzenlenir ve onlar istediği sürece orijinal halinde kalırlar. Bütünlük, veri şifreleme ve hashing gibi güvenlik yöntemleri kullanılarak uygulanmaktadır. Verilerdeki değişiklikler sunucu çökmesi ya da elektromanyetik darbeler gibi insan kaynaklı olmayan olayların bir sonucu olabilir. Bu yüzden veri bütünlüğünü sağlamak için yedekleme sistemlerinin olması oldukça önemlidir. Ana prensiplerden sonuncusu olan kullanılabilirlik, bilgi ve kaynakların ihtiyacı olan kullanıcıların

kullanımına açık olmasını sağlayan prensiptir. Bir kullanıcı ihtiyacı olan bilgiye ihtiyacı olan zamanda ulaşamıyorsa kullanılabilirlik prensibine göre o bilgi güvende değildir. Kullanılabilirlik ilkesi donanım bakımı, yazılım düzeltme ve ağ optimizasyonu gibi yöntemlerle uygulanmaktadır. Bu ilke yedekleme, RAID (Ucuz Disklerin Artıklıklı Dizisi) ve yük devretme gibi işlemlerde herhangi bir sorun ortaya çıktığında oluşan zararları azaltmak için kullanılmaktadır [13]. Belirtilen üç ana prensibin aynı anda gerçekleşmesi bilginin korunması için büyük bir önem arz etmektedir. Bu prensiplerden bir tanesinin eksik olduğu durumda kullanıcı bilgilerinin güvenliğinde açıklık olduğuna işaret edilmektedir.

4.2 Kişisel Verilerin Önemi

Dijitalleşen dünyada kişisel bilgilerin kullanımı giderek yaygınlaşmaktadır, bugün bir siteden alışveriş yapmak için bile kullanıcıların birçok kişisel verisini paylaşması sistemler tarafından istenmektedir. Kişisel veri, Avrupa Akreditasyon Merkezi'nin (European Accreditation) Kişisel Veri Koruma Politikası'na göre "ad, adres, doğum tarihi, e-posta, IP adresi veya telefon numarası gibi bir kişiyi doğrudan tanımlamaya izin veren bilgiler veya kişiyi dolaylı olarak tanımlayan başka bilgilerle kullanıldığında o kişinin tanınmasını sağlayan veri bütününe" denilmektedir [14]. Kişisel veri süreci ise bu veri ile ilgili yapılan tüm etkinlikleri kapsamaktadır. Örneğin verinin toplanması, kaydedilmesi, saklanması, kullanılması, değiştirilmesi, sınırlandırılması ve imha edilmesi gibi. Olası bir veri kaybını önlemek adına günümüzde hem kurumlar hem de birçok resmi yönetim tarafından farklı çalışmalar gerçekleştirilmektedir. Firmalar verinin saklanması gibi veri sürecini kapsayan diğer eylemlerin de yer aldığı yönetmelikler hazırlayarak bu konuda çalışanlarını bilgilendirirler. Resmi yönetimler ise, kişisel veri ile ilgili süreçler kapsamında kişisel veriyi saklama ve korumaya yönelik kanunlar üzerinde çalışırlar. Bu bağlamda, Türkiye'de 2016 yılında 6698 sayılı Kişisel Verileri Koruma Kanunu yayınlanmıştır; bu kanunda kişilerin temel hakkı olan bilgilerin saklanması ve korunması ele alınarak olası ihlalleri önlemek adına birtakım kurallar vurgulanmaktadır [15].

4.3 Güvenlik Açıkları

Bilişim dünyasında, bilgi ve bilginin korunması için alınan önlemler kritik bir konu olarak ele alınmaktadır. Her gün giderek artan cihaz ve internete bağlı kullanıcı sayısı, artan siber saldırılarla birlikte bilgi güvenliğinin sürdürülebilir bir şekilde sağlanması konusunda endişe yaratmaktadır. Çünkü bilgi yeteri kadar korunmadığında bilginin güvenliği tehlikeye girebilir ve bu durum güvenlik açığına sebep olmaktadır. Bu güvenlik açıklarından yararlanılarak yapılan saldırıların sonuçları hem bireyler hem de kurumlar için oldukça kritiktir. Bireyler için bu durum kimlik hırsızlığına ve finansal geçmişinin ele geçirilmesine yol açar ve kredi notuna zarara kadar büyük sorunlar doğurur. Kurumlar için güvenlik açıkları çok büyük mali cezalar, itibar ve iş kaybına yol açabilir ve bu saldırılardan arınmak uzun süren maliyetli bir süreç olabilir. Günümüzde ne yazık ki teknolojinin gelişim hızına ayak uyduramayan bilgi güvenliğini koruma yöntemleri çeşitli güvenlik açıklarının ortaya çıkmasına sebep olmaktadır. ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) güvenlik açığını "bir bilgi sistemi, sistem güvenlik prosedürleri, iç kontroller ile uygulamada yer alan ve tehdit kaynakları tarafından istismar edilebilecek bir zayıflık" olarak tanımlamaktadır [16]. Bilgi güvenliğindeki zayıflıklar teknik olabileceği gibi insan hatalarından da kaynaklanabilir. Bu zayıflıklar sonucunda "bilgi kaynaklarına veya hizmetlerine yetkisiz erişim sağlama veya bilgi sistemlerine zarar verme veya vermeye çalışma denemeleri" olarak tanımlanan güvenlik saldırıları ortaya çıkmaktadır [17]. Teknik saldırılar ve insan kaynaklı saldırılar olmak üzere güvenlik saldırıları da kendi içerisinde türlere ayrılmaktadır.

4.3.1 Sosyal mühendislik saldırıları

Hassas bilgileri korumak için alınan önlemlerde büyük bir artış ve verimlilik olmasına rağmen, insanlar hala güvenlik zincirinin manipüle edilebilir en zayıf halkası olarak görülmektedir. 2015 yılında IBM Security Service tarafından yayınlanan raporda güvenlik açıklarının %95'inden fazlasının insan hatalarından kaynakladığı belirtilerek bilgi güvenliği kapsamında kullanıcı ihmallerinin giderek arttığı vurgulanmaktadır [18]. Günümüzde saldırganlar tarafından insanların bu zayıflıkları hedef alınarak ve birbirinden farklı manipülasyon yöntemleri kullanılarak hassas bilgiler ele geçirilmektedir. Sosyal mühendislik, bilgi güvenliği bağlamında insanları manipüle ederek gizli ve hassas bilgilerinin ele geçirildiği en yaygın saldırı

türlerinden biridir. Tamamen insan etkileşimine dayanan, insanları normal güvenlik prosedürlerini kırmaları için kandıran ve teknik bir yöntem olmayan sosyal mühendislik, güvenlik açığı yöntemleri arasında gerçekleşmesi diğer yöntemlere göre daha kolaydır.

Sosyal mühendisler kullanıcılardan hassas bilgi almak için farklı teknikler kullanmaktadır. Bu kapsamda yapılan saldırılar literatürde iki farklı kategoriye ayrılmaktadır: İnsan tabanlı saldırılar ve bilgisayar tabanlı saldırılar [19]. İnsan tabanlı sosyal mühendislik saldırısında saldırgan, mağdur ile etkileşime girerek bilgiler toplar, bu tür saldırılar tamamen saldırganın kandırma yöntemine dayanmaktadır. Kullanıcı adı, şifre, kredi kartı numarası, diğer banka bilgileri, ID, doğum tarihi gibi önemli bilgiler şahsen veya telefon yoluyla toplanabilir. İnsan kaynaklı bu saldırılar tamamen karşı tarafı kandırmayı esas alarak gerçekleşmektedir, kısaca mağdur kişinin davranışlarındaki ya da o anki psikolojisindeki zayıflıklardan yararlanılarak bu tür saldırılar yapılmaktadır. Bu saldırılar genelde güvenilir bir kişi olarak maskelenen saldırganlar tarafından gerçekleşebilir. Bu saldırı türünün en yaygın örneği bir bilgisayar sistemine erişmek için acil yardıma ihtiyacı olan yönetici ya da üst düzey bir müdür gibi görünerek saldırı gerçekleştirmektir. Bu teknik, asistan gibi daha alt pozisyonlarda çalışıp üst düzey çalışanlara yardım etme sorumluluğuna sahip olan kişileri hedef almaktadır. Saldırganlar bu şekilde yani karşı tarafı kandırarak bir müdür ya da yöneticinin şifre bilgilerini kolayca ele geçirebilirler.

Teknik olmayan bu yaklaşıma dayalı saldırıların en yaygın yöntemi ise şahsen gerçekleştirilen "Omuz Sörfü (Shoulder Surfing)" adı verilen, kullanıcıların kimliğini doğrulamak için kullanılan şifrelerin saldırganlar tarafından teknik bir destek almadan doğrudan gözlemler yapılarak kullanıcı şifrelerini öğrendikleri yöntemlerdir [20]. Omuz Sörfü daha kalabalık yerlerde bilgi almanın en etkili yoludur, çünkü şifresini giren kullanıcının yanında durmak ve onun kimliğini doğrulamak için girdiği şifre ya da PIN'i izleyerek ele geçirmek diğer bilgi güvenliği saldırılarına göre çok daha basittir. Örneğin, ofiste faturalarını ödemek isteyen bir kişi etrafındaki kalabalığa aldırış etmeden telefonunda banka uygulamasını açar ve kullanıcı adı, şifre gibi önemli bilgilerini yazarak giriş yapar, bu sırada yanından geçen çalışma arkadaşı bu bilgilerini görür ve ele geçirir. Gözlediği bilgileri kullanarak sonradan uygulamaya giriş yaptığında istediği birçok işlemi gerçekleştirebilir.

Bilgisayar tabanlı sosyal mühendislik saldırıları bilgisayar yazılımı yardımıyla elde edilmek istenilen bilgileri ele geçirmek için yapılan saldırı türüdür. İnsan tabanlı sosyal mühendisliğin aksine, bu tür saldırılarda mağdurla birebir etkileşim söz konusu değildir [21]. Bilgisayar tabanlı sosyal mühendislik saldırıları arasında sahte e-postalar, pop-up pencere saldırılar ve oltalama (phishing) gibi birbirinden farklı saldırı çeşitleri yer almaktadır. Bu tür içinde en yaygın saldırı tipi "Oltalama" adı verilen, meşru bir kurumdan ya da adresten geliyor gibi gözüken sahte e-posta kullanarak kimlik hırsızlığı yapmayı, gizli ve kişisel bilgileri ele geçirmeyi amaçlayan tekniktir [22]. Oltalama genellikle bankaları, kredi kartı şirketleri veya diğer kurumları taklit eden saldırganların gönderdiği e-postaları içermektedir. Örneğin, saldırgan, bir bankadan e-posta gönderir gibi mağdura gönderim yaparak hesap numarası veya PIN gibi bilgilerini ele geçirebilir. Oltalama, sadece sahte e-postaları içermez, hassas verileri ele geçirmek amacıyla gerçek sistemleri taklit etmek için tasarlanmış sohbetler, sahte sosyal medya hesapları ve web-siteleri de oltalamanın konusu olabilir. Bu tür bir saldırı sahte bir e-posta iletisi ile başlar, saldırganlar adres benzerliğini veya bir kurumun logosunu kullanarak kullanıcıların şifre, kredi kartı numarası gibi hassas bilgilerine erişim sağlarlar. Saldırganların yolladıkları mailler genellikle güvenli bir siteye ait gözüken bir bağlantı içerir. Tanıdık görünen bu linke tıkladığında karşılaştığı sayfaya güvenen mağdur kullanıcı adı, şifre ve PIN gibi bilgilerini paylaşmaktan çekinmez ve saldırıya uğrayarak farkında olmadan bilgilerini ele verir. Bir diğer yaygın oltalama örneği, saldırganlar tarafından farklı ülkeye taşınma, iş bulma imkanı sağlayan orijinal görünümlü e-postalardır. Bu maili alan mağdurlar ülke dışına çıkmak için gönderilen mailde belirtilenleri yaparak banka bilgileri, kimlik bilgileri gibi kritik bilgilerini saldırganlarla fark etmeden paylaşırlar.

Saldırganların elde etmek istedikleri bilgilere ulaşması, her zaman omuz sörfü, oltalama ya da bir yazılımın güvenlik açığından yararlanarak mümkün olmayabilir. Parola kuralları ve şifreleme gibi etkin güvenlik uygulamaları sayesinde hedefine ulaşamayan saldırganlar farklı yöntemlere yönelebilirler. Bu yöntemlerden bazıları: kaba kuvvet saldırıları, casus yazılımlar, sözlük saldırıları ve şifre saldırılarıdır.

4.3.2 Şifre saldırıları

Şifreler ATM'ler, internet hizmetleri ve cep telefonlarında kimlik doğrulama vb. gibi çeşitli bilgi işlem uygulamalarında önemli bir rol oynamaktadır. Şifreleri kullanmanın temel amacı, yetkisiz kullanıcıların sisteme erişimini engellemektir. Bu tür uygulamalarda parolalar gereklidir, fakat yine de geleneksel parola sistemlerindeki birçok hata sebebiyle kullanıcılar açısından çok güvenli olmadıkları düşünülmektedir. Bunun sebebi ise birçok sisteme yapılan büyük çaplı saldırıların şifre saldırılarından kaynaklamasıdır.

Bugün kullanıcılar, birçok web-sitesine ve internet ağına girerken uzun ve karmaşık şifreler belirlemeleri konusunda bilgilendirilmektedir. Şifresi zayıf ve tahmin edilebilir olan kullanıcılar giriş yaptıkları esnada şifrelerini değiştirmek ve güçlendirmek konusunda uyarılmaktadır. Her ne kadar bu yöntem giderek yaygınlaşsa da şifre saldırıları günümüzde bilgi güvenliği saldırıları arasında en çok kullanılan türlerden biri olarak kabul edilmektedir. Şifre saldırıları kullanıcı şifrelerini doğrudan tahmin etme ve şifreleri kırma olarak kendi içerisinde ikiye ayrılmaktadır. En yaygın şifre saldırısı türü olan şifre tahmin etme yöntemi, kullanıcıların şifrelerini manuel ya da otomatik yöntemler kullanarak lokalden ya da uzaktan tahmin etmesidir. Günümüzde, hala internet üzerindeki birçok ağ uzun ve karmaşık şifreler gerektirecek şekilde yapılandırılmamıştır, bu durum bir saldırganın istediği bir ağa erişmesini oldukça kolaylaştırmaktadır. Kullanılan tüm kimlik doğrulama protokolleri de bu saldırılara karşı eşit oranda etkili değildir. Örneğin, LAN Manager kimlik doğrulaması küçük ve büyük harfe duyarlı olmadığı için orayı hedef alan saldırıda tahmin edilmesi gereken parolada küçük veya büyük harf olmadığı dikkate alınmaz. Şifre tahmin etme saldırılarını hem çevrimiçi hem de çevrimdışı gerçekleştirebilmek mümkündür. İnternetteki her sunucunun kayıtlarına çevrimiçi bir şifre tahmini saldırısı riski bulunmaktadır. Bu tahmini saldırı, kimlik bilgilerini kullanarak uzaktan giriş yapmaya çalışan sürekli bir deneme dizisidir. Çevrimdışı bir parola tahmin etme saldırısında ise, saldırgan birtakım sistem veya uygulamaya giriş bilgileri, kullanıcı adı veya şifre bilgilerini alır ve sonra kendi makinelerinde şifreleri tahmin etmeye çalışabilir. Çevrimdışı gerçekleşen bu tahmin durumunda, hedef sistemden elde edilen bilgiler ile makinedeki bilgilerin eşleşip eşleşmediği kontrol edilerek saldırı yapılmaktadır [23].

Şifrelerin tahmin edilmesi için saldırganlar tarafından birçok farklı yaklaşım ve otomatik şifre tahmin programları kullanılmaktadır. En fazla zaman alan ve en başarılı saldırı yöntemi, ele geçirilmek istenen şifre için olası her karakter kombinasyonunun denendiği kaba kuvvet saldırılarıdır. Şifre kırma yöntemi de yine saldırganlar tarafından tercih edilen şifre saldırılarından biridir. Şifre kırma işlemi parolanın art arda tahmin edilmesiyle gerçekleşmektedir, genellikle parola başarılı bir şekilde bulunana kadar bilgisayarın çok sayıda birleşimi denediği bir bilgisayar algoritması kullanılarak yapılmaktadır. Kırma işleminin yapılmasının altında yatan en önemli neden kullanıcının haberi olmadan cihazına yetkisiz bir şekilde erişim sağlamaktadır. Bu durum bankacılık bilgilerine erişmek amacıyla şifreleri çalmak gibi siber suçlarla sonuçlanmaktadır.

4.3.3 Kaba kuvvet saldırıları

Kaba kuvvet (brute force) saldırısı, bir kullanıcı şifresi veya kimlik bilgilerini ele geçirmek için kullanılan deneme yanılma yöntemidir. Bir parolayı tahmin etmek için mümkün olan her harf, sayı ve karakter kombinasyonunu kullanarak tekrarlanan oturum açma girişimlerini içerir. Saldırganlar bu yöntemle bir sistemin hesaplarına erişebilir, ardından veri çalabilir, hesapları kapatabilir veya başka bir türde saldırı gerçekleştirebilir. Literatürde kaba kuvvet saldırılarının, zaman alan bir yaklaşım olmasına rağmen yanıltıcı olmadıkları kabul edilmektedir. Kaba kuvvet saldırılarının manuel olarak gerçekleştirilmesi oldukça zordur. Bunun yerine, saldırganlar, sistemlere yönelik binlerce deneme girişimini gerçekleştiren ve otomatik pilotta çalışan, bot adı verilen basit kodlar yazarlar. Tipik olarak, bu botlar saldırganlar tarafından özel olarak yazılıp pek çok saldırıya uğramış makineye kolayca dağıtılmak üzere tasarlanmıştır. Bu bot veya bot grupları, binlerce şifre üreten veya bir kelime listesi kullanan ve diğer yaygın olarak erişilebilen araçlarla birlikte çalışmaktadır [24]. Botun gerçekleştirmesi gerekenler programlama açısından çok temeldir. Örneğin, bazı parametreler ayarlanmalıdır (sitenizin giriş formuna erişim), bir talep de bulunulmalıdır (bir kullanıcı adı ve şifre kombinasyonu deneyin) ve yanıtı kontrol etmelidir (çalışıp çalışmadığını kontrol edin) ve ardından başarılı olana kadar tekrarlamak için ayarlama yapılmalıdır.

Kaba kuvvet saldırıları da birbirinden farklı şekilde gerçekleşebilir. Örneğin, kimlik bilgilerinin geri dönüşümü kaba kuvvet saldırı çeşitlerinden biridir; bu türde önceki

saldırılardan gelen kullanıcı adları ve parolalar kullanılmaktadır. Ters kaba kuvvet saldırıları ise bu türe ikinci bir örnektir. Burada saldırı kullanıcı adının değil, bilinen bir değer olarak kullanıcının parolasının bilinmesiyle başlamaktadır. Şifreye sahip olan saldırgan daha sonra doğru kullanıcı adını bulmak için normal kaba kuvvet saldırısı ile aynı düzeni izleyecektir. Üçüncü tür ise, en çok kullanılan şifrelerin veya sayısal dizilimlerin (12345678, qwerty gibi) denenerek gerçekleştirildiği saldırı türüdür. Kaba kuvvet saldırıları arasında en yaygın olan dördüncü türe sözlük saldırıları (dictionary attack) adı verilmektedir. Sözlük saldırıları kimlik doğrulama mekanizmasını çok sayıda olasılık deneyerek yenmeye çalışan bir saldırı türüdür. Sözlük saldırıları, kaba kuvvet saldırıların aksine bütün olasılıkların detaylı bir şekilde arandığı saldırılardır [25]. Bu tür saldırılarda sözlükteki kelimeler listesinden tipik olarak türetilmiş ve başarılı olması en muhtemel olasılıklar kullanılmaktadır.

4.3.4 Casus yazılımlar

Casus yazılım (spyware), kullanıcının izni olmadan bir bilgisayar veya ağ hakkında bilgi toplayan ve paylaşan bir tür kötü amaçlı yazılımdır. Orijinal yazılımın bir bileşeni ya da doğrudan kötü amaçlı bir yazılım üzerinden yanıltıcı reklamlar, web siteleri, e-posta, anlık iletiler veya doğrudan dosya paylaşım bağlantıları kullanılarak bu tür saldırılar gerçekleştirilebilir. Diğer kötü amaçlı yazılım türlerinden farklı olarak, casus yazılımlar kullanıcı bilgilerini ele geçirmek isteyen reklam verenler veya şirketlerin yanı sıra suç örgütleri tarafından da yoğun bir şekilde kullanılmaktadır. Kaynağından bağımsız olarak, casus yazılım kullanıcıdan gizlenir ve algılaması genellikle zordur; ancak bozulmuş sistem performansı ve istenmeyen bir davranışın sıklığı (yönlendirilmiş tarayıcı ana sayfası, pop-up'lar vb.) gibi belirtileri mevcuttur. Casus yazılımlar, kullanıcı bilgilerini ilgili reklam verenlere ya da diğer taraflara satmak için kullanılmaktadır. Bu yazılımlar, internette gezinme alışkanlıkları ve indirme etkinliği dahil olmak üzere hemen hemen her türden bilgiye erişebilirler. Casus yazılımla ilgili en büyük endişe, varlığının tespit edilebilir olup olmadığına bakılmaksızın, kullanıcının hangi bilgilerinin yakalandığı, gönderildiği veya kullanıldığı hakkında herhangi bir bilgisinin olmamasıdır.

Casus yazılım, kullanıcının adı, adresi, şifreleri, banka ve kredi kartı bilgileri ve sosyal güvenlik bilgileri gibi kişisel ayrıntıları elde etmek için tuş kaydediciler kullanabilir. Dosyaları sistemin sabit diskine tarayabilir, diğer uygulamaları

izleyebilir, ek bir casus yazılım yükleyebilir, çerezleri okuyabilir ve sistemin internet ayarlarını değiştirebilir. Ayarlardaki bu değişim bağlantı hatalarına veya bilgisayarda teknik arızalara neden olabilir. Arızalanan cihazları yeniden kurmadan bu değişiklerin giderilmesi oldukça zordur.

Kullanıcıları kandırmak için birbirinden farklı tekniklerin kullanıldığı dört ana casus yazılım türü bulunmaktadır. Bunlardan ilki, reklam destekli bilgisayar yazılımıdır (Adware). Bu tür casus yazılımlar kullanıcının ilgisini çeken hizmet ve ürünleri önceden tahmin etmek amacıyla tarayıcısının geçmişini ve indirmelerini izlemesidir. Reklam destekli bu yazılım, kullanıcılara aynı veya benzer ürün ve hizmetlerin reklamlarını gösterir ve onları bu reklamlara tıklamaya ya da herhangi bir satın alma yapmaya ikna eder. Bu yöntem pazarlama amacıyla kullanılır ve cihazları yavaşlatmaktadır. İkinci tür, Truva adı verilen kötü amaçlı yazılımların meşru bir yazılım görünümünde kendilerini gizledikleri bir türdür. Örneğin, Truva atları indirme sırasında bir Java güncellemesi olarak görünebilir, bu kötü niyetli yazılım üçüncü şahıslar tarafından kontrol edilir ve daha çok kimlik numarası, kredi kartı bilgileri gibi kullanıcıların hassas bilgilerine erişmek için kullanılmaktadır. Üçüncü tür, çerezlerin takip edilmesidir; bunun amacı kullanıcının yaptığı aramaları, geçmişi ve indirmeler gibi web aktivitelerini pazarlama amacıyla izlemektir. Son casus yazılım türü sistem görüntülemesidir; bu tür casus yazılım, kullanıcıların bilgisayarlarında yaptığı her şeyi yakalayabilirler. Sistem görüntülemeleri tüm tuş vuruşlarını, e-postaları, sohbet iletişim diyaloglarını, ziyaret edilen web sitelerini ve çalışan programları kaydetmektedir [26].

Yukarıda bahsi geçen saldırı tipleri bilgi güvenliği konusunda hem bireyler hem de kurumlar için gerekli önlemler alınmadığında kaçınılmaz hale gelmektedir. En basit gözüken saldırıların bile önüne geçmekte zorlanılan bilişim dünyasında bilgi güvenliği kapsamında alınan geleneksel önlemlerin yeterli olmadığı görülmektedir. Güvenlik açığından ve olası güvenlik saldırılarından korunmak için güvenlik duvarları kullanmak, düzenli olarak cihaz güncellemeleri yapmak gibi bilinen birtakım önlemler bilgi güvenliğini sağlamayı hedeflemektedir. Ancak sadece bahsi geçen teknik önlemleri almak güvenlik açığını ortadan kaldırmak için yeterli değildir; kullanıcıların olası güvenlik açıklarına ve saldırılarına karşı tutumlarını tespit etmek ve önlemek burada kritik bir rol oynamaktadır, çünkü bireyler hala bilgi güvenliği kapsamında en zayıf halka olarak görülmektedir. Tez kapsamında

tasarlanan model, bilgi güvenliğinin ve kişisel verilerin önemini vurgulayan, bahsedilen güvenlik açıklarının ve saldırı yöntemlerinin önüne geçmek için yeni teknikleri kullanan bir yöntemdir.

5. KULLANICI KİMLİK DOĞRULAMA

Hızla gelişen teknoloji ile insan hayatına giren bilgi teknolojileri sayesinde günlük ve fiziksel olarak yürütülen birçok eylem artık çevrimiçi ortamda yürütebilir hale gelmiştir. Sağlıktan iletişime, alışverişten finansa, hatta vatandaşlık işlemlerine kadar çevrimiçi ortamdaki sistemlerde hızlı bir şekilde kullanıcılar ihtiyaçlarını giderebilmektedir. Bu kolaylaştırılmış sistemler, doğal olarak hem kullanıcılar hem de servis sağlayıcılar için güvenlik kaygılarını da beraberinde getirmektedir. Birden çok kullanıcıya hizmet veren çevrimiçi sistemler, hem kullanıcılarını tanımlamak ve doğrulamak hem de bilgi güvenliğini sağlamak için farklı yollara başvurmaktadırlar. Temel olarak, kullanıcı kimlik doğrulama; tanımlama ve doğrulama adımlarından oluşmaktadır.

Tanımlama**,** genel olarak sistemler tarafından kullanıcıyı tanımlayacak eşsiz bir değeri ifade etmektedir. TCKN, e-posta, telefon numarası veya sistem kuralları tarafından onaylanmış özgün bir kullanıcı adı ve bu kullanıcı adı ile eşleşen sistemlerin kendi kuralları çerçevesinde belirlenen şifreler ile kullanıcılar sisteme kaydedilmektedir. Farklı kullanıcı gruplarının farklı yetkilere sahip olabildiği bu sistemlerde, bu şekilde yapılan sınıflandırmalar da kullanıcı tanımlama için oldukça önemlidir. Örneğin, yönetici yetkilerine sahip bir kullanıcı, sistem içerisinde birçok modülü görüntüleme ve değiştirme yetkisine sahip olabilirken, sıradan bir kullanıcı sadece kendi hesabı ile ilgili işlemleri yapabilme yetkisine sahiptir.

Doğrulama sistemler tarafından kayıt altına alınan kullanıcıların, sisteme erişmek istediklerinde daha önceden belirlenen kullanıcı adı ve şifre bilgileri ile doğrulanarak sisteme girmelerine izin verilmesini ya da girmelerinin engellenmesini ifade etmektedir.

Kullanıcı kimlik doğrulama bilgi sistemlerine erişimde, kullanıcıların veya diğer programların sisteme kendini tanıttığı işlemlerdir. Kullanıcı kimlik doğrulama, üç faktöre dayanır ve bu bağlamda üç sınıfa ayrılır [27].

Kullanıcı kimlik doğrulama faktörleri;

- Bilgi faktörü, “kullanıcının bildiği bir şey” (şifre, PIN, güvenlik soruları gibi)

- Nesne faktörü, “kullanıcının sahip olduğu bir şey” (kimlik kartı, özel kartlar, cep telefonu gibi)

- Biyometrik faktör, “kullanıcının olduğu veya yaptığı bir şey” (parmak izi, DNA dizisi, ses gibi) olarak sayılabilir.

Bunlarla ilişkili olarak kullanıcı kimlik doğrulama;

- Kullanıcıların sahip olduğu bilgileri kullanan (what you know); Bilgi Tabanlı,

- Kullanıcıların sahip olduğu nesneleri kullanan (what you have); Nesne Tabanlı,

- Kullanıcıların fiziksel ve davranışsal özelliklerini kullanan (what you are); Biyometrik Tabanlı olarak sınıflandırılabilir.

Kullanıcı kimlik doğrulama ayrıca, faktörlerin tek başlarına ya da birlikte kullanılmasına göre tiplere ayrılabilir.

5.1 Kullanıcı Kimlik Doğrulama Tipleri

Kullanıcıların kimlik doğrulamaları yapılırken, sistemlerin ve kullanıcıların güvenlik ihtiyaçlarına göre, faktörlerin tek başlarına veya birlikte kullanılması ile farklı seviyelerde güvenlik sağlanmaktadır. Açıklanan bilgi, nesne ve biyometrik faktörlerin kullanımlarına göre kimlik doğrulama tiplere ayrılabilir.

5.1.1 Tek faktör kimlik doğrulama

Kişinin kimliğini doğrulamak için belirtilen üç faktörden yalnızca birini kullanmasına tek faktör kimlik doğrulama (SFA) denir. Güvenlik seviyesi olarak oldukça zayıf kalacağı için kritik bilgilerin tutulduğu sistemlerde tercih edilmez.

Şifrelerin kötü niyetli ellere geçmesi halinde ikinci bir faktöre sahip olunmadığı için oldukça güvensizdir. Hassas verilerin saklanmadığı uygulamalar için tercih edilebilir.

5.1.2 İki faktör kimlik doğrulama

İki faktör kimlik doğrulama (2FA), açıklanan faktörlerden ikisinin kombine şekilde kullanılması ile sağlanır. Buna verilebilecek en iyi örneklerden biri bankacılık uygulamalarında tek seferlik OTP (One Time Password) şifrelerin kullanılmasıdır. Bankalar müşterilerini hali hazırda kullandıkları bir kullanıcı adı ve şifre ile sistemlerine alırken, ikinci bir faktör olarak, onların cep telefonlarına tek kullanımlık bir şifre gönderirler ve bu şifrenin sisteme girmeden iletilmesini isterler. OTP'ler aynı zamanda tek sefer kullanılabildiği için farklı saldırı çeşitlerine karşı da önlem alınmış olmaktadır. İki faktör doğrulama doğru kullanım ile oldukça güvenli olarak değerlendirilmektedir.

5.1.3 Çok faktör kimlik doğrulama

Çok faktör kimlik doğrulama (MFA) kullanıcı doğrulama için ikiden fazla faktörün bir arada kombine bir şekilde kullanılması ile sağlanır. MFA'nın işleyişi 2FA ile aynıdır. Örnek olarak, çok yüksek güvenlikli sistemlere girerken bir şifre, günlük olarak üretilen bir PIN ve aynı zamanda parmak izi, yüz tanıma gibi sistemlerin birbirine entegre bir şekilde kullanılması verilebilir. Oldukça güvenli bir doğrulama tipi olduğu kabul edilmektedir.

5.1.4 Güçlü kimlik doğrulama

Güçlü kimlik doğrulama, kimlik doğrulama yapılabilmesi için iki veya daha fazla yetkilendiriciye dayandırılmış katmanlı tiptir [28]. Kullanılan faktörler birbiriyle ilişkisiz olmalı ve tıpkı OTP gibi faktörlerden birinin yalnızca bir defa kullanılması gerekmektedir. Bu faktör aynı zamanda tekrar edilemez ve başkaları tarafından üretilemez olmalıdır.

5.1.5 Sürekli kimlik doğrulama

Geleneksel yöntemler, kişileri sadece sisteme girerken oturum açma sırasında tanımlar ve doğrular. Bu da aslında, oldukça önemli bir güvenlik açığını beraberinde getirmektedir, çünkü kullanıcı sisteme giriş yaptıktan sonra onun yerine başkası işlemlere devam edebilir ve bilgi güvenliği noktasında ciddi tehlike oluşturabilir. Bunun önlenmesi için davranışsal biyometrik yöntemler, kullanıcılar sistemin içerisindeyken kullanıcı hareketlerini izleyerek onları sürekli şekilde doğrular. Bu yöntemler sürekli ve aktif kimlik doğrulama olarak adlandırılmaktadır.

5.2 Kullanıcı Kimlik Doğrulama Sınıfları

Kullanıcı kimlik doğrulama Şekil 5.1'deki gibi üç ana başlık altında sınıflandırılır.

Şekil 5.1 : Kullanıcı kimlik doğrulama sınıfları.

5.2.1 Bilgi tabanlı kimlik doğrulama

Bilgi tabanlı kimlik doğrulama, dijital ortamlarda sisteme kayıtlı kullanıcıları doğrulamak için kullanıcının elinde bulunan bilgilerin kullanıldığı yöntemdir. Bu yöntemde kullanıcıların kolayca bilebileceği ancak kesinlikle kimseyle paylaşmayacağı bilgiler kullanılmaktadır. Bu bilgiler şifre, kullanıcı adı olabildiği gibi belirli güvenlik soruları da olabilir. Yönteme konu olan ve doğrulanan bilgiler oldukça gizli veya tercihe göre açık olabilir; bu tamamen sistemin ihtiyacına bağlı bir ayrımdır. İki çeşit Bilgi Tabanlı Kimlik Doğrulama metodu vardır: Statik Bilgi Tabanlı Kimlik Doğrulama ve Dinamik Bilgi Tabanlı Kimlik Doğrulama.

5.2.1.1 Statik bilgi tabanlı kimlik doğrulama

Sistemlere kayıt aşamasında kullanıcı tarafından sistemle paylaşılan bilgilerin doğrulama sırasında kullanılması yöntemidir. Kullanıcı, hesabına giriş yaparken veya hesaba girişteki asıl şifreyi unuttuğunu beyan ettiğinde birçok çevrimiçi sistem tarafından kullanıcıyı doğrulamak ve kimliğini ispatlamak için kullanılan bir yöntemdir.

Sisteme ilk erişimde kullanıcıdan alınan bu bilgiler, kullanıcı güvenliği gereği sadece doğrulamada kullanılması gerekmektedir. Bu bilgiler, örneğin bankaların sık sık kullandığı "Anne kızlık soyadı" bilgisi gibi gizli kalması gereken bilgiler olabildiği

gibi sistemin ihtiyacına göre içinde “En sevdiğiniz hayvan”, “İlk iş yeriniz” gibi bir soru demeti şeklinde de kullanıcıdan alınabilir.

Statik Bilgi Tabanlı Kimlik Doğrulama, hala çevrimiçi ortamda sıklıkla kullanılmaya devam etse de, bilgi güvenliği açısından zaafları çeşitli örneklerle ispatlanmıştır. Bunların önüne geçmek için bu yöntemi kullanan sistemlerin bilgileri nasıl sakladığı ve koruduğu konusunda oldukça titiz davranmaları gerekmektedir. Örnek olarak, 2008 yılında Alaska valisi Sarah Palin’in Yahoo hesabı, bir öğrenci tarafından ele geçirilmiştir. Öğrenci, valinin Yahoo hesabının şifresini sıfırlamak için sorulan güvenlik sorularının cevaplarını kısa bir internet araştırmasıyla bularak, hesaba kolayca erişim sağlamıştır [29].

Öte yandan, statik bilgi tabanlı kimlik doğrulama sistemleri, kullanıcıların kolayca hatırlayabileceği bilgileri kilit olarak kullansa da, Google’ın 2015 yılında yaptığı araştırma, kullanıcılardan en sevdiği yemek sorusuna verdiği cevabı bir ay sonra %74’ünün, üç ay sonra %53’ünün, bir yıl sonra ise sadece %47’sinin hatırlayabildiğini ve bilgisayar korsanlarının da %19.7 başarı oranıyla bu cevapları tahmin edebildiğini göstermektedir [30]. Statik yöntem kaba kuvvet saldırılarına da oldukça açıktır. Bu örnek ve çalışmalar statik bilgi tabanlı kimlik doğrulama yönteminin birçok açıdan bilgi güvenliği tehdidi içerdiğini göstermektedir.

5.2.1.2 Dinamik bilgi tabanlı kimlik doğrulama

Sistemlere kayıt aşamasında veya daha önceden alınmış bilgilerin değil, çeşitli kaynaklardan alınan verilerin ve veri madenciliği yöntemleri de kullanılarak oluşturulan bilgilerin kullanıldığı yöntemdir. Günümüzde birçok şirket, statik bilgi tabanlı kimlik doğrulama yöntemindeki açıklardan dolayı dinamik bilgi tabanlı kimlik doğrulama yöntemine geçiş yapmaktadır.

Bu yöntemde oluşturulacak sorular için verilere çeşitli yollarla erişilebilmek mümkündür. Veriler kullanıcılardan direkt olarak alınabildiği gibi, güvenilir kaynaklardan satın alınan veriler de olabilir. Burada dikkat edilmesi gereken, dolandırıcıların da ücretsiz ve kolay bir şekilde erişebildiği veri kaynaklarının kullanılmaması gerektiğidir. Veriler elde edildikten sonra en önemli nokta kullanıcıya doğru soruların sorulmasıdır. Çevrimiçi olarak kolayca ulaşılamayan, tahmin edilemeyen cevapları olan sorular bu yöntemde tercih edilir. Dinamik sistemde sorular ve cevaplar önceden belli değildir. Veri işleme yöntemleri

kullanılarak, “aylık kredi ödeme tutarı” gibi kişinin tipik kimlik bilgileri dışında kalan, yani kişi cüzdanını çaldırsa bile hırsızın o cüzdan içindeki kimlik bilgilerinden ulaşamayacağı, cüzdan dışı sorular da denen bir soru seti hazırlanır ve bu set kullanıcı verileri değiştiği için dinamik olarak yenilenir.

Statik yönteme göre daha güvenli olsa da gerçeklemesi daha maliyetli bir yöntemdir. Ayrıca, her insanın dijital ortamda dinamik soru oluşturacak kadar verisi bulunmadığı için daha kısıtlı bir kesime hitap etmektedir.

5.2.2 Nesne tabanlı kimlik doğrulama

Nesne tabanlı kimlik doğrulama yöntemleri, kullanıcıların sistem tarafından tanınması için onların fiziksel olarak yanlarında taşıyabildikleri araçlara ihtiyaç duyar. Akıllı kartlar bu yönteme örnek olarak verilebilir. Akıllı kartlar, kullanıcıyı doğrulayan bir şifre veya sertifikaya sahip olup bunları içinde barındırır. Girilmek istenen sistem bu kartlar içindeki bilgiyi kendi elinde bulunanla karşılaştırır ve kullanıcıyı doğrular. Bu bağlamda, sadece yazılım değil donanım gereksinimleri de vardır.

Çok faktörlü kimlik doğrulama yöntemlerinde kullanılmaktadır; kişiye özel nesneler birer donanım doğrulayıcı olarak kimlik doğrulamasına katkı sağlamaktadır. Bankaların müşterilerine sunduğu kartla para çekmeye yarayan ATM cihazları da bu mantıkla çalışır, müşteri önce kartını takar ardından şifresini girer ve kimliğini doğrulayarak işlemlerini gerçekleştirir.

Bu yöntemde bağımlı olunan fiziksel nesnenin başkası tarafından ele geçirilmesi bir risk teşkil etmektedir. Nesne Tabanlı Kimlik Doğrulama yöntemleri, kullanıcıların sürekli yanlarında bulundurmaları gereken araçlara ihtiyaç duyduğu için maliyetli ve daha az kullanışlı olarak değerlendirilmektedir.

5.2.3 Biyometrik tabanlı kimlik doğrulama

Biyometri, insanların eşsiz fiziksel ve davranışsal özelliklerinin ölçümü ile bunların istatistiksel analizlerini kullanarak kimlik doğrulama ve tanıma için kullanılan yöntemlerdir. Bunlar parmak izleri ve gözler gibi fizyolojik özellikleri veya bir güvenlik bulmacasını tamamlamak için kullanılan davranışsal özellikleri içermektedir. Bu verilerin benzersiz, kalıcı ve toplanabilir olması gerekmektedir. Biyometri, uzun yıllardır insanları ayırt etmek için kullanılan bir yöntemdir. Eski

zamanlarda suçluları parmak izinden tespit etmek için kullanılan bu yöntem günümüzde kimlik doğrulama prosedürlerine kadar birçok alanda güvenlik önlemi olarak da kullanılmaktadır.

Biyometrik özellik aşağıdaki dört ilkenin sağlanması olarak da tanımlanmaktadır [31].

- Evrensellik: her insanda olan bir özellik.
- Benzersizlik: her insanda farklı şekilde olan, kendine özgü bir özellik.
- Kalıcılık: Zamanla değişmeyen bir özellik.
- Elde edilebilirlik: Fiziksel cihazlarla nicel olarak ölçülebilir olan özellik.

Bunlarla birlikte pratik bir biyometrik sistemde ayrıca aşağıdakilere de dikkat edilmelidir.

- Performans: Kimliğin tanınması ve doğrulanması için hız ve süre değerleri
- Kabul edilebilirlik: Kullanıcıların bu yöntemleri kullanmayı kabul etmiş olmaları

Biyometrik sistemler doğrulama ve tanıma adımlarını içermektedir. Doğrulama adımında, sistem kullanıcıdan aldığı veriyi kendi elindeki veri ile karşılaştırır ve kullanıcıyı doğrular. Bu adımda, "Bu veri, A kullanıcısına mı ait?" sorusu sorulur. Tanıma adımında ise sistem kullanıcının bireysel verisini veri tabanındaki diğer verilerle karşılaştırır. Bu adımda "Bu veri kimin?" sorusu sorulur [32].

5.2.3.1 Fiziksel biyometrik tabanlı kimlik doğrulama

Fiziksel özellikli doğrulama, insanların sahip olduğu ve mümkün olduğunca özgün olan fiziksel özellikleri ile onları doğrulayacak bir cihazın birlikte çalışması ile sağlanır. Kullanıcıların, ayırt edici fiziksel özelliklerinin sensörler yardımıyla kimlik doğrulama için kullanılmasıdır.

Parmak izi tanıma

Parmak izinin kişiye özel olan yaşamış ve doğacak insanların hiçbirinde tekrarı olmayacak kadar özgün karakteristik bir özellik olduğu varsayılmaktadır. Parmaktaki deri girinti ve çıkıntılı yapısıyla vücudun diğer yerlerindeki deri yapısından farklılaşmıştır. Parmak üzerindeki küçük detaylar şekil ve konum olarak özelleşmiştir ve insan hayatı boyunca deformasyona uğramadıkça değişmez. İnsan

vücudunda bulunan bu karakteristik özellik kimlik doğrulamada kullanılmak için oldukça uygundur.

Parmak izi uzun yıllardır insanları fiziksel özelliklerine dayanarak ayırt etmede kullanılmaktadır [33]. Avrupalı kaşif Joao de Barros 14. Yüzyılda Çin'de mürekkep kullanarak ilk parmak izlerini kaydetmiştir. 1890'da Alphonse Bertillon, suçluların tespitine yardımcı olmak için parmak izinden kişi tespiti yapılan bir yöntem geliştirmiştir.

Başka bir deyişle, kendine ait bir algoritmaya sahip olan parmak izi en güvenli kimlik belirleme yöntemlerinden biridir. Suç tanımlama, erişim kontrolü, ATM kartı tanımlama gibi adli ve sivil birçok alanda kullanılmaktadır. Eski yöntemler düşük performanslı ve zor olduğundan, hızlı parmak izi okuyucular geliştirilmiştir [34].

Parmak izi tanıma sistemleri iki adımda çalışır: kullanıcıyı tanıma ve doğrulama. Tanıma adımında kullanıcı, parmak izi sensörüne parmaklarını tanıtır, sistem kullanıcıyı özgün bir kimlik bilgisi ile kaydeder ve parmak izini bu bilgi ile eşleyerek veri tabanında saklar. Böylece kullanıcının, kimliği ile eşleşen bir parmak izi değeri sistemde tutulur. Doğrulama adımında ise kullanıcı parmak izini sensöre okuttuğu anda parmak izi verisi veri tabanında tutulan değerlerle karşılaştırılır ve daha önce tanımlanmış eşik değerinin üzerinde bir eşleşme bulunursa kullanıcı doğrulanır [35].

Yüz tanıma

Görüntü analizi ve anlayışının en başarılı uygulamalarından biri olan yüz tanıma son yıllarda mobil cihazlara da bu yazılım ve donanımların entegre edilmesi ile birlikte oldukça popüler olmuştur. Yüz tanıma insan yüzünün karakteristik özelliklerini referans alarak analiz eder ve doğrulama için bu verileri kullanır. İnsanların yüzleri, tek yumurta ikizleri hariç birbirinden farklı olduğu için özgün bir veri olarak kabul edilmektedir.

Yüz tanımanın kimlik doğrulamada kullanılabilmesi için uzun yıllardır çalışmalar yapılmaktadır. 1964 ve 1965 yıllarında Bledsoe, Helen Chan ve Charles Bission ile beraber bilgisayarları insan yüzlerini tanımak için kullanmaya başlamıştır, bu yaklaşımda göz merkezleri, ağız gibi yüzdeki belirli bölgeler işaretlenmiş ve bu işaretler arasındaki mesafeler kimlik doğrulama için kullanılmaya çalışılmıştır. Bu çalışmada birçok fotoğraftan oluşturulan bir veri kümesinde verilen fotoğrafı içeren küçük bir kümenin çıkarılması amaçlanmıştır. Başın pozisyonu, aydınlatma,

yaşlanma gibi etkenler çalışmanın sürekliliğini etkilemiştir [36]. Bu temel üzerine yüz tanıma çalışmaları devam etmiştir. 1997 yılında Christoph von der Malsburg tarafından geliştirilen sistem endüstriyel olarak birçok yer tarafından da kullanılabilir hale gelmiştir. Bıyık, sakal, saç değişimleri ve güneş gözlükleriyle bile kimlik tespiti yapılabilir hale gelmiştir [37]. 2006'da yüz tanıma algoritmalarının performansı, Face Recognition Grand Challenge'da değerlendirilmiş ve 1995'teki verilerden 100 kat, 2002'deki verilerden 10 kat daha hızlı performansa sahip sistemlerin geliştirildiği görülmüştür [38].

Yüz tanıma teknolojileri bir kimlik doğrulama yöntemi olarak mobil cihazlara kameraların entegre şekilde üretilmesi sayesinde sıklıkla kullanılmaktadır. Kalabalık gruplar içinde kişi tespiti için spor müsabakalarında, suçlu tespitleri için güvenlik güçleri tarafından, kimlik doğrulama için gümrüklerde, akıllı ev sistemlerinde ve müşteri doğrulama için bankacılık uygulamalarında olmak üzere birçok alanda kullanılmaktadır.

Her insanın yüzünün kendine ait karakteristik özellikleri vardır, yüz tanıma programları yüzler üzerinde belirlediği noktalarla ayrıştırmayı yapar. Gözler arasındaki mesafe, burun genişliği, göz yuvalarının derinliği, elmacık kemiklerinin şekli, çene çizgisinin uzunluğu gibi özellikler başlıca ayırt edici olarak kullanılır. Kullanıcılardan alınan veriler görüntü işleme, makine öğrenmesi, derin öğrenme gibi bilgisayar bilimlerinin de yardımıyla işlenir ve anlamlandırılır.

Kameralar yardımıyla toplanan verilerin işlenmesine dayanan yüz tanıma yöntemleri farklı mimikler, yüzde oluşan değişimler, ışık, diğer nesneler gibi birçok dış faktörden etkilenmektedir. Yüz tanıma algoritmalarının kesinliğinin arttırılması için bilimsel çalışmalar devam etmektedir.

İris tanıma

İris göze rengini veren, gözün ön kısmındaki saydam tabakanın arkasında bulunan ve göze gelen ışık miktarını ayarlayan kas yapısıdır. İris gözde bulunan özgün bir yapı olması, diğer organlara göre deformasyona daha az uğrama riski olması sebebiyle kimlik doğrulamada tercih edilebilir. Genetik olarak özdeş bireylerin bile birbirinden farklı iris yapılarına sahip olduğu bilinmektedir.

Biyometrik kimlik doğrulamada iris tanıma kullanılabilmesi için bilgisayarlı görme, örüntü tanıma ve istatistik teknikleri kullanılır. İris tanıma için bu adımlar kullanılır:

segmentasyon; göz resminde iris bölgesinin bulunması, normalizasyon; iris görüntüsünün uygun boyutlara getirilmesi, özellik kodlaması; sadece irisin en ayırt edici özelliklerini içeren bir şablon oluşturulmasıdır [39].

Retina tanıma

Retina göz küresinin arka duvarını kaplayan ve görme hücrelerinden oluşan bir ağ tabakasıdır. Retina, biyometrik kimlik doğrulamada gözün arkasında bulunan kan damarını analiz ederek kullanılır. Optik bir kuplör aracılığıyla düşük yoğunluklu bir ışık kaynağı kullanılarak retina taranır. Veri toplanırken kullanıcının belirli bir noktaya bir süre bakması istenmektedir. Gözlük veya lens kullanımı retina tanıma teknolojilerinin doğruluğunu etkilemektedir. Bu nedenlerle, kullanıcılar tarafından çok tercih edilen bir yöntem değildir [40].

El geometrisi tanıma

El geometrisi adından da anlaşılacağı gibi elin geometrik yapısını ifade etmektedir. Çeşitli konumlardaki parmakların genişliği, avuç içi genişliği, avuç içi kalınlığı, parmakların uzunluğu gibi özellikleri içermektedir. Bu değerler toplum içinde ciddi farklara sahip olmasa da kimlik doğrulama için kullanılabilmektedir [41].

El geometrisi tanıma yönteminde el görüntüsü alındıktan sonra görüntü hizalanır. Ardından el geometrisi görüntülerinin çıkarımı yapılır. Bu görüntüler ilgili bölümlere ayrılarak incelenir. İncelenen görüntülerin, el özelliklerine dayanarak özellik çıkarımı yapılır. Çıkarımlar sonrası eldeki verilerle doğrulama ve tanıma yapılabilmektedir [42].

El geometrisi tanıma teknolojileri, parmak izindeki direkt temaslı veya retina tanımadaki aydınlatma koşulları gibi çevresel koşullardan daha az etkilendiği için daha kolay ve ucuz bir yöntemdir. Ancak, el verileri benzersiz denemez, deformasyona açıktır. Bu nedenlerle, tam güvenli bir kimlik doğrulama aracı olarak kabul edilmemektedir.

Avuç içi tanıma

Avuç içi de tıpkı parmak izi gibi girinti ve çıkıntılardan oluşmaktadır. Avuç içinin alanı parmak ucu alanından büyük olduğu için avuç içindeki vadiler daha belirgindir. Bu sebeple de avuç içi okuyucuların daha geniş bir alanı tanıması beklenmektedir. Avuç içi tarayıcıları el içindeki girinti, çıkıntı ve kırışıklıkları işleyerek tanıma ve doğrulama yapmaktadır [43].

DNA tanıma

DNA, tüm canlıların yaşamsal işlevleri ve gelişmeleri için gerekli olan genetik kodu taşıyan bir nükleik asittir. Bireyin bireyselliği için sahip olduğu benzersiz koddur. DNA tek yumurta ikizleri hariç her insan için farklı bir koddur. Ancak, üç konu DNA biyometrisinin kimlik doğrulama uygulamalarında kullanılmasını kısıtlamaktadır.

- Hassasiyet ve kirletme: Daha sonra kötüye kullanılabilir olması,
- Gerçek zamanlı tanıma sorunları: DNA sonuçlarının anlık olarak alınmasının zor olması,
- Mahremiyet sorunları: Kişinin belirli bir hastalığa karşı olan zaafının DNA üzerinden elde edilebilir olması [31].

DNA her ne kadar en kesin kimlik doğrulama yöntemi olsa da hızlı sonuç alınamaması ve maliyetli işlemler gerektirmesi sebebiyle tercih edilmemektedir. Ancak, laboratuvar ortamında kanıtlardan suçluların eşleştirilmesi ve akrabalık testi gibi alanlarda kullanılmaktadır.

5.2.3.2 Davranışsal biyometrik tabanlı kimlik doğrulama

Fiziksel özelliklere kıyasla davranışsal doğrulamada ek bir donanıma ihtiyaç duymadan kişinin hali hazırda sahip olduğu özellikler kullanılarak doğrulama yapılabilmektedir. Bu özelliği ile davranışsal biyometri sürekli doğrulamada kullanılmak için oldukça uygundur. Kullanıcı sistemde çevrimiçiyken zaten yaptığı hareketler izlenerek sürekli doğrulama yapılabilir. Davranışsal biyometrik özellikler, fiziksel özelliklere göre zamanla daha değişken ve daha az ayırt edici olduğundan, ikinci faktör sistemlerde kullanılmaya daha uygundur.

Davranışsal biyometri için veriler toplandıktan sonra dikkat edilmesi gereken, tanımlama aşamasında kullanıcıyı yeterince ayırt edici özelliklerini kullanarak tanımlama ve seçilen özelliklerin kullanıcıyı net bir şekilde tanımlayabiliyor olmasıdır. Doğrulama yaparken de istatistiksel yöntemler, makine öğrenmesi veya derin öğrenme gibi teknikler kullanılarak doğruluk payı arttırılabilir.

İnsanlar günlük eylemlerinde benzersiz bilgi ve becerilerini uygulayarak kişisel birer imza niteliğinde farklı tarzlar ve yöntemler kullanır. Davranış biyometrisi tanımlanırken zaman boyutu da oluşturulan bu imzanın bir parçası olarak dahil

edilmelidir. Davranışsal biyometri kullanıcının davranışlarını analiz eder, profil oluşturur ve doğrulamaya çalışır.

Davranışsal biyometri beş temel başlığa ayrılmaktadır. Birinci kategori, bir metni veya bir insan tarafından üretilen bir çizimi incelemeye dayanan yazar tabanlı biyotmetriler; burada yazarın noktalama işaretleri yada fırça darbeleri gibi kendine özgü stil özellikleri gözlemlenir. İkinci kategori, insan bilgisayar etkileşimine dayanan biyometriden oluşur. Araştırmacılar, insanların bilgisayarlarla olan etkileşimlerini izleyip, kullanıcıların kendine has özelliklerini takip ederek doğrulama yapmaya çalışır. İnsan bilgisayar etkileşime dayanan biyometri klavyeler, bilgisayar fareleri ve insanların bunları kullanımı sırasındaki hareketlerinin gözlenmesi ve farklı yazılımlarla etkileşim esnasında kullanıcının ortaya koyduğu yöntem veya stillerin ölçülerek gözlenmesi olan iki alt kategoriye ayrılabilir. Üçüncü kategori, ikinci kategoriye oldukça paralel olan düşük seviyeli gözlemlenebilir, bilgisayar yazılımı eylemleriyle toplanabilecek insan bilgisayar etkileşimi tabanlı biyometri setidir. Burada toplanan veriler kullanıcı tarafından farkında olmadan istemsizce üretilmektedir; sistem aramalarından, denetim kayıtlarından verileri birbiriyle ilişkilendirerek ortaya bir ilişki koymaya çalışır. Dördüncü kategori, insanın kaslarını kullanma yeteneği yani motor becerilerine dayanır. İnsanın kas hareketleri beynin, iskeletin, eklemlerin ve sinir sisteminin düzgün işleyişi ile kişinin kimlik doğrulamasını olağan kılar. Motor becerilerin büyük bir çoğunluğu, genetik olarak gelmez, öğrenilir ve geliştirilir. Bu beceriler izlenerek, kullanıcılar arasında ayırt edici birer özellik olarak kullanılmaya çalışılır. Beşinci kategori ise, bir insanın nasıl yürüdüğü, vücudundaki kas hareketlerini nasıl yaptığı, bir nesneyi nasıl tutuğu gibi davranışlarını takip eder, bunları analiz ederek kimlik doğrulamasını bir olasılık haline getirir [44].

Ses ve konuşma

Ses aslında hem fiziksel hem de davranışsal biyometri olarak tanımlanabilmektedir. Bir kişinin sesinin özellikleri; ses yolu, burun ve ağız boşlukları ve dudaklar gibi sesin oluşmasında kullanılan bileşenleri temel alır. Bu sayılan fiziksel özellikler insan doğası için aynıdır. Ancak, kişinin davranışsal olarak nitelendirilen konuşması yaş, sağlık durumu, duygu hali gibi faktörlerle değişir ve ayırt edici olur; ama yine de büyük ölçekte kullanım için uygun olmayabilir. Metne dayalı sistemler, önceden tanımlanmış bir metne bağlı şekilde ses tanıması yapar. Metne bağlı olmayan

sistemler, dinamik olarak ses tanıması yaptığı için daha ayırt edici sayılmaktadır. Ses tanıma sistemleri ortam gürültüsü, sesteki değişimler gibi çevresel faktörlerden etkilenmektedir [31].

Göz hareketleri

İnsanların göz hareketlerinden ve bakışından, davranışsal kimlik doğrulama yapılmasıdır. Fiziksel olarak iris ve retina tanımasından farklı olarak burada, göz hareketleri ayırt edici özellik olarak kullanılmaktadır. Kişinin göz hareketleri takip edilirken, yüz ifadeleri de kayıt altına alınır ve göz yörüngelerinin hareketleri iki boyutlu bir düzlemde, dikkat noktaları ile beraber değerlendirilir. Tüm veriler beraber analiz edildiğinde ise, göz hareketlerinden kişilerin belli oranlarda ayırt edilebileceği ile ilgili sonuçlar alınabilmektedir [45].

İmza

İmza uzun yıllardır yasal ve ticari işlemlerde bir doğrulama aracı olarak varlığını sürdürmektedir. İmzalar zamanla değişebilen ve sahibinin fiziksel ve duygusal durumundan etkilenen verilerdir.

İmza tanıma, statik ve dinamik olarak iki şekilde yapılabilir. Statik yöntemde, kullanıcılar bir kağıda imza atar ve bu kağıt optik olarak tarandıktan sonra dijitalleştirilir, dijitalleşen bu veri analiz edilerek çevrim dışı olarak kimlik doğrulama yapılır.

Dinamik yöntemde ise kullanıcılar gerçek zamanlı olarak bir tablete imza atar, çevrimiçi olarak bu imzalar analiz edilerek kimlik doğrulama yapılabilir. Bu dinamik veri seti kullanılarak; hızlanma, hız, anlık yörünge açısı, anlık yer değiştirme, merkezcil hızlanma gibi faktörlerin birer parametre olarak değerlendirilmesiyle sonucun kesinliği arttırılır [46].

İmzayı atan el çeşitli fiziksel ve genetik faktörlerden etkilenebilir, hızlı ve dinamik bir operasyon olan imza atma, zaman içinde değişime uğramaya açıktır. Bu nedenle doğrulamada kullanılmasında dezavantajlar olduğu düşünülmektedir.

El yazısı

El yazısından tanıma verilen bir metnin yazarını el yazısından bulmaya yarayan yöntemdir. Bu yöntemde karakterler ve şekillerin geometrisi, açıları ve koordinatları incelenir ve analiz edilir. İmza tanıma gibi statik ve dinamik olmak üzere iki

kategoride incelenebilir. Kullanıcı bir kağıda ya da tablete yazı yazar; bu yazılar statik ve dinamik olarak analiz edilerek kişi tespiti yapılabilir.

Yürüyüş

Yürüyüş biyometrik olarak kişinin yürüdüğü uzay-zamansal yol olarak tanımlanabilir. Yürüyüş biyometrik kimlik doğrulama yöntemi olarak çok ayırt edici sayılmasa da, bazı düşük güvenlikli sistemler tarafından kullanılmaktadır. Yürüme davranışsal bir biyometridir; vücut ağırlığındaki dalgalanmalar, eklemler ve beyindeki yaralanmalar nedeniyle uzun süre aynı kalamaz. Yürüyüş tanıma sistemleri tıpkı yüz tanıma sistemlerindeki gibi kullanıcıdan veriyi kayıt yaparak alır. Ardından, kimlik doğrulama için videodan eklemlerin konumu ve hareketlerini ölçer ve işler. Girdi ve hesaplama açısından maliyetli bir yöntem olduğu düşünülmektedir [31].

Dudak hareketleri

Dudak hareketleri de davranışsal biyometride kullanılmaktadır. Yüz tanımada olduğu gibi bu yöntemde de bilgisayarlı görme, görüntü işleme ve istatistik kullanılır.

Görüntüler üzerinde önce yüzün, ardından ağızın ve son olarak dudakların yeri belirlenir. Dudakların hareketleri saptanır ve kişiye özgü özellikler çıkarılarak doğrulama yapılmaya çalışılmaktadır [47].

Davranış dinamikleri

İnternetin hayatımıza girmesi ile beraber sosyal medya kullanımı da büyük bir hızla artmıştır. Bu yöntemde insanların sosyal ağ hareketlerini kullanarak kişi tanımlamanın uygulanabilirliği incelenmektedir. Bu yöntemin incelemesinde sosyal medyadaki profil bilgileri ile bu ağlardaki etkileşimler girdi olarak kullanılabilmektedir [48].

Fare etkileşimi dinamiği

Bilgisayarlarla birlikte fareler birer işaretleme aygıtı olarak yaygın biçimde kullanılır hale gelmiştir. Bir davranışsal biyometri olarak fare etkileşimi dinamiği, kullanıcıları fare kullanım şekillerinden doğrulamayı amaçlamaktadır. Kullanıcının benzersiz fare kullanım hareketleri bir dizi fare işlem seti, mesafe ölçümü, tıklamalar gibi çıkarılan davranışsal özellikler yardımıyla meşru bir kullanıcının profiliyle karşılaştırılarak doğrulama yapılmaya çalışılır. Sürekli aktif bilgisayar kullanımı devam ettiği için

sadece doğrulama da değil, sürekli bir şekilde kimlik doğrulamaya da olanak sağlamaktadır [49].

Tuşlama dinamiği

Tuşlama dinamiği, insanları klavyede yazma stil ve ritimlerinden tanıma ve kimlik doğrulama yapma yöntemidir. Tarihsel olarak telgraftan başlayarak daktilo ve ardından bilgisayarlarda kullandığımız klavye donanımı ile insanlar tuşlama yaparak iletişim kurmaktadırlar. Sürekli kullanımda olan klavyeler sayesinde, kişilerin kimliğinin sürekli doğrulaması da yapılabilmektedir.

Tuşa basma süresi, tuşu bırakma süresi, bir tuşu bırakıp diğerine basma arasında geçen süre, yazım yanlışları gibi değerler parametre olarak kabul edilerek analiz edilir. Kullanıcıların klavyede yazma stilleri ve ritimleri kullanılarak onlara ait profil desenleri oluşturulur.

Tuşlama dinamiği bir davranışsal biyometridir. Statik olarak sadece sistem girişlerinde ve dinamik olarak sürekli hareketlerin izlenmesi şeklinde kullanılabilir. Kullanıcı hareketlerinden toplanan veriler yapay sinir ağları, istatistik gibi teknikler kullanılarak anlamlandırılır.

Dokunma dinamiği

Teknolojinin hızlı gelişmesi ve evrimleşmesi ile beraber taşınabilir bilgisayarlar hayatımızın vazgeçilmez birer parçası haline gelmiştir. Daha küçük, ergonomik ve kullanışlı üretilen mobil cihazlar çoğunlukla dokunmatik ekranlara sahiptir. Dokunma dinamikleri de kişilerin dokunmatik ekranlı cihazlarla etkileşimi yardımıyla kimlik doğrulama yaparak güvenlik sağlamayı amaçlamaktadır.

Dokunma dinamikleri, insandan insana değişen benzersiz özellikler olarak kabul edilmektedir ve davranışsal biyometrik veriler olarak kullanılmaktadırlar. Dokunma dinamikleri başlıca aşağıdaki özelliklere sahiptir.

- Kişiden kişiye değiştiği için ayırt edicidir.
- Hali hazırda kullanılan farklı güvenlik sistemlerine entegre edilebilirler ve gelişmiş güvenlik sağlarlar.
- Dokunma dinamiklerinin ölçülmesi özellikle fiziksel biyometrik veriler gibi maliyetli değildir. Mobil cihazların çoğunda gelen sensörler yardımıyla oldukça maliyetsiz bir şekilde elde edilebilirler.

- Yine bu sensörler yardımıyla birçok diğer sistem gibi sadece ilk girişteki doğrulamada değil, sürekli olarak izlenip loglanabildikleri için sürekli kimlik doğrulamada kullanılmaya oldukça uygundur. Kullanıcı davranış verilerini sisteme girmek zorunda değildir, sistemler arka planda kullanıcının haberi olmadan dokunma davranışları ile kullanıcıların bu verilerini alabilir ve sürekli olarak maliyetsiz bir şekilde doğrulama yapabilir.
- Göz, parmak izi tanıma gibi sistemler ek cihazlara ihtiyaç duyar ve çevresel koşullardan örneğin ortam aydınlığından etkilenirler. Ancak, dokunma verilerinin çevresel koşullara karşı bağımlılığı daha azdır.
- Dokunma dinamikleri, kullanıcılara yeni bir cihaz kullanmasını ve buna alışmasını zorunlu kılmaz, hali hazırda kullanıcıların sürekli olarak kullanmaya alışkın oldukları cihazlar yardımıyla kimlik doğrulama görevini yapar.

  Bu avantajlarının yanında dokunma dinamikleri ile ilgili uygulamalar geliştirilirken mobil uygulamalar içine ekstra bir görev getirdiğinden performans sorunu yaratmayacak tasarımlar yapılmalıdır. Dokunma dinamikleri de diğer davranışsal veriler gibi fiziksel biyometrik verileri kullanan yöntemlere göre daha düşük doğruluğa sahiptir. Bu nedenle uygulamalar geliştirilirken mümkün olan en yüksek doğruluk değeri elde edilmeye çalışılmalıdır. Dokunma dinamiği uygulamaları, kullanıcıların değişen davranışlarından etkilenirler ve yeniden adaptasyon sağlamaları sırasında doğruluk değerleri düşer. Bu nedenle de geliştirilen uygulamaların kullanıcılarda oluşabilecek bu değişimleri hızlıca öğrenmesi ve adapte olması gerekmektedir.

  Tuşlama dinamiği ve dokunma dinamiği kavramları birbirinden keskin çizgilerle ayrılamamaktadır. Evrimsel ve yöntemsel olarak birbirinin üzerine koyan yöntemlerdir. Tez çalışması kapsamında geliştirilen uygulama, dokunma dinamiği tekniklerini kullandığı için bu iki yöntem kullanılarak yapılan çalışmalar detaylı bir şekilde incelenmiştir.

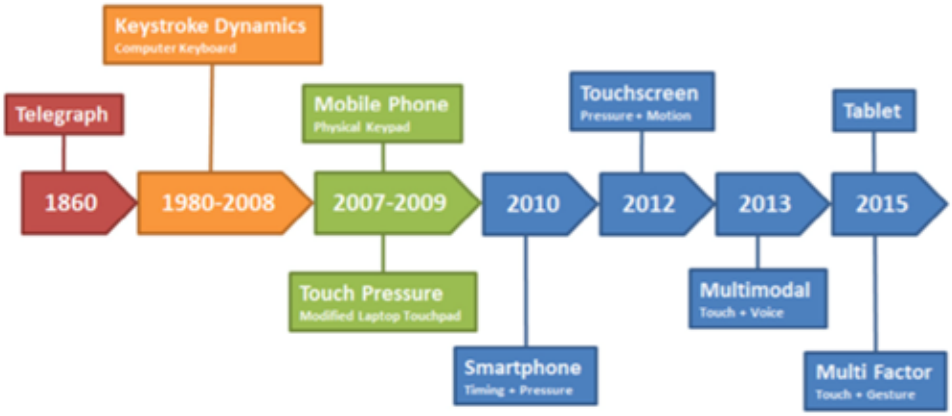
6. LİTERATÜR ARAŞTIRMASI VE BENZER ÇALIŞMALAR

Geçtiğimiz yüzyıl boyunca yapılan deneyler yürüme, yazma, konuşma gibi aktivitelerin bir dizi eylem tarafından yönetildiğini ve bu eylemlerin modellenerek tahmin edilebileceğini göstermiştir. Motor sistemler bu modellere göre hareketi planlar ve kontrol eder. Bilgisayarların hayatımızda hızla artan yeri beraberinde davranışsal biyometri doğrulama yöntemlerinden tuşlama dinamiği ve dokunma dinamiğini getirmiştir. Farklı çalışma alanları olsa da tuşlama ve dokunma dinamiği tarihsel olarak Şekil 6.1'de gösterildiği gibi birbiriyle bağlantılıdır. Bu nedenle, bu bölümde sırasıyla tuşlama dinamiği ve dokunma dinamiği üzerine yapılan çalışmalarla ilgili araştırmalar anlatılmıştır.

Tuşlama dinamiği olarak adlandırdığımız yöntem tarih olarak aslında 19. yüzyıla kadar dayanır, bu dönemde telgrafların yoğun olarak kullanılması ile birlikte telgraf operatörlerinin yazım ritminden diğer operatörleri ayırt edebildikleri görülmüştür. 2. Dünya savaşı sırasında ise, "Gönderenin Yumruğu (Fist of the Sender)" ismi verilen bir metot ile telgraf anahtarlarının ritmini, hızını ve senkronizasyonunu kullanarak telgraf göndericisinin kimliği belirlenmeye çalışılmıştır. Operatörler takip edilerek askeri birliklerin hareketi bu yolla izlenebilir olmuştur [50]. 1980'lerde ise Amerika Birleşik Devletleri'ne bağlı Ulusal Bilim Vakfı ve Ulusal Standartlar Bürosu yazma modelleri kullanılarak ayırt edici ve benzersiz modeller üretilebileceği üzerine çalışmalar yürütmüşlerdir [51].

20. yüzyılda farklı becerilere sahip 37 telgraf operatörü ile deneyler yapılmış ve deneyler sonunda operatörlerin birbirlerini yazım şekillerinden tanıyabildikleri görülmüştür. Daktilo ile yazım sırasında davranışlardan bir modelleme yapılmıştır. Yazan kişi tarafından karakterlerin tanınması ve algılanması bir adım olarak kabul edilmiştir. İkinci aşamada, algılanan kelimeler el ile yazılmaya başlamadan kısa bir süre hafızada tutulmaktadır. Üçüncü aşamada ise, ayrı karakterler komutlara çevrilir ve parmaklar kas hareketleri yardımıyla tuşlara basar. Bu adımda acemi ve uzman kullanıcılar arasında tuşlara basma süreleri arasında farklar tespit edilmiştir.

Dördüncü aşama ise, metnin geri bildirim ile doğrulanması adımıdır. Tuş vuruşu yapıldıktan sonra görsel ve işitsel olarak geri bildirim ile kontrol sağlanır [53].



Şekil 6.1 : Dokunma dinamiği tarihi gelişimi [52].

6.1 Tuşlama Dinamiği

Banerjee ve Woodard tuşlama dinamiğinin davranışsal biyometrideki performansını incelemiştir. Yazılarında önceki çalışmalardan, davranışsal biyometrinin psikoloji ile ilişkisi ve yöntemlerden bahsetmişlerdir. Ölçüm parametreleri olarak tuşa basma ve tuşu bırakma arasında geçen süreler kullanılmıştır [54].

Venko ve Kumar'ın kaleme aldığı çalışmada, güvenlikte temel sorunların çözümü için tuşlama dinamiğinde bekleme süresi, uçuş süresi gibi özellikler Hausdorff zamanlaması, ortalama, medyan ve standart sapma gibi işleme teknikleriyle analiz edilmiştir. Yapılan çalışmalarda Yapay Sinir Ağları da kullanılmıştır. PP (Press - Press) ve RR (Release - Release) değerleri ayırt edici olarak seçilmiştir. Her bir kullanıcı için bir eşik değerinin belirlendiği tuş dinamiği değerleri, kurulan sistemde kullanıcılar eğitildikten sonra belirlenmektedir. Deneyler sırasında hem geçerli hem de geçersiz kullanıcılara yer verilmiş, geçersiz kullanıcılara geçerli şifreler söylenmiştir. Hata değeri 0.001'den düşük ise kullanıcı geçerli sayılmıştır. Deneyler sonucunda, FAR %4.99 elde edilmiştir [55].

Chandrasekar, Kumar ve Maheswari çalışmalarında, Hausdroff zamanlama değerleri, ortalama, standart sapma ve gecikme, digraf ve bunların kombinasyonlarının medyanı ölçülmüş ve performansları karşılaştırılmıştır. PP, RR ve RP (Release - Press) ayırt edici özellik olarak seçilmiştir. Öznitelik çıkarımı için Stokastik

Difüzyon Arama ve Yerçekimi Arama Optimizasyonu kullanılmıştır. Doğrulama işlemlerinde Yapay Sinir Ağları kullanılmıştır [56].

Kim ve Kang, tuşlama dinamiğinin giriş tabanlı sistemlerde ve sürekli kimlik doğrulama operasyonlarında kullanılabileceğine değinen çalışmalarında, serbest metinler yazdırılan kullanıcıların yazma hızlarının arasındaki farkı ayırt edici özellik olarak seçmiştir. 150 katılımcıdan İngilizce ve Korece kişi başı 13000'den fazla tuş vuruşu ile toplanan verilerle, EER 0.44 elde edilmiştir [57].

Gaines, Lisowski, Press ve Shapirp çalışmalarında daktilo üzerinde ardışık tuş vuruşları arasındaki zamanların kaydedildiği deneyler yapmıştır. Deney, ilk deneyden 4 ay sonra aynı paragrafların yazdırılması ile tekrarlanmış ve kimlik doğrulama yapılması amaçlanmıştır [58].

Deutschmann, Nordström ve Nilsson davranışsal biyometrik verilerin sürekli kimlik doğrulamada kullanılabilirliği üzerine araştırmalar yapmıştır. Davranışsal biyometri olarak yalnızca tuş dinamiği değil aynı zamanda fare etkileşim dinamiğini de kullanmışlardır. Toplam 10 hafta boyunca 99 kullanıcı tarafından test edilen sistemlerinde kullanıcılar ortalama 103 tuşlama, 6606 fare dinamiği ile eğitilmişlerdir. Çalışma ile birlikte az sayıda kişiden oluşan gruplar üzerinde de olsa tuşlama dinamiklerinin sürekli kimlik doğrulamada kullanılabileceği görülmüştür [59].

Prabha ve Vidhyapriya davranışsal biyometrik verilerin saldırılara karşı alınan önlemlerde daha az maliyetli olduğuna dikkat çeken çalışmalarında, tuşlama dinamiğinin yanı sıra hızla hayatımıza giren mobil cihazları ve onların dokunmatik ekranlarını da değerlendirmeye almıştır. Mobil cihazların dokunmatik ekranları kullanılarak 4 haneli şifrelerin numerik klavye yardımıyla girdirilmesi ile testler yapılmış ve anomaliler tespit edilmeye çalışılmıştır. 23-42 yaş aralığında 50 kullanıcı üzerinde yapılan deneylerde, kullanıcının tuşa basarken bekleme süresi, RP, parmak eğimi, basınç ve parmak tabletten ayrılırken oluşan eğim değerleri parametre olarak kabul edilmiştir. Çalışma sonunda, EER 0.26667 elde edilmiştir [60].

6.2 Dokunma Dinamiği

Peng ve diğerleri çalışmalarında, giyilebilir gözlüklerin büyük popülerlik kazanacağının; ancak buradaki verilerin gizliliğinin bir risk olduğu üzerinde

durmuştur. Sürekli kimlik doğrulama yapılabilmesi için tek dokunuş, ileri kaydırma, geri kaydırma, iki parmak ile ileri kaydırma, iki parmak ile geri kaydırma ve ses ayırt edici özellikler olarak değerlendirilmiştir. 32 kullanıcı üzerinde yapılan testlerde dokunmatik değerler ve ses beraber ele alındığında sürekli doğrulama için başarılı sonuçlar elde edilmiştir [61].

Bevan ve Fraser yaptıkları çalışmada, insanın fiziksel özellikleri ve mobil cihazlar üzerindeki dokunmatik hareketleri beraber olarak değerlendirmiştir. Antropometri, insan vücudundaki uzuvların boyutları ile ilgili ve aralarındaki orandan bahseder. Bu çalışmada da insanın baş parmağının uzunluğu ile dokunmatik ekranlardaki kaydırma hareketi arasındaki ilişki incelenmiştir. 178 denek ile yaklaşık 19000 kaydırma hareketi incelenmiş ve deney sonucunda uzun kişilerin daha hızlı ve ivmeli kaydırma süreleri elde ettiği görülmüştür. Bu çalışmayla kadın ve erkekler arasında ekrana dokunma basıncı arasındaki farklar da incelenmiştir [62].

Antal ve Szabo çalışmalarında, kullanıcılara psikolojik bir anket yapmış ve cevapları ekranda bulunan bir kaydırma nesnesi aracılığıyla toplamıştır. Kullanıcıların cevap verirken yaptıkları yatay kaydırma hareketi ile veriler toplanmış ve bunların ayırt edici özellikleri üzerine çalışılmıştır [63].

Antal, Bokor ve Szabo diğer çalışmalarında, kullanıcıların dokunmatik ekranlar üzerindeki yatay ve dikey kaydırma hareketlerini izleyerek kimlik doğrulama ve cinsiyet tespiti yapmayı amaçlamıştır. 71 kullanıcı 8 farklı mobil telefon ve tablette bir veri seti ile test edilmiştir [64].

Zhou ve diğerleri, dokunmatik cihazların yaygınlaşması ile beraber hem giriş hem de sürekli doğrulamada dokunmatik verilerin kullanılabileceğini savunan çalışmalarında, hem tuşlama dinamiğini hem dokunma dinamiğini birlikte analiz etmiştir. Deneyler sonucunda sadece tuşlama dinamiğine göre üretilen hibrit çözüm daha başarılı değerler elde etmiştir [65].

Buriro, Crispo ve Conti yaptıkları çalışmada, akıllı telefon kullanıcılarının telefon kilidini açma, ekran kilidini açma ve telefonu kulağına götürme şekillerini davranışsal biyometri niteliği olarak ele alıp değerlendirmiştir. 85 kullanıcıdan toplanan yaklaşık 10200 davranış verisi kullanıcıların yürüyüş, oturma, ayakta durma gibi aktivitelerine göre gruplanarak değerlendirilmiştir [66].

Kambourakis ve diğerleri çalışmalarında, tuşlama dinamiklerinin mobil cihazlar üzerinde kimlik doğrulamadaki etkilerini araştırmak için örnek uygulama geliştirmiştir. Tuşlama dinamiğindeki parametrelere ek olarak hız ve mesafeyi de eklemiş, verilen bir metnin yazılması ve şifre girişi metotları ile denemişlerdir [67].

Rajalakshmi ve diğerleri yaptıkları çalışmada, dokunma dinamiklerini kullanarak hem güvenlik hem de performans değerlerini analiz etmişlerdir. Kullanıcının kaydırma hareketleri izlenmiş; basınç, cihazın ekran yönü ve koordinatları toplanmış, bunlar yapay sinir ağları kullanılarak sınıflandırılmış ve %82 doğruluk elde edilmiştir [68].

Zheng ve diğerleri yaptıkları çalışmada, insanların dokunmatik ekranlarda kendilerine özgü davranışlar sergilediklerini göstermek için hızlanma, basınç, boyut ve zaman değerlerini birleştirerek 4 haneli ve 8 haneli nümerik şifreler ile 80'den fazla kullanıcı üzerinde yaptıkları deney verilerinde %3.65'e varan EER elde etmişlerdir [69].

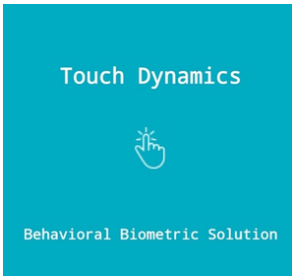
7. GELİŞTİRİLEN MODEL VE UYGULAMA

Bilgisayarların hayatımızın vazgeçilmez birer parçası haline gelmesi ile daha küçük ve ergonomik bilgisayara duyulan ihtiyaç sonucu, hızla gelişen akıllı telefonlar özellikle Android ve IOS işletim sistemlerinin sağladığı altyapı ile birlikte kullanıcıların hemen hemen tüm çevrimiçi hizmetlere anında erişebilmesini ve dijital kimliklerin ceplerde taşınan bir hal almasını sağlamıştır.

Kullanıcıların akıllı telefonları kullanırken dokunmatik ekranlarla girdikleri etkileşim davranışsal biyometrik verilere dahil edilmektedir. Her kullanıcının ekrana dokunma davranışı, dokunma kuvvetinin hızı, ritmi, basıncı, parmağın açısı gibi davranışsal tercihlerden benzersiz birer davranış profili oluşturulabilmektedir.

Bu çalışma kapsamında, kullanıcılardan oluşturulan numerik klavye yardımıyla dokunma dinamiği verileri toplanmaktadır. Geleneksel sistemlerde önceden belirlenmiş bir PIN, numerik klavyeler yardımıyla doğru olarak girildiğinde kullanıcılar sistemlere dahil edilmektedir. Ancak, bu PIN değerleri gerek sosyal mühendislik gerekse farklı saldırılarla ele geçirilebilen şifreler olduğu için, sadece bu değerlerin doğru girilmesi kullanıcı kimlik doğrulama için yeterli olmamaktadır. Tam bu noktada, dokunma dinamikleri güvenlik seviyesini arttırmak için kullanılabilir olmaktadır.

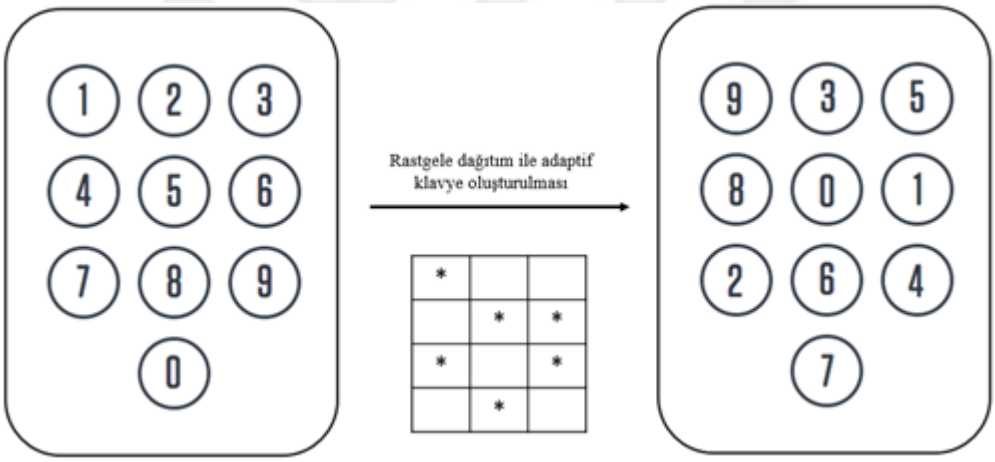
Çalışma kapsamında, kullanıcılardan dokunma dinamiği verilerinin toplanıp işlenebileceği bir ara yüz sağlamak adına, Şekil 7.1'de gösterilen "Touch Dynamics" isimli bir Android mobil uygulama geliştirilmiştir.



Şekil 7.1 : Touch Dynamics uygulaması logo.

Dokunma dinamikleri üzerine daha önceki örnek çalışmalar incelendiğinde, hem alfa numerik hem de numerik klavyelerin kullanıldığı görülmektedir. Bu çalışmada numerik klavye kullanımı tercih edilmiştir.

Gerek donanımsal klavyelerde gerekse dokunmatik ekranlarda yazarken tuşların düzeni insan zihninde birer desen gibi düşünülebilir. Mobil cihazlarda numerik klavye denildiğinde birçok insan aklına 0'dan 9'a kadar rakamlardan, 0'ın en altta olduğu ve 3'e 4'lük bir matristen oluşan tasarım gelmektedir. Bu zaman içinde farkında olmadan örtük öğrenilen bir desendir. Ancak, çalışma kapsamında geliştirilen uygulamadaki numerik klavye adaptif bir tasarımdır ve kullanıcılar sisteme kayıt olurken 0'dan 9'a rakamların yerleri rastgele dağıtılarak Şekil 7.2'de gösterildiği gibi onlara özel adaptif bir klavye üretilmektedir. Kullanıcılar bu adaptif klavyeleri kullanıp, rastgele üretilen 6 karakterli numaraları yazarak tanımlama ve doğrulama yapmaktadırlar.



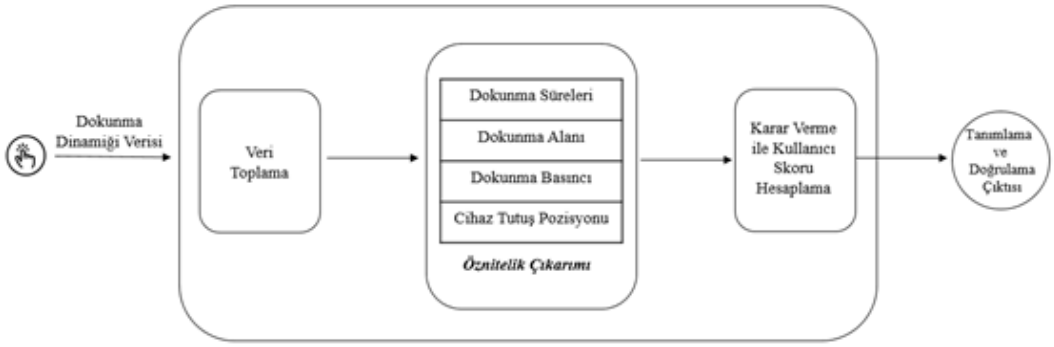
Şekil 7.2 : Numerik klavye kullanıcı bazlı rastgele dağıtım.

Kullanıcı tanımlama ve doğrulama işlemleri de üretilen bu adaptif klavyeler yardımıyla yapılmaktadır. Toplanan verilerin yardımıyla tanımlanan kullanıcıların, geliştirilen dokunma dinamiği uygulaması ile hem kimlik doğrulaması hem de anomali tespiti yapılabilmesi amaçlanmaktadır.

Biyometrik tabanlı kimlik doğrulama üzerine olan çalışmalarda, çalışmalar verilerin toplanması, işlenmesi, öznitelik çıkarımı, karar verme mekanizması ve performans değerlendirme olarak alt başlıklara ayrılmaktadır.

7.1 Modelleme Süreci

Uygulamanın modelleme süreci Şekil 7.3'de gösterildiği gibi veri toplama, öznitelik çıkarımı ve karar verme adımlarından oluşmaktadır.



Şekil 7.3 : Uygulama modellemesi.

7.1.1 Veri toplama

Bir kullanıcı kimlik doğrulama işlemi kullanıcıyı tanımlama ve kullanıcıyı doğrulama olmak üzere iki ana başlıktan oluşur. Tanımlama adımında sistemler kullanıcılarını topladıkları bilgilerin yardımıyla ayırt edici özelliklerini kullanarak tanımlarlar.

Çalışma kapsamında geliştirilen uygulama için kullanıcı tanımlama adımında, kullanıcılara sisteme ilk girişlerinde KVKK metnini onaylamaları sonrasında kısa bir bilgilendirme sayfası gösterilir. Bu sayfada kullanıcıların kendilerine özel üretilen klavye ile nasıl eğitileceği anlatılır. Ardından kullanıcılar belirlenen deneme sayısındaki başarılı tekrar ile eğitilir ve bu sırada dokunma davranış verileri toplanır.

Veri toplama adımı için geliştirilen süreç 30 farklı kullanıcı tarafından denenmiştir. Kullanıcılara, 100000 ile 999999 arasındaki 6 karakterli sayılar rastgele üretilerek gösterilmiş ve kendilerine özel oluşturulmuş adaptif klavye yardımıyla bu numaraları girmeleri istenmiştir. Herhangi bir hatalı girişte, silme tuşu o ana kadar o sayı için girilen tüm karakterleri silmiş ve o sayı için toplanan dokunma dinamiği verileri sıfırlanmıştır. 30 farklı kullanıcının her biri için eğitim aşamasında toplam 30 farklı doğru giriş yapmaları istenmiştir. Toplam olarak 30 kullanıcı * 30'ar deneme * 6 karakterli giriş olmak üzere 5400 dokunma hareketinden, her bir hareket 7 farklı değeri tuttuğu için 37800 dokunma dinamiği verisi toplanmıştır. Ayrıca, kullanıcılara deneyler sonrası kullanıcı deneyimi ve farkındalığını ölçen 15 soruluk

bir anket yapılmıştır. Bu anket verileri de sistem başarısı ölçümü ve sonuçların analizinde kullanılmaktadır.

7.1.2 Öznitelik çıkarımı

Öznitelik çıkarımı adımı, kullanıcılardan toplanan verilerin sistemde kullanıcıların karakterize edilip özgün profillerinin oluşturabilmesi için ayırt edici niteliklerinin belirlenmesidir. Öznitelik çıkarımı, hem kullanıcı tanımlama hem de kullanıcı doğrulama adımı için gereklidir.

Bu çalışma kapsamında; tuşlara dokunma süreleri arasındaki zaman farkları, dokunma alanı, dokunma basıncı ve cihaz tutuş pozisyonu öznitelik olarak kullanılmıştır.

7.1.2.1 Dokunma süreleri

Hem tuş dinamiği hem de dokunma dinamiğinde en çok kullanılan ayırt edici özelliktir. Geliştirilen uygulamada kullanıcılardan 6 karakterli bir rakam dizisini doğru olarak girmeleri beklenmektedir. Doğal olarak, bu adımda toplam 6 rakama dokunmaları gerekmektedir. Dokunma sürelerinin hesaplanabilmesi için, kullanıcıların bir rakama dokundukları an ve o rakamı bıraktıkları andaki zaman damgası değerleri tutulmuştur.

Dokunma ve bırakma süreleri arasındaki farklar milisaniye cinsinden hesaplanmaktadır. Uygulamada her tuşa ait dokunma ve bırakma süreleri tutulduğu için, birbirleriyle ilişkileri de tüm dokunma davranışları için incelenebilmektedir. Örneğin, ilk tuşa dokunma ve ikinci tuşa dokunma süreleri arasındaki fark veya ilk tuşa dokunma ile son tuşu bırakma süreleri arasındaki fark, tüm bu değerlerin anlık zaman damgası verisine sahip olunduğu için hesaplanabilmektedir.

Uygulamada kullanıcıların bir tuşa dokunma anlarındaki zaman damgası P (press), bir tuşu bırakma anlarındaki zaman damgası R (release), basılı kalma süresi ise bir tuşa dokunma ve bırakma arasında geçen zaman D (dwell) olmak üzere denklem 7.1'deki gibi hesaplanmaktadır.

$$DT_n = R_n - P_n \tag{7.1}$$

İki başarılı dokunma arasındaki zaman farkı, uçuş süresi F (flight) olarak ifade edilirse, bu uygulama için denklem 7.2, 7.3, 7.4 ve 7.5'de gösterilen 4 farklı değer özniteliğe dahil edilmiştir.

$$F_1T_n = P_{n+1} - R_n \tag{7.2}$$

$$F_2T_n = R_{n+1} - R_n \tag{7.3}$$

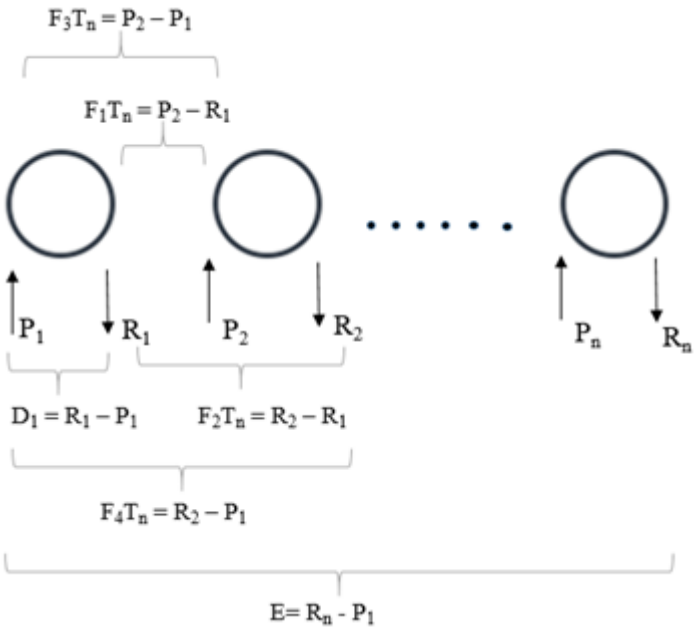
$$F_3T_n = P_{n+1} - P_n \tag{7.4}$$

$$F_4T_n = R_{n+1} - P_n \tag{7.5}$$

Dokunma süresi, son başarılı rakamın bırakılması ile ilk başarılı rakama dokunulması arasındaki zaman farkı E (elapse time) olmak üzere denklem 7.6'daki gibi hesaplanmaktadır ve uygulamada öznitelik değerlerine dahil edilmiştir.

$$E_n = R_6 - P_1 \tag{7.6}$$

Dokunma süresi olarak uygulamada DT_n, F_1T_n, F_2T_n, F_3T_n, F_4T_n ve E_n değerleri öznitelik olarak kullanılmıştır ve Şekil 7.4'te gösterildiği gibi hesaplanmıştır.



Şekil 7.4 : Dokunma süreleri hesaplamaları.

7.1.2.2 Dokunma alanı

Eller ve parmaklar insanların büyük çoğunluğunda birbirinden farklı olduğu için dokunma dinamiğini inceleyen bir uygulamada ekrana dokunma alanı ayırt edici bir

özellik olarak kabul edilebilir. Farklı parmak ucu boyutuna sahip kullanıcılar farklı dokunma alanına sahiptirler. Kullanıcının ekrana dokunduğu noktaların alan cinsinden değeri çalışma kapsamında öznitelik olarak kullanılmıştır. Her bir dokunma eylemi için dokunma alanı ayrı ayrı tutulmaktadır.

7.1.2.3 Dokunma basıncı

Kullanıcıların ekranla etkileşime girerken dokunma anında ekrana uyguladıkları basınç çalışma kapsamında öznitelik olarak kullanılmıştır. Dokunma basıncı gözlemleyerek taklit edilmesi zor olduğu için güvenli bir ayırt edici özellik olarak değerlendirilmektedir. Kullanıcılardan 6 karakterli sayıları girerken her bir dokunma eylemi için basınç değerleri cihazlardaki sensör yardımıyla alınmıştır.

7.1.2.4 Cihaz tutuş pozisyonu

Dokunma eylemlerinin özellikleri birer ayırt edici özellik olduğu gibi cihaz tutuş pozisyonları da ayırt edici özellik olarak değerlendirilmektedir. İnsanlar mobil cihazları kullanırken farklı tutuş pozisyonları sergilerler; bu bağlamda cihaz tutuş pozisyonu da çalışma kapsamında öznitelik olarak kullanılmıştır. Bu özelliğin hesaplanabilmesi için cihazlardaki jiroskop sensörleri kullanılmıştır. Jiroskop sensörü x,y ve z üç boyutlu konum bilgisini anlık olarak vermektedir, bu veriler üç farklı boyut için de ayrı ayrı tutulmuştur. Cihaz tutuş pozisyonu bir kullanıcı için kendi içinde de sık sık değişebileceğinden bu değerin önceliği çalışma kapsamında düşük tutulmuştur.

7.1.3 Karar verme

Karar verme, kullanıcılardan toplanan verilerin öznitelik çıkarımından belirlenen parametrelerin de kullanılarak, kimlik doğrulama sırasında kullanıcıların gerçekten o kullanıcı olup olmadığının tespit edildiği adımdır. Yapılan literatür araştırmalarında biyometrik çalışmaların karar verme adımlarında; karar ağacı, yapay sinir ağları, uzaklık ölçümü, makine öğrenmesi, kümeleme analizi, standart sapma ve ortalama gibi istatistiksel tekniklerin kullanıldığı görülmüştür.

Bu çalışma kapsamında, istatistiksel yöntemler karar verme adımında kullanılacak teknik olarak tercih edilmiştir. Dokunma dinamikleri, büyük çoğunlukla dokunmatik taşınabilir cihazlarla insanlar arasındaki etkileşimden ortaya çıkmaktadır. Mobil cihazlar, gelişen teknolojiye rağmen kompleks bilgisayarlardan daha düşük işlem

kapasitelerine sahiptir. Örnek çalışmalarda kullanılan diğer teknikler, hem daha çok kaynak kullanımı, zaman ve performans gerektirdiğinden hem de veri işleme ve analiz için herhangi bir dış sunucuya ihtiyaç kalmaması için, bu çalışmada istatistiksel yöntemler karar verme adımında tercih edilmiştir.

Eğitim adımında toplanan veriler kullanılarak her bir öznitelik için hesaplanan ortalama değerler, uygulama doğrulama performansını belirleyen eşik değerin de yardımıyla, her bir öznitelik için ayrı ayrı, kullanıcı girdisi ile karşılaştırılarak denklem 7.7'deki hesaplama yardımıyla doğrulama yapılmaktadır.

$$| \text{Beklenen değer} - \text{Asıl değer} | < \text{Eşik Değeri} * \text{Beklenen değer} \qquad (7.7)$$

7.2 Uygulama Mimarisi

İnsan bilgisayar etkileşiminin bir sonucu olarak ortaya çıkan davranışsal biyometrik verilerle kullanıcı kimlik doğrulamasının en güncel örnekleri, her geçen gün insan hayatında kendisine daha çok yer edinen mobil cihazlarda bu işlevi yerine getiren uygulamaların geliştirilmesidir. Bu çalışma kapsamında, gerek literatür araştırmalarındaki örnek çalışmalardan edinilen bilgiler gerekse kullanıcı deneyimleri ve ihtiyaçları göz önüne alınarak bir model tasarlanmış ve bu model bir "Touch Dynamics" ismi verilen Android uygulaması olarak geliştirilmiştir.

7.2.1 Kullanılan teknolojiler

Dokunma dinamiği ile kullanıcı kimlik doğrulama çalışması kapsamında, tasarlanan modeli gerçeklemek için bir Android mobil uygulama geliştirilmiştir. Android, Linux çekirdeğini kullanan Google firmasının desteklediği dünyanın en çok kullanılan mobil işletim sistemidir. Touch Dynamics uygulaması da Java programlama dili ile Android Studio IDE'si kullanılarak geliştirilmiştir.

Uygulamada kullanıcı kaydı, doğrulama ve veri tabanı için Firebase platformu kullanılmıştır. Sistemlerin büyük çoğunluğu, özellikle de kompleks ve fazla kullanıcılı sistemler; kullanıcılarını sistemlerine kaydetme, doğrulama, verilerini veri tabanlarında saklama ve bunlara tekrar ulaşmaya, uygulamalar; aynı veriye farklı cihazlardan erişmeye, sistem yöneticileri de kolayca kullanıcı hareketlerine ulaşarak bunları analiz etmeye ihtiyaç duymaktadır. Firebase, farklı platformlar için bu konularda çözüm bulan oldukça popüler bir üründür ve uygulama yönetimi, kullanıcı

etkinlikleri, veri tabanları, bildirim gönderme gibi fonksiyonları güvenli bir şekilde yerine getirmektedir. Touch Dynamics uygulamasında, kullanıcı verilerini toplama, işleme ve davranışsal verilerden doğrulama yapmayı amaçladığı için, sunucu tarafına ekstra bir kodlama yapmadan, Firebase platformundaki fonksiyonları kullanılarak sunucu ihtiyaçları giderilmiştir.

Uygulamada kullanıcı kayıt ve doğrulama için Firebase Auth kullanılmıştır. Burada e-posta ve şifre modu tercih edilmiştir. Böylece kullanıcılar sunucu kodu olmadan güvenli bir şekilde doğrulanabilmiş ve yetkilendirilebilmiştir.

Touch Dynamics uygulamasında, kullanıcıların verilerini saklamak için geleneksel yöntemlerin aksine, gerçek zamanlı veri tabanı kullanılmıştır. Firebase Realtime Database ile uygulama verileri bulut ortamda saklanmaktadır. Bu sayede mobil, web, masaüstü bilgisayarlar gibi farklı istemciler aynı veriye senkron olarak erişebilmektedirler. Veriler geleneksel yöntemlerde olduğu gibi SQL ile oluşturulan tablolar ile saklanıp taşınmamakta; JSON objeleri şeklinde saklanarak aktarımı kolaylaştırılmaktadır. Uygulama tarafında ise implemente edilen callback interface'ler sayesinde verilerdeki değişim anlık olarak izlenebilmektedir.

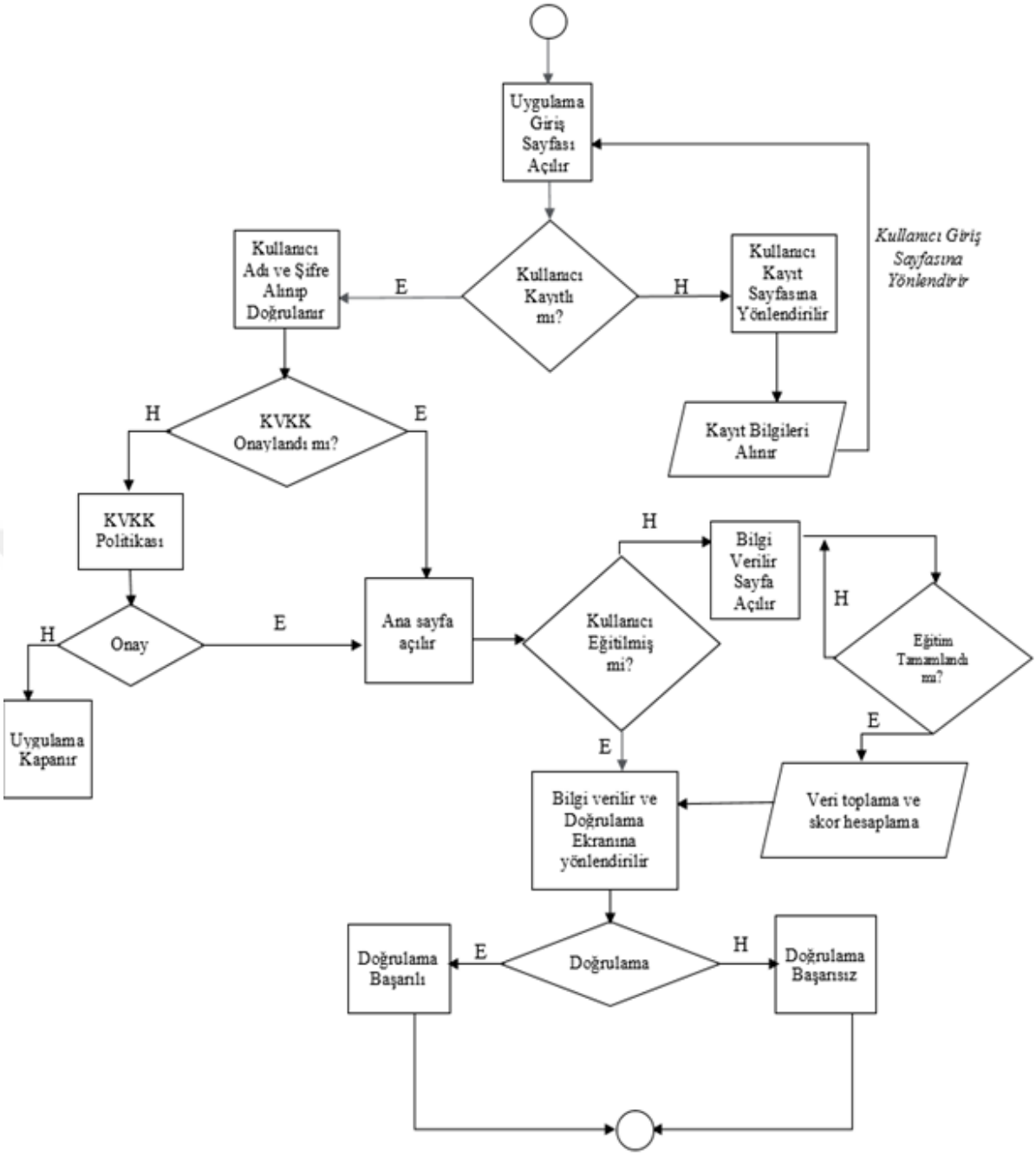
Model tasarımında belirlenen ayırt edici özelliklerden jiroskop değerlerinin bulunabilmesi için, Android'in TYPE_GYROSCOPE sensörü kullanılmıştır. Bu sensör sayesinde cihazın x, y ve z eksenlerinin her biri için yön ölçümü yapılabilmesini sağlayan verilere ulaşılabilmektedir. Bu veriler yardımıyla, cihaz tutuş pozisyonu hesaplanmaktadır.

Kullanıcı dokunma verileri için ise MotionEvent nesnesi kullanılmıştır. Android cihazlarda kullanıcının dokunma anındaki farklı değerlerini tutan bu nesne sayesinde, dokunma ve bırakma anı, dokunma basıncı ve kullanıcının parmağının ekrana temas ettiği dokunma alanı değerlerine erişilmiştir.

7.2.2 Akış diyagramı

Geliştirilen Touch Dynamics uygulaması kullanıcı kaydı, kullanıcı girişi, "Kişisel Verilerin Korunması ve İşlenmesi Hakkında Aydınlatma Metni", ana sayfa ve kullanıcı tanımlama ve doğrulamasının yapıldığı adımlardan oluşmaktadır.

Bu adımlara bağlı olarak uygulamanın akış diyagramı Şekil 7.5'te detaylı olarak gösterilmiştir.



Şekil 7.5 : Uygulama akış diyagramı.

7.2.3 Parametrik değişkenler

Sistem, Çizelge 7.1'de açıklandığı gibi üç parametrik değişkene sahiptir.

Çizelge 7.1 : Uygulamada kullanılan parametrik değişkenler.

Parametrik değişken	Açıklama
TRAINING_COUNT	Kullanıcılara eğitim aşamasında kaç tane deneme yaptırılacağının tutulduğu değerdir.

Çizelge 7.1 (devam) : Uygulamada kullanılan parametrik değişkenler.

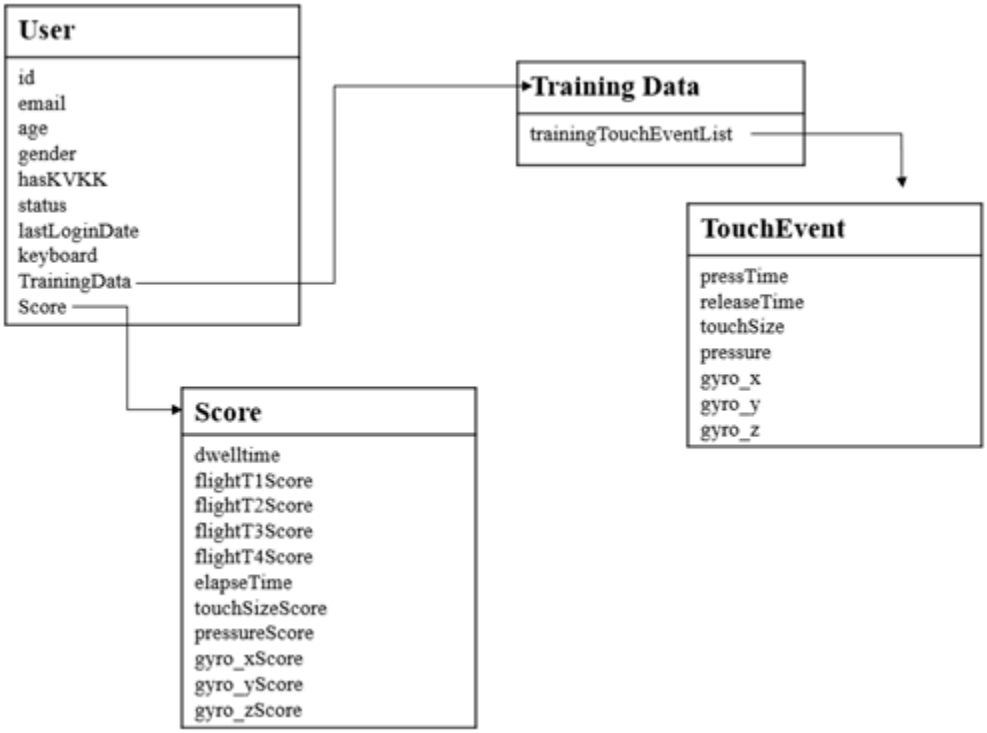
Parametrik değişken	Açıklama
THRESHOLD	Uygulama doğrulama performansını belirleyen eşik değerdir. Doğruluk değeri olarak belirlenen bu eşik değer düşük olarak tanımlanırsa, hata payı yüksek olan denemelerde sisteme giriş yapabilecektir. Güvenlik seviyesini azaltmak isteyen uygulama yöneticileri bu değeri azaltabilir.
AUTH_MODE	Uygulama sürekli ve statik doğrulama olmak üzere iki modda çalışmaktadır.

Statik doğrulama modunda, eğitimde elde edilen veriler kullanıcı skoru belirlenmesinde bir defa kullanılır ve bu skor üzerinden doğrulama yapılır.

Sürekli doğrulama modunda ise, kullanıcının doğrulandığı her değer eğitim verisine katılır ve kullanıcı skoru güncellenir.

7.2.4 Nesne listesi ve gerçek zamanlı veri tabanı

Uygulama nesne listesi ve gerçek zamanlı veri tabanı Şekil 7.6'da gösterilmiş ve nesne elemanları Çizelge 7.2, 7.3, 7.4 ve 7.5'te açıklanmıştır.



Şekil 7.6 : Nesne listesi ve gerçek zamanlı veri tabanı ilişki diyagramı.

Çizelge 7.2 : Kullanıcı nesnesi.

User	Kullanıcıları Tanımlayan Nesne
id	Firebase gerçek zamanlı veri tabanında kullanıcıyı tanımlamak için kullanılan değişken
email	Kullanıcılardan kayıt sırasında alınan e-posta adresi
age	Kullanıcılardan kayıt sırasında alınan yaş bilgisi
Gender	Kullanıcılardan kayıt sırasında alınan cinsiyet bilgisi
hasKvkk	Kullanıcının daha önce KVKK metnini onaylayıp onaylamadığını gösteren değişken
status	Kullanıcıların eğitim aşamasında mı doğrulama aşamasında mı olduklarını gösteren değişken
lastLoginDate	Kullanıcının uygulamaya giriş yaptığı son tarih
keyboard	Kullanıcının sisteme kaydında oluşturulan rastgele klavye değeri
trainingData	Kullanıcıların eğitim sırasındaki özniteliklerinden oluşan verilerin tutulduğu nesne
score	Kullanıcının belirlenen kurallara göre hesaplanan skor değerlerinin tutulduğu nesne

Çizelge 7.3 : Kullanıcı eğitim verisi nesnesi.

TrainingData	Kullanıcı eğitim verilerinin tutulduğu nesne
List<List<TouchEvent>> trainingTouchEventList	Eğitim sırasındaki tüm denemelerin belirlenen dokunma dinamiği verilerini içeren liste

Çizelge 7.4 : Kullanıcı dokunma dinamiği veri nesnesi.

TouchEvent	Kullanıcı dokunma dinamiklerinin tutulduğu nesne
pressTime	Herhangi bir tuşa dokunma anı zaman damgası değeri
releaseTime	Dokunulan tuşu bırakma anı zaman damgası değeri
touchSize	Dokunma alanı değeri
pressure	Dokunma basıncı değeri
gyro_x	Cihaz jiroskobu x koordinatı
gyro_y	Cihaz jiroskobu y koordinatı
gyro_z	Cihaz jiroskobu z koordinatı

Çizelge 7.5 : Kullanıcı performans değeri nesnesi.

Score	Kullanıcı performans değerlerinin tutulduğu nesne
dwellTime	Dokunulan tuşa basılı kalma süresi
flightT1Score	Bir tuşa dokunulma anı ile bir önceki tuşu bırakma anı arasındaki uçuş zaman farkı
flightT2Score	Bir tuşu bırakma anı ile bir önceki tuşu bırakma anı arasındaki uçuş zaman farkı
flightT3Score	Bir tuşa dokunulma anı ile bir önceki tuşa dokunulma anı arasındaki uçuş zaman farkı
flightT4Score	Bir tuşu bırakma anı ile bir önceki tuşa dokunma anı arasındaki uçuş zaman farkı
elapseTime	6 karakterli rakamlar girilirken son tuşu bırakma anı ile ilk tuşa dokunma anı arasındaki zaman farkı
touchSizeScore	Kullanıcının dokunma alanı verilerinden hesaplanan değer
pressureScore	Kullanıcının dokunma basıncından hesaplanan değer

Çizelge 7.5 (devam) : Kullanıcı performans değeri nesnesi.

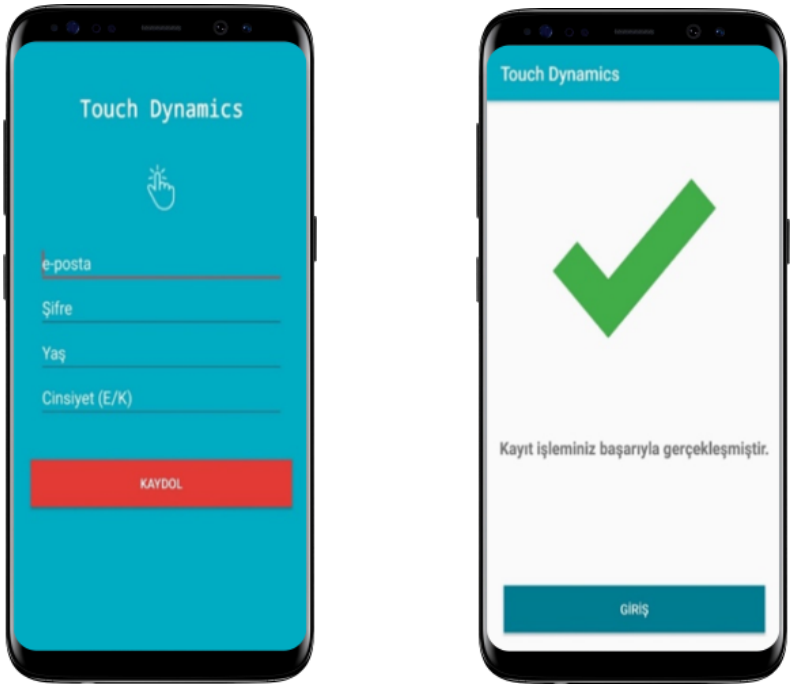
Score	Kullanıcı performans değerlerinin tutulduğu nesne
gyro_xScore	Cihaz jiroskobu x koordinatı verilerinden hesaplanan değer
gyro_yScore	Cihaz jiroskobu y koordinatı verilerinden hesaplanan değer
gyro_zScore	Cihaz jiroskobu z koordinatı verilerinden hesaplanan değer

7.3 Uygulama Akışı

7.3.1 Kullanıcı kayıt

Kullanıcı kayıt sayfası, uygulamayı ilk defa açan ya da henüz üyeliği bulunmayan kullanıcıları kayıt etmek için geliştirilmiştir. Bu ekranda Şekil 7.7'de gösterildiği gibi uygulamaya gireceği kullanıcı adı yerine geçecek e-posta adresi, uygulamaya girmesi için kullanılacak şifre ve istatistiki veriler için kullanılacak yaş ve cinsiyet bilgileri alınır. Bu bilgiler kullanıcı nesnesine eklenerek, veri tabanında yeni bir kullanıcı oluşturulur. Aynı zamanda, rakamlardan oluşan kullanıcılara özel üretilmiş klavye bilgisi de bu adımda kullanıcı nesnesi içine eklenir.

Burada alınan şifre bilgisi çalışma kapsamında, dokunma dinamikleri ile kullanıcı doğrulamada kullanılacak olan şifre ile ilgili değildir. Sisteme ilk defa kaydolacak ya da daha sonra doğrulama yapmak isteyen bir kullanıcıyı, sisteme tanımlama amacıyla eklenmiştir.



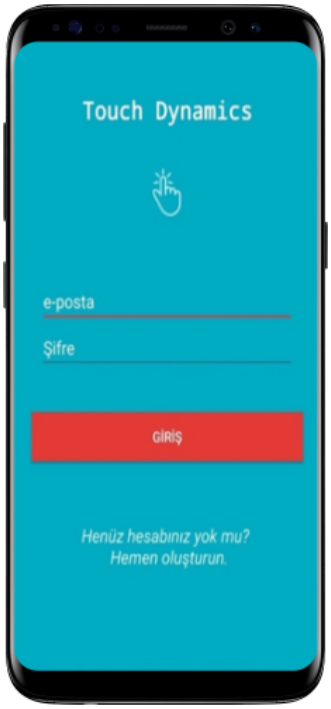
Şekil 7.7 : Kullanıcı kayıt ekranı görüntüsü.

7.3.2 Kullanıcı girişi

Giriş sayfası, sisteme kayıt olan kullanıcıların sisteme başarılı bir şekilde giriş yapabilmeleri için Şekil 7.8'de gösterildiği gibi geliştirilmiştir. Kullanıcı sisteme kayıt olurken girdiği e-posta ve şifre bilgileri ile giriş butonuna dokunarak sisteme giriş yapabilir.

Kullanıcıların bilgilerini eksiksiz ve doğru girmesinin ardından, e-posta ve şifre bilgileri Firebase Authentication yardımıyla sistem tarafından doğrulanır. Kullanıcı doğrulandıktan sonra veri tabanından kullanıcı nesnesi alınır ve kullanıcının daha önceden KVKK metnini onaylayıp onaylamadığı kontrol edilir. Eğer onaylamışsa, kullanıcı ana sayfaya yönlendirilir, eğer onaylamamışsa onaylaması için KVKK sayfasına yönlendirilir. Aynı zamanda, kullanıcı her giriş yaptığında veri tabanında tutulan son giriş tarihi alanı da giriş anındaki tarih ile güncellenir. Son giriş tarihi alanı ile kullanıcının uzun süreli sisteme giriş yapmadığı zamanlarda, kullanıcıya tekrar eğitim için bir hatırlatma gönderilebilmesi amaçlanmıştır.

Sisteme henüz kayıt olmamış kullanıcıların kayıt olabilmesi için, giriş sayfasında "Henüz hesabınız yok mu? Hemen oluşturun." metni bulunmaktadır. Kullanıcılar bu metne dokunarak kullanıcı kayıt sayfasına yönlenebilirler.



Şekil 7.8 : Kullanıcı giriş ekranı görüntüsü.

7.3.3 KVKK

Çalışma kapsamında geliştirilen uygulama, sisteme kayıt olurken kullanıcılardan e-posta adresi, yaş, cinsiyet gibi kişiyi doğrudan tanımlamaya yarayan bilgileri almaktadır. Ayrıca uygulama, çalışma amacı gereği hem eğitimler hem doğrulama adımlarında dolaylı olarak kişiyi tanımlamaya yarayabilecek hassas verileri toplamakta, işlemekte ve saklamaktadır. Bu bağlamda, 6698 sayılı "Kişisel Verileri Koruma Kanunu" kapsamında, sisteme giriş yapan kullanıcılara bir defalık "Kişisel Verilerin Korunması ve İşlenmesi Hakkında Aydınlatma Metni" Şekil 7.9'daki gibi gösterilmekte ve kullanıcıların devam edebilmeleri için bu metni onaylamaları istenmektedir.

Kullanıcılar metni okuduktan sonra "Okudum, Onayladım." butonu yardımıyla ana sayfaya yönlendirilirler. Metni kabul etmeyen kullanıcıların devam etmesine izin verilmez. Metni onaylayan kullanıcılar için kullanıcı nesnesindeki KVKK metnini okuduğunu belirten alan güncellenir. Bu alan sayesinde, metin kullanıcılara bir dahaki girişlerinde gösterilmez ve doğrudan ana sayfaya yönlenirler. Uygulamada kullanılan "Kişisel Verilerin Korunması ve İşlenmesi Hakkında Aydınlatma Metni" Ek A.1'de verilmiştir.

Şekil 7.9 : KVKK onay ekranı görüntüsü.

7.3.4 Ana sayfa

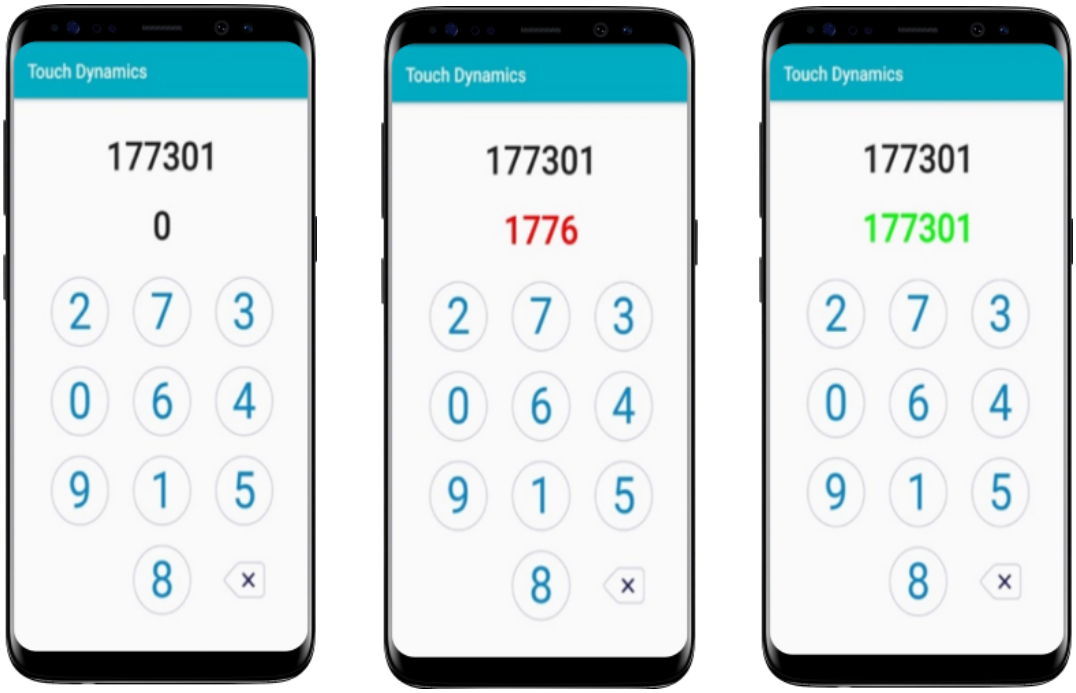
Uygulamaya giriş yapan kullanıcılar Şekil 7.10'da gösterilen ana sayfaya yönlendirilir. Henüz verileri toplanmamış kullanıcılar için uygulama hakkında kısa bir bilgilendirme ve eğitim sırasında neler yapması gerektiği ile ilgili bir bilgilendirme metni gösterilir ve "Eğitime Başla" butonu ile kullanıcılar eğitim sayfasına yönlendirilir. Sistem tarafından eğitilmiş kullanıcılara ise, doğrulama adımı ile ilgili bir bilgi verilir ve "Doğrulamaya Başla" butonu ile doğrulama sayfasına yönlenmeleri sağlanır.

Şekil 7.10 : Uygulama ana sayfa görüntüsü.

7.3.5 Numerik klavye

Kullanıcılara her biri için özel olarak üretilmiş numerik klavye, girmeleri beklenen ve o an girdikleri sayılar Şekil 7.11'deki gibi gösterilir. 0-9 rakamları klasik numerik klavyelerin aksine, yerleri dağıtılarak kullanıcıya sunulur. Eğitim aşamasında kullanıcılardan üst üste belirtilen sayıda doğru giriş yapmaları beklenmektedir. Herhangi bir karakter yanlış girildiği anda girilen sayının rengi kırmızı olur, hedef sayı tamamen doğru girildiğinde ise rengi yeşil olur ve bir sonraki sayı üretilir. Doğrulama için gelen kullanıcılarda da aynı kurallar geçerlidir; ancak bu adımdaki kullanıcılar doğru giriş yaptıktan sonra, performans skorları ile karşılaştırılarak sistemin kullanıcıyı doğrulaması halinde işlem başarılı ekranına yönlendirilirler. Sistem tarafından doğrulanamayan kullanıcılar, doğrulama başarısız ekranına yönlendirilirler.

Hedef sayı, 100000 ile 999999 arasında rastgele olarak üretilir ve kullanıcı girilen sayı alanına girdiği her bir karakter için anlık olarak karakter bazında karşılaştırma yapılır. Bir karakterin bile yanlış girilmesi durumunda, silme tuşu ile o ana kadar girilen tüm karakterler silinir. Buradaki amaç, tuşlar arasındaki tuşa dokunma ve tuşu bırakma zamanları arasındaki farkların öznitelik olarak belirlenmesi dolayısıyla, eğer karakter bazlı silinme yapılmış olursa bu sürelerin ciddi şekilde etkilenerek analiz değerlerini bozacak olmasıdır.

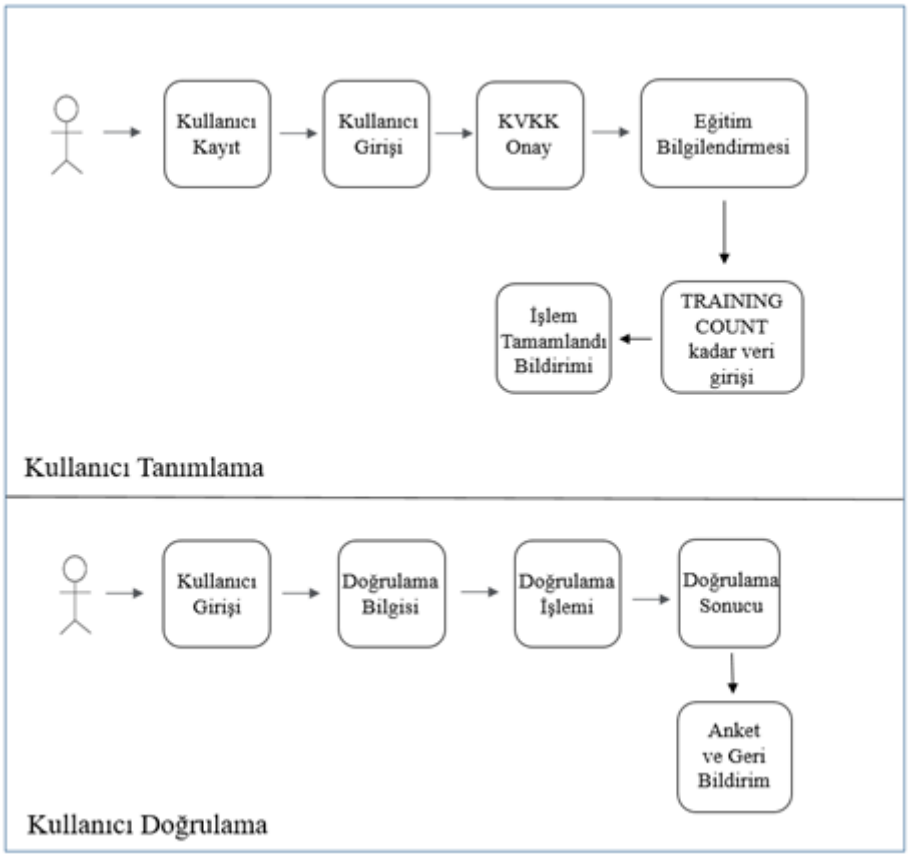


Şekil 7.11 : Uygulama numerik klavye ekran görüntüsü.

7.4 Deneyler ve Değerlendirme Sonuçları

7.4.1 Deneyler

Deneyler Şekil 7.12'de gösterildiği gibi Kullanıcı Tanımlama ve Doğrulama olmak üzere iki adımda gerçekleştirilmiştir.



Şekil 7.12 : Uygulama kullanıcı diyagramı.

Modellenen ve geliştirilen uygulama deneyleri 30 kullanıcı katılımıyla yapılmıştır. Uygulamanın parametrik değişkenleri deneyler sırasında;

- TRAINING_COUNT: 30
- THRESHOLD: 0.8
- AUTH_MODE: Statik

olacak şekilde belirlenmiştir. Bir diğer deyişle, her bir kullanıcıya eğitim aşamasında 30 deneme yaptırılmış, doğruluk değeri 0.8 olarak belirlenmiş ve uygulama eğitim verileri doğrulama adımında gelen değerlerle güncellemeyen statik modda çalıştırılmıştır.

Toplamda 30 kullanıcı * 30 deneme * 6 dokunma = 5400 dokunma verisi toplanmıştır.

Eğitim adımını tamamlayan kullanıcılara eğitimlerini tamamladıklarını bildiren işlem başarılı sayfası gösterilmiştir. Bu işlemle beraber toplanan veriler istatistiksel yöntemle işlenerek kullanıcı performansları hesaplanmıştır. Elde edilen değerler, kullanıcı nesnesi altındaki skor nesnesine atanmıştır.

Kullanıcı tanımlama adımının tamamlanmasından sonra, ana sayfaya yönlendirilen kullanıcılara, doğrulama adımı ile ilgili bilgiler verilmiştir. Her bir kullanıcıdan, sistemin yanlış reddetme oranını hesaplayabilmek için 5 defa doğrulama denemesi yapmaları istenmiştir. Her bir deneme ardından, doğrulamanın başarılı veya başarısız olduğu işlem sonuç ekranları yardımıyla kullanıcılara gösterilmiştir. Kullanıcı doğrulama deneylerini de tamamlayan kullanıcılara, davranışsal biyometri tabanlı kimlik doğrulama uygulaması hakkında 15 soruluk bir anket yapılmıştır.

Deneylerin ikinci kısmında, uygulamanın performansını belirlerken kullanılmak üzere, sisteme sahtekar giriş denemeleri yapılmıştır. Daha önce sisteme kayıt olan ve deneyleri tamamlayan kullanıcılardan sisteme giriş yapmaları istenmiş, ancak bu sefer doğrulama adımında daha önce sistem hakkında hiç bilgi verilmemiş ve eğitilmemiş denekler tarafından o an giriş yapan kullanıcı yerine doğrulama yapması istenmiştir. Asıl kullanıcılar giriş yaptıktan sonra, cihazlara sahtekar giriş denemesi yapacak deneklere verilmiştir. Toplam 5 farklı sahtekar denek yardımıyla, 10 farklı eğitilmiş kullanıcı hesabına 100 farklı sahtekar doğrulama denemesi yapılmıştır. Böylece, kişiye özel tasarlanan klavye ve veri toplama sonrası hesaplanan puanlar yardımıyla doğrulanan kullanıcılar yerine, başka kişiler girmeye çalıştığında oluşacak performans, yanlış kabul oranı, ölçülmüştür.

7.4.2 Anket

Deneylerle tanımlama ve doğrulama adımlarını tamamlayan kullanıcılara, hem çalışma ve uygulama hakkında geri bildirim almak hem de davranışsal biyometri hakkındaki farkındalıklarını ölçmek için 15 sorudan oluşan bir anket yapılmıştır [EK A.2]. Bu ankette kullanıcılara günde ne kadar telefonla ilgilendikleri, şifrelerini ne sıklıkla değiştirdikleri, şifrelerini belirlerken hangi kriterleri uyguladıkları, kişisel verilerin güvenliği ile davranışsal biyometri hakkında sorular sorulmuş, geliştirilen uygulama hakkında geri bildirimler alınmıştır.

Anket sonuçları sayesinde, mobil cihazların insan hayatındaki yeri, davranışsal verilerin önemi hakkındaki farkındalık, deneklerin bilgi güvenliği hakkındaki bilgisi ve bilinci, geliştirilen uygulamanın örtük öğrenme desteğindeki başarısı, kullanıcıların öğrenme şekilleri konularında çıkarımlar yapılması sağlanmıştır.

7.4.3 Değerlendirme metrikleri

Bir biyometrik sistemin performansı ölçülürken belirli metrikler kullanılır. Mükemmel bir sistemde hata oranının sıfır olması beklense de bu gerçekte pek de mümkün değildir. Bir biyometrik sistemin doğruluğunu ölçerken, sisteme birçok gerçek ve sahtekar girişimde bulunulur ve bunlar kaydedilir. Benzerlik puanlarına, değişken bir puan eşiği uygulanarak FRR ve FAR hesaplanır.

Biyometrik sistemlerde doğrulama için bir eşik değeri belirlenir ve performans bu eşik değeri ile elde edilen sonuçların karşılaştırılmasıyla bulunur. Eşik değeri, sistemin değerleri ve güvenlik kriterlerine göre belirlenir. Burada tanımlanan FAR ve FRR değerleri, eşik değerine bağlı olarak değişecek, normalde geçerli kullanıcıyken reddedilen ya da sahtekar kullanıcıyken sisteme kabul edilenler bu değerin azaltılıp çoğaltılmasıyla değişecek, bu da performans kriterlerine göre sistemi etkileyecektir [70].

FAR : Yanlış kabul oranı = Sahtekar başarılı giriş sayısı / Toplam sahtekar giriş deneme sayısı

FRR : Yanlış ret oranı = Yanlış reddedilme sayısı / Toplam gerçek giriş deneme sayısı

EER : Eş hata oranı

7.4.4 Değerlendirme sonuçları

30 kullanıcı ile yapılan deneyler sonucunda, 30 * 5 = 150 toplam gerçek giriş denemesinden 25 yanlış reddedilme gerçekleşmiştir. Bu durumda,

FRR = 25 / 150 = 0.16 hesaplanmıştır.

5 kullanıcı ile yapılan denemelerde, 5 * 20 = 100 toplam sahtekar giriş denemesinden 28 sahtekar başarılı giriş gerçekleşmiştir. Bu durumda,

FAR = 28 / 100 = 0.28 hesaplanmıştır.

Bu verilerle, EER = 0.22 hesaplanmıştır.

8. SONUÇ VE ÖNERİLER

Bu çalışma kapsamında, kullanıcıların davranışsal biyometrik verileri kullanılarak kimlik doğrulama yapan bir model tasarlanmış ve uygulama geliştirilmiştir. Çalışmada, insan bilgisayar etkileşiminin artan mobil cihaz kullanımı ile paralel olarak öneminin artması, adaptif tasarımların kullanıcılara pasif olarak öğretilmesini sağlayacak örtük öğrenme yöntemi, bilgi güvenliği ve güvenlik açıkları hakkında detaylı bilgiler verilmiş, kullanıcı kimlik doğrulama için kullanılan yöntemler detaylı şekilde açıklanmış ve karşılaştırılmıştır. Literatür araştırmaları ve benzer çalışmalar özetlenmiş, ardından çalışma kapsamında tasarlanan model teknik olarak açıklanmış ve deneyler yapılarak sonuçları belirlenen performans metrikleri yardımıyla değerlendirilmiştir.

Dokunma dinamikleri kişiden kişiye göre değişen ayırt edici özellikler olarak kabul edilmektedir. Artan mobil cihaz kullanım oranları ile beraber ortaya ciddi derecede dokunma verisi çıkmaktadır. Ayrıca, mobil cihazlardaki sensörler yardımıyla birçok veriye kolayca ulaşılabilmektedir. Bu bağlamda tasarlanan model ve geliştirilen uygulama kullanıcı kimlik doğrulama ve anomali tespitinde kullanılabilir bir performans sergilemiştir.

Geliştirilen uygulama 30 kişi üzerinde denenmiş, her bir kullanıcı için 30'ar deneme ile öğretilmiş, ardından doğru giriş ve sahtekar giriş denemeleri yapılarak performans ölçülmüştür. Deneyler sonucunda, 0.16 FRR, 0.28 FAR ve 0.22 EER değerleri elde edilmiştir.

8.1 Kullanılan Yöntemler

Tez çalışması kapsamında, her bir kullanıcıya özel adaptif numerik bir klavye üretilmiş, bu klavye belirlenen deneme sayısı ile kullanıcılara örtük öğrenme yöntemi ile öğretilmiştir. Bu kullanıcı tanımlama sürecinde, kullanıcıların mobil cihazlarla olan etkileşiminden dokunma dinamiği verileri toplanmıştır. Dokunma verileri;

- Dokunma süreleri,

- Dokunma alanı,
- Dokunma basıncı,
- Cihaz tutuş pozisyonu olmak üzere dört ayırt edici özellik kullanılarak çıkarımlar yapılmıştır.

Toplanan veriler istatiksel yöntemlerle analiz edilmiş ve her kullanıcı için birer profil oluşturulmuştur. Kullanıcı doğrulama adımında, oluşturulan profillerdeki performans verileri doğrulama sırasındaki değerler ile eşik değeri de dikkate alınarak karşılaştırılmış ve kullanıcı doğrulaması yapılmıştır.

8.2 Sonuçlar

Tez kapsamında geliştirilen uygulama fiziksel biyometrik verilerden yararlanarak doğrulama yapılan sistemlerdeki gibi ekstra cihazlara ihtiyaç duymadığı, hali hazırda mobil cihazlardaki sensörler yardımıyla verileri elde ettiği için diğer yöntemlere göre maliyet olarak oldukça uygundur. Ayrıca, cihazlarda bulunan sensörleri kullanan dokunma dinamiği uygulamaları ile yalnızca sistemlere girişte değil, sistem içerisindeki hareketler de kullanıcıya hissettirilmeden arka planda izlenebilmektedir. Bu veriler analiz edilerek anomali tespiti yapılabilmektedir.

Uygulama diğer mobil işletim sistemlerini kullanan cihazlar için de geliştirilebilir. Bu durum, zaten fazlasıyla vakit geçirilen mobil cihazları kullanarak bu uygulamaların doğrulama yapabileceğini göstermekte, ek bir donanım ihtiyacı ortaya çıkarmamaktadır. Bu ayrıca, kullanıcı deneyimi açısından da oldukça önemli bir avantajdır.

Çalışma kapsamında tasarlanan model yalnızca sistem girişlerinde değil, ikinci faktör kimlik doğrulama olarak da kullanılabilir. Düşük güvenlik ihtiyacı duyan uygulamalar için sistem girişlerinde kullanılabilir olsa da daha yüksek güvenlik seviyesine ihtiyaç duyan sistemlerde ek bir ürünle birlikte ikinci faktör kimlik doğrulama ürünü olarak kullanılması daha sağlıklı olacaktır. Ayrıca, genelde bankaların kullandığı OTP gibi kısa mesajla iletilen tek kullanımlık şifreler yerine kullanılarak ciddi bir maliyeti de ortadan kaldırabilir.

Geliştirilen model fiziksel biyometrik çözümlere göre daha düşük doğruluk payına sahiptir. Ancak maliyeti düşük olduğu için, farklı çözümlerle birlikte kullanılabilir.

Sistemin bir diğer dezavantajı ise, zaman için de değişebilecek kullanıcı davranışlarıdır. Bu durumun önüne geçmek için kullanıcıların verileri sürekli izlenerek performansları takip edilmelidir. Unutma, davranış değişikliği gibi durumların önüne geçilmeye çalışılmalıdır.

Deneylerin son adımında kullanıcılara yapılan anketlerden aşağıdaki sonuçlar çıkarılmıştır.

- Denekler günde ortalama 3-5 saat telefonları ile ilgilendiklerini belirtmiştir. Bu da mobil cihazların hayatımızda ne kadar önemli bir yer kapladığını ve buradaki insan bilgisayar etkileşiminden ortaya çıkan verilerin önemini göstermiştir. Bu bilgi, dokunma dinamiği verilerinin kimlik doğrulama için ne kadar kullanılabilir olduğunu göstermektedir.
- Deneklerin büyük çoğunluğu sistemler zorlamadıkça şifrelerini değiştirmediklerini belirtmişlerdir. Bu durum bir güvenlik açığı niteliğinde değerlendirilebilir. Statik şifrelerin belirlenmesi ve bunların sürekli olarak kullanılması sosyal mühendislik yöntemi kullanan saldırganların işini kolaylaştırmaktadır. Tez kapsamında geliştirilen uygulama ile kullanıcılar hatırlamak veya değiştirmek zorunda oldukları şifreler yerine, günlük hayatlarını etkileyecek ekstra bir eylem gerektirmeden mobil cihazlara dokunma aktiviteleri ile doğrulanabilmektedir. Sürekli kimlik doğrulamayı sağladığı için dokunma dinamiği yöntemleri geleneksel yöntemlere göre bu konuda daha uygundur.
- Deneklerin tamamı, daha kolay hatırlayabilmek için farklı çevrimiçi sistemlere kayıt olurken birbirine çok benzeyen ya da birbirinin aynısı şifreleri tercih ettiklerini belirtmiştir. Bu durum beraberinde çok ciddi bir güvenlik açığını getirmektedir. Dolandırıcılar, kişisel bilgilere dayanarak tahmin ettikleri ya da başka yöntemlerle bir hesabının şifresini ele geçirdikleri kullanıcıların, diğer tüm sistemlerdeki hesaplarını da bu yüzden ele geçirebilirler. Tez kapsamında geliştirilen uygulama, kullanıcının farkında olmadan öğrendiği klavye yardımıyla davranışlarından çıkarım yaparak kimlik doğruladığı için bu açıdan geleneksel yöntemlerdeki sorunlara bir çözüm olarak değerlendirilebilir.

- Deneklerin büyük çoğunluğu, her ne kadar teknolojiyle iç içe olsalar da veri güvenliği konusunda bilgi sahibi olmadıklarını belirtmişlerdir. Bu durum, çevrimiçi sistemleri bilinçsiz kullanma dolayısıyla da güvenlik açığına sebep olmaktadır. Ancak, tez kapsamında geliştirilen uygulama, kullanıcıların farkında olmadan rutin hareketlerini takip ederek verileri pasif olarak toplayıp değerlendirdiğinden bilinçsiz kullanıcılar için de bilgi güvenliği sağlamaktadır. Dokunma dinamiği uygulamaları için kullanıcılardan ekstra bir eylem istenmemekte, aksine rutin kullanımları izlenerek çıkarımlar yapılmaktadır. Bu da kullanıcı deneyimi açısından geleneksel yöntemlere göre oldukça avantajlıdır.
- Denekler tez kapsamında tasarlanan bir modelin parçası olan adaptif numerik klavyenin veri güvenliği konusunda ek bir katman olduğunu düşündüklerini belirtmişlerdir ve güvenlik yöntemi olarak faydalı bulmuşlardır.
- Deneklerin tamamı, kendilerine ait rastgele rakamların dağıtıldığı klavyeyi deneyler sırasında farkında olmadan öğrendiklerini belirtmiştir. Bu, tez çalışması kapsamında örtük öğrenme yönteminin adaptif tasarım yardımıyla başarıyla uygulandığını göstermektedir.

8.3 Öneriler

Dokunma dinamikleri konusu geliştirilen farklı uygulamalarda belirlenen öznitelikler yardımıyla büyümeye devam etmektedir. Bu çalışmalar beraberinde oldukça büyük ve önemli kişisel verileri de getirmektedir. Bu bağlamda, teknolojinin gelişme hızını yakalayamayan bilgi güvenliği bilinci konusunda bir risk ortaya çıkmaktadır. Dokunma dinamiği verileri kişiler arasında ayırt edici bir nitelik taşıdığı için oldukça hassas verilerdir. Bu noktada, hem kullanıcılar bilinçli hareket etmeli hem de bu verileri toplayan sistemler kişisel verilerin gizliliği ve güvenliği konusunda hassasiyet göstermelidir.

Öte yandan, bu uygulama da diğer tüm davranışsal biyometrik yöntemler gibi daha maliyetsiz olsa da fiziksel biyometrik yöntemlere göre doğruluk değeri düşüktür. Bu durumdan dolayı, davranışsal biyometrik tabanlı kullanıcı kimlik doğrulama sistemleri ikinci faktör kimlik doğrulamada kullanılmak için daha uygundur.

KAYNAKLAR

[1] **De Houwer, J., Barnes-Holmes, D.,& Moors, A.** (2013). What is learning? On the nature and merits of a functional definition of learning. *Psychonomic Bulletin & Review*, 20(4), 631-642. doi: 10.3758/s13423-013-0386-3

[2] **Guthrie, E.R.** (1935). *Psychology of Learning*. Oxford, England: Harper.

[3] **Frensch, P.A., & Runger, D.** (2003). Implicit Learning. *Current Directions in Psychological Science*, 12(1), 13-18. doi: 10.1111/1467-8721.01213

[4] **Akbulut-Taş, M., Karataş-Coşkun, M.** (2014). The Effect of Explicit Teaching and Implicit Learning of Concept and Generalization Structure on the Acquisition of Explicit Knowledge of Concept of Generalization Structure. *Çukurova University Faculty of Education Journal*, 43(1), 19-38. doi: 10.14812/cufej.2014.001

[5] **Mathews, R.C., Buss, R.R., Stanley, W.B., Blanchard-Fields., & et al.** (1989). Role of implicit and explicit processes in learning from examples: A synergistic effect. *Journal of Experimental Psychology: Learning, Memory, an Cognition*, 15(6), 1083-1100. doi: 10.1037/0278-7393.15.6.1083

[6] **Cleeremans, A., & Dienes, Z**. (2008). Computational Models of Implicit Learning. *The Cambridge Handbook of Computational Psychology*, 396–421. doi: 10.1017/CBO9780511816772.018

[7] **DeKeyser, R.** (2003). Implicit and Explicit Learning. *The Handbook of Second Language Learning Acquisition*, 312-348. doi: 10.1002/9780470756492.ch11

[8] **Reber, A.S.** (1967). Implicit Learning of Artificial Grammars. *Journal of Verbal Learning and Verbal Behavior*, 5, 858- 863.

[9] **Nissen, M.J., & Bullemer, P.** (1987). Attention Requirements of Learning: Evidence from Performance Measures. *Cognitive Psychology*, 19, 1-32

[10] **Berry, D. C., & Broadbent, D.E.** (1984). On the Relationship between Task Performance and Associated Verbalizable Knowledge. *The Quarterly Journal of Experimental Psychology Section A*, 36(2), 209-231. doi: 10.1080/14640748408402156

[11] **Kissel, R.** (2013). Glossary of Key Information Security Terms. *National Institute of Standards and Technology*. Alındığı tarih: 15.04.2019, adres: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913810. (s.97)

[12] **Gürol, C., & Sağıroğlu Ş**. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, 9(3), 165-174.

[13] **Suhail Q., & Quadri, S.M.K.** (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, 7(3), 185-194.

[14] **European Co-operation for Accreditation.** (2018). EA Personal Data Protection Policy. Alındığı tarih: 16.04.2019, adres: https://european-accreditation.org/information-center/ea-personal-data-protection-policy/.

[15] **Mevzuat.** (2016). Kişisel Verilerin Korunması Kanunu. Alındığı tarih: 17.04.2019, adres: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf.

[16] **Ronald, R.S.** (2012). Guide for Conducting Risk Assessments. *National Institute of Standards and Technology (NIST) Special Publication*. Alındığı tarih: 15.04.2019, adres: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[17] **Agrafiotis. I., Nurse, J.R.C., Goldsmith, M., Creese, S., & Upton, D.** (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1), 1-15.

[18] **IBM.** (2015). Analysis of cyber attack and incident data for the financial services industry from IBM's worldwide security services operations. *IBM 2015 Cyber Security Intelligence Index for Financial Services Research Report.* Alındığı tarih: 15.04.2019, adres: https://www.ibm.com/downloads/cas/OBMG6BJL.

[19] **Maan, P.S., & Sharma, M.** (2012). Social Engineering: A Partial Techical Attack. *IJCSI International Journal of Computer Science Issues*, 9(2), 557.

[20] **Waghmare, P., Longadge, R., & Kapgate, D.** (2014). A Review on Shoulder Surfing Attack in Authentication Technique. *IJCSN International Journal of Computer Science and Network*, 3(6), 573.

[21] **Daş, R. & Gündüz, M.Z**. (Ekim, 2014*). Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri*. Bilgi Güvenliği ve Kriptoloji Konferansı, İTÜ, İstanbul.

[22] **Dodge, R. C., Carver, C., & Ferguson A.J.** (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73-80.

[23] **Morris, R., & Thompson, K.** (1979). Password Security: a case history. *Communications of the ACM*, 22(11), 594-597.

[24] **Vaithyasubramanian, S., Christy A., & Saravanan, D.** (2014). An analysis of Markov password against Brute force attack for effective web applications. *Applied Mathematical Science*, 8(117), 5823-5830.

[25] **Owens, P. J.** (2008). *A Study of Passwords and Methods Used in Brute-Force SSH Attacks.* (Yüksek Lisans Tezi, Clarkson Üniversitesi, New York). Alındığı tarih: 15.04.2019, adres: https://people.clarkson.edu/~owensjp/pubs/Owens_MS_thesis.pdf.

[26] **Rader, E., & Wash, R.** (2015). Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1), 121-144.

[27] **O'Gorman, L.** (2003). Comparing Paswords, Tokens, and Biometrics for User Authentication. *Proceedings of the IEEE*, 91(12), 2019-2040.

[28] **Committee on National Security Systems**. (2010). National Information Assurance Glossary. Alındığı tarih: 15.04.2019, adres: https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf. (s.71).

[29] **Baukes, M.** (2018, Ocak, 22). Everbody Knows: How Knowledge-Based Authentication Died. *Forbes*. Alındığı tarih: 14.04.2019, adres: https://www.forbes.com/sites/forbestechcouncil/2018/01/22/everybody-knows-how-knowledge-based-authentication-died/#22f235dd4eee.

[30] **Bonneau, J., Bursztein, E., Caron, I., Jackson, R., & Williamson, M.** (2015). Secrets, Lies, and Account Recovery. *Proceedings of the 24th International Conference on World Wide Web- WWW' 15*. doi: 10.1145/2736277.2741691

[31] **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. Alındığı tarih: 17.04.2019, adres: https://people.eecs.berkeley.edu/~johnw/cs294-97/papers/intro-biometric.pdf.

[32] **Wayman, J. L.** (2001). Fundamentals of Biometric Authentication Technologies. *International Journal of Image and Graphics,* 1(1), 93-13.

[33] **Bhattacharyya, D., Ranjan, R., Alisherov, A.F., & Choi, M.** (2009). Biometric Authentication: A Review. *International Journal of u- and e- Service, Science and Technology*, 2(3), 13-27.

[34] **Lee, H. C., & Gaensslen, R. E.,** (1991). *Advances in fingerprint technology*. New York, NY: Elsevier.

[35] **Uchida, K.** (2005). Detection and Recognition Technologies Fingerprint Identification. *NEC Journal of Advanced Technology*, 2(1), 19-27.

[36] **Leeuw, K., & Bergstra J.** (Eds). (2007). *The History of Information Security: A Comprehensive Handbook*. Oxford, England: Elsevier.

[37] **Science Daily**. (1997). *"Mugshot" Can Find A Face in the Crowd- Face Recognition Software Prepares to Go to Work in the Streets.* Alındığı tarih: 17.04.2019, adres: https://www.sciencedaily.com/releases/1997/11/971112070100.htm.

[38] **Pontin, M.W.** (2007). Better Face Recognition Software. *MIT Technology Review*. Alındığı tarih: 18.04.2019, adres: https://www.technologyreview.com/s/407976/better-face-recognition-software/.

[39] **Kak, N., Gupta, R. & Mahajan, S**. (2010). Iris Recognition System. *International Journal of Advanced Computer Science and Applications*, 1(1), 34-40.

[40] **Liu, S., & Silverman, M.** (2001). A practical guide to biometrical security technology. *IT Professional,* 3(1), 27-32. Alındığı tarih: 17.04.2019, adres: https://ieeexplore.ieee.org/document/899930.

[41] **Jain, K. A., Ross, A., & Pankanti, S.** (1999). A Prototype Hand Geometry-based Verification System. *2nd International Conference on Audio- and Video- based Biometrics Person Authentication* (ss. 166-171). Washington DC.

[42] **Kumar, A., Wong, D.C.D., Shen, C.H., & Jain, K.A**. (2003). Personal Verification Using Palmprint and Hand Geometry Biometric. *International Conference on Audio- and Video- based Biometrics Person Authentication* (ss. 668-678). Berlin.

[43] **Zhang, D., & Shu, W.** (1999). Two novel characteristics in palmprint verification: datum point invariance and line feature matching. *Pattern Recognition*, 32(4), 691-702.

[44] **Yampolskiy, R.V., & Govindaraju, V.** (2008). Behavioural biometrics: a survet and classification, *Journal of Biometrics*, 1(1), 81-113. doi: 10.1504/IJBM.2008.018665

[45] **Rigas, I., Economou, G., & Fotopoulos, S.** (2012). Biometric Identification based on the eye movements and graph matching techniques, *Pattern Recognition Letters*, 33(6), 786-792.

[46] **Faundez-Zanuy, M.** (2007). On-line signature recognition based on VQ-DTW, *Pattern Recognition*, 40(3), 981-992.

[47] **Dalka, P, & Czyzewski, A.** (2009). Lip movement and gesture recognition for a multimodal human-computer interface, *2009 International Multiconference on Computer Science and Information Technology*, 7(3), 124-139.

[48] **Sultana, M, Paul, P. P., & Gavrilova, M.** (2015). Social behavioral biometrics: and emerging trend, *International Journal of Pattern Recognition and Artificial Intelligence*, 29(8), 1556013.

[49] **Shen, C., Cai, Z., Guan, X., Du, Y., & Maxion, R.A.** (2013). User Authentication Through Mouse Dynamics, *IEEE Transactions on Information Forensics and Security*, 8(1). 16-30.

[50] **L. F. Coppenrath and Associates.** (2001). *Biopassword Technology Overview*. Alındığı tarih: 23.04.2019, adres: http://www.lfca.net/Reference Documents/Biometric Technology Overview.pdf.

[51] **L. F. Coppenrath and Associates.** (2001). *Biometric Solutions By Classification*. Alındığı tarih: 23.04.2019, adres: http://www.lfca.net/Reference Documents/Biometric Solutions By Classification.pdf.

[52] **Teh, P.S., Zhang, N., Teoh, A.B.J., & Chen, K.** (2016). A survey on touch dynamics authentication in mobile devices, *Computer and Security*, 59, 210-235. doi: 10.1016/j.cose.2016.03.003

[53] **Bryan, W.L., & Harter, N.** (1897). Studies in the physiology and psychology of the telegraphic language, *Psychological Review*, 4(1), 27-53.

[54] **Banerjee, S.P., & Woodard, D.L.** (2012). Biometric authentication and identification using Keystroke Dynamics: A survey, *Journal of Pattern Recognition Research*, 7(1), 116-139. doi: 10.13176/11.427

[55] **Chandrasekar, V., & Suresh Kumar, S.** (2015). A dexterous feature selection artificial immune system algorithm for keystroke dynamics, *Stochastic Analysis and Applications*, 34(1), 147-154.

[56] **Chandrasekar, V., Kumar, S.S, & Maheswari, T.** (2016). Authentication based on keystroke dynamics using stochastic diffusion algorithm, *Stochastic Analysis and Applications*, 34(1), 155- 164.

[57] **Kim, J., Kim, H., & Kang, P.** (2018) Keystroke Dynamics-based user authentication using freely typed text based on user adaptive feature extraction and novelty detection, *Applied Soft Computing*, 62, 1077-1087.

[58] **Gaines, R.S., Lisowski, W., Press, S.J, & Shapiro, N**. (1980). Authentication by Keystroke Timing: Some Preliminary Results, No. RAND-R-2526-NSF. Alındığı tarih: 19.04.2019, adres: https://www.rand.org/pubs/reports/R2526.html.

[59] **Deutschmann, I., Nordstrom P., & Nilsson, L.** (2013). Continuous Authentication Using Behavioral Biometrics, *IT Professional*, 15(4), 12-15. doi: 10.1109/MITP.2013.50

[60] **Prabha, R.S, & Vidhyapriya, R.** (2017). Intruder Detection System Based on Behavioral Biometric Security, *Journal of Science & Industrial Research,* 76, 90-94.

[61] **Peng, G. Zhou, G., Nguyen, D.T., Qi, X., Yang, Q., & Wang, S.** (2016). Continuus Authentication with Touch Behavioral Biometrics and Voice on Wearable Glasses*, IEEE Transactions on Human – Machine Sytems*, 47(3), 404-416. doi: 10.1109/THMS.2016.2623562

[62] **Bevan, C., & Fraser, D.S.** (2016). Different strokes for different folks? Revealing the physical characteristics of smartphone users from their swipe gestures, *International Journal of Human- Computer Studies*, 88, 51-61.

[63] **Antal, M., & Szabo, Z.L.** (2015). Biometric authentication based on touchscreen swipe patterns, *9th International Conference Interdisciplinarity in Engineering*, INTER-ENG, Romania. Alındığı tarih: 19.04.2019, adres: https://core.ac.uk/download/pdf/82013149.pdf.

[64] **Antal, M., Bokor, Z., & Szabo, L.Z.** (2015). Information revealed from scrolling interactions on mobile devices, *Pattern Recognition Letters*, 56, 7-13.

[65] **Zhou, L., Kang Y., Zhang, D., & Lai, J.** (2016). Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones*, Decision Support Systems*, 92,14-24.

[66] **Buriro, A., Crispo, B., & Conti, M**. (2019). A bimodal behavioral biometric-based user authentication scheme for smartphones, *Journal of Information Security and Applications*, 44, 89-103.

[67] **Kambourakis, G., Damopoulos, D., Papamartzivanos, D., & Pavlidakis, E.** (2014). Introducing touchstroke: keystroke-based authentication system for smartphones, *Security and Communication Networks*, 9(6), 542–554. doi: 10.1002/sec.1061

[68] **SenthilPrabha, R., Vidhyapriya, R., & RavithaRajalakshmi, N.** (2016). Performance analysis for a Touch dynamic authentication system with reduced feature set using neural networks, *IETE Journal of Research*, 62(2), 198- 204.

[69] **Zheng, N., Bai, K., Huang, H., & Wang, H.** (2014). You are How You Touch: User Verification on Smartphones via Tapping Behaviors, *2014 IEEE 22nd International Conference on Network Protocols,* 221-232.

[70] **Gümüş, F., Ata, O., & Balık, H.H.** (2018). Davranışsal Biyometrinin 5 Yılı: Kimlik Doğruluma ve Anomali Tespit Uygulamaları, *Fırat Üniversitesi Müh. Bil. Dergisi,* 30(1), 345-364.

EKLER

EK A.1 : Kişisel Verilerin Korunması ve İşlenmesi Hakkında Aydınlatma Metni
EK A.2 : Touch Dynamics Uygulaması Deney Geribildirim Anketi

EK A.1

Kişisel Verilerin Korunması ve İşlenmesi Hakkında Aydınlatma Metni

Bu tez kapsamında kullanılan kişisel verilerinizin güvenliği hususuna azami hassasiyet göstermekteyiz. Bu bilinçle, bu çalışmaya katılan tüm şahıslara ait her türlü kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**KVK Kanunu**")'na uygun olarak işlenerek, muhafaza edilmesine büyük önem atfetmekteyiz. Bu sorumluluğumuzun tam idraki ile KVK Kanunu kapsamında tanımlı "Veri Sorumlusu" sıfatıyla, kişisel verilerinizi aşağıda izah edildiği surette ve mevzuat tarafından emredilen sınırlar çerçevesinde işlemekteyiz.

1) Kişisel Verilerin Hangi Amaçla İşleneceği

İşbu tez için gerçekleştirilen çalışma kapsamında uygulama kullanıcılarının dokunma etkinliklerini kapsayan birtakım davranışsal biyometrik verilerine ihtiyaç duyulmaktadır. Bu kapsamda toplanan kişisel verileriniz, kanun tarafından öngörülen temel ilkelere uygun olarak ve Kanun'un 5. ve 6. maddelerinde belirtilen kişisel veri işleme şartları ve amaçları dahilinde bizim tarafımızdan yapılan çalışmanın geliştirilmesi amacıyla işlenecektir.

2) İşlenen Kişisel Verilerin Kimlere ve Hangi Amaçla Aktarılabileceği

Toplanan kişisel verileriniz, bu tez nezdindeki çalışmayı yürütmek ve test etmek amacıyla, tez içerisinde kullanılacaktır. Verilerin kullanıldığı çalışma, 6698 sayılı Kanun'un 8. ve 9. maddelerinde belirtilen kişisel verileri işleme şartları ve amaçları çerçevesinde İstanbul Teknik Üniversitesi tarafından belirlenen jüri üyelerine sunulacak ve kabul edildiği takdirde Yükseköğretim Kurulu'na iletilecektir.

3) Kişisel Veri Toplamanın Yöntemi ve Hukuki Sebebi

Tez için kullandığımız kişisel verileriniz geliştirilen çalışmada denenmek amacıyla mevzuata ve Kanun'a uygun bir şekilde hukuki sebeplerine dayanılarak toplanmaktadır. Toplanan kişisel verileriniz 6698 sayılı Kanun'un 5. ve 6. maddelerinde belirtilen kişisel veri işleme şartları ve amaçları kapsamında bu Bilgilendirme'nin (b) ve (c) maddelerinde belirtilen amaçlarla da işlenebilmekte ve aktarılabilmektedir.

4) Kişisel Veri Sahibinin 6698 sayılı Kanun'un 11. Maddesinde Sayılan Hakları

Kişisel veri sahipleri olarak, haklarınıza ilişkin taleplerinizi aşağıda düzenlenen yöntemlerle bize iletmeniz durumunda talebin niteliğine göre talebi en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandıracağız. Ancak, işlemin ayrıca bir maliyeti gerektirmesi halinde, tarafımızdan Kişisel Verileri Koruma Kurulu'nca belirlenen tarifedeki ücret alınacaktır. Bu kapsamda kişisel veri sahipleri;

- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- 6698 sayılı Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme haklarına sahiptir.

6698 sayılı Kanunu'nun 13. maddesinin 1. fıkrası gereğince, yukarıda belirtilen haklarınızı kullanmak ile ilgili talebinizi, yazılı veya Kişisel Verileri Koruma Kurulu'nun belirlediği diğer yöntemlerle bize iletebilirsiniz. Kişisel Verileri Koruma Kurulu, şu aşamada herhangi bir yöntem belirlemediği için, başvurunuzu, 6698 sayılı Kanun gereğince, yazılı olarak bize iletmeniz gerekmektedir. Bu çerçevede 6698 sayılı Kanunu'n 11. maddesi kapsamında yapacağınız başvurularda yazılı olarak başvurunuzu ileteceğiniz kanallar ve usuller aşağıda açıklanmaktadır:

Yukarıda belirtilen haklarınızı kullanmak için kimliğinizi tespit edici gerekli bilgiler ile 6698 sayılı Kanunu'n 11. maddesinde belirtilen haklarınızdan kullanmayı talep ettiğiniz hakkınıza yönelik açıklamalarınızı içeren talebinizi; bize ekte yer alan Veri Sahibi Başvuru formunu doldurarak ve formun imzalı bir nüshasını İTÜ Öğrenci İşleri Daire Başkanlığı'na kimliğinizi tespit edici belgeler ile bizzat elden iletebilir, noter kanalıyla veya 6698 sayılı Kanun'da belirtilen diğer yöntemler ile gönderilebilir veya ilgili formu ridvanozguvenir@gmail.com adresine güvenli elektronik imzalı olarak iletebilirsiniz.

EK A.2

Bu anketin amacı az önce kullanmış olduğunuzu Davranışsal Biyometrik Çözümler uygulaması ile ilgili geri bildirim toplayarak dokunma dinamiği uygulaması ile ilgili farkındalığınızı artırmaktır.
Bu anket 15 sorudan oluşmaktadır. Sorulara eksiksiz ve gerçekçi cevap vermeniz çalışmamıza daha fazla katkı sağlayacaktır.
Katkınız için şimdiden çok teşekkürler.

1) Günde ortalama ne kadar süre telefonunuzla ilgileniyorsunuz?

   1 saatten az ☐
   1-3 saat ☐
   3-5 saat ☐
   5 saatten fazla ☐

2) Şifrelerinizi ne sıklıkla değiştiriyorsunuz?

   Haftada bir ☐
   Ayda bir ☐
   3 ayda bir ☐
   6 ayda bir ☐
   Zorunlu olmadıkça değiştirmiyorum. ☐

3) Farklı site veya sistemlere giriş yaparken şifre seçiminizi önceki şifrelerinize benzer şekilde mi belirlersiniz?

   Evet ☐
   Hayır ☐

4) Şifrelerinizi hatırlamak için bir yere not alır mısınız?

   Evet ☐
   Hayır ☐

5) Bir uygulamaya giriş yaptığınızda kişisel bilgilerin korunması ile ilgili bildirimleri tüm ayrıntılarıyla okur musunuz?

   Evet ☐
   Hayır ☐

6) Sizce uygulamada yer alan bilgilendirmeler çalışmayı tamamlama için yeterli midir?

   Evet ☐
   Hayır ☐

7) Sizce bu uygulama için sunulan deneme sayısı kişiselleşen klavyeyi öğrenmek için yeterli midir?

   Evet ☐
   Hayır ☐

8) Uygulamayı kimlik doğrulama yöntemi olarak faydalı buldunuz mu?

Evet ☐
Hayır ☐

9) Sizce klavyenin kişiye özel üretilmesi veri güvenliğinizi artırır mı?

Evet ☐
Hayır ☐

10) Deneyin eğitim aşamasında bana özel oluşturulan klavyeyi farkında olmadan öğrendiğimi düşünüyorum.

Evet ☐
Hayır ☐

11) 0'in olduğu pozisyondaki sayıyı kolay öğrendiğinizi düşünüyor musunuz?

Evet ☐
Hayır ☐

12) Davranışsal verilerin kimlik doğrulama işlemi için kullanıldığını biliyor muydunuz?

Evet ☐
Hayır ☐

13) Sizce kullanıcı kimlik doğrulama işlemindeki en etkili yöntem davranışsal biyometrik kimlik doğrulama mıdır?

Evet ☐
Hayır ☐

14) Bu uygulama sayesinde kimlik doğrulama ve bilgi güvenliğinin korunması konusunda sizde bir farkındalık oluştu mu?

Evet ☐
Hayır ☐

15) Çevrimiçi ortamlarda kişisel verilerimi paylaşırken güvensizlik hissediyorum.

Evet ☐
Hayır ☐

Eklemek istediklerinizi lütfen buraya yazınız:

ÖZGEÇMİŞ

Ad-Soyad : Rıdvan ÖZGÜVENİR

Doğum Tarihi ve Yeri : 01.02.1991, Bakırköy

E-posta : ridvanozguvenir@gmail.com

ÖĞRENİM DURUMU:

- **Lisans** : 2014, İTÜ, Bilgisayar ve Bilişim Fakültesi, Bilgisayar Mühendisliği
- **Yüksek Lisans** : 2019, İTÜ, Bilişim Uygulamaları, Bilgi ve Haberleşme Mühendisliği

MESLEKİ DENEYİMLER:

- Mayıs 2013 – Haziran 2014 tarihleri arasında Cardtek Group'ta Yazılım Geliştirmeci olarak çalıştı.
- Temmuz 2014'ten beri Yapı Kredi Bankası'nda Proje Mühendisi olarak çalışmaktadır.