T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ PROGRAMI
YÜKSEK LİSANS TEZİ

KURUMLARDA SİBER GÜVENLİK TABANLI ZİYARETÇİ KONTROL SİSTEMİ TASARIMI VE UYGULAMASI

Mehmet NACAROĞLU

Danışman
Prof. Dr. Çiğdem TARHAN

İZMİR – 2023

TEZ ONAY SAYFASI

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum "Kurumlarda Siber Güvenlik Tabanlı Ziyaretçi Kontrol Sistemi Tasarımı ve Uygulaması" adlı çalışmanın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

27/07/2023

Mehmet NACAROĞLU

ÖZET

Yüksek Lisans Tezi

Kurumlarda Siber Güvenlik Tabanlı

Ziyaretçi Kontrol Sistemi Tasarımı ve Uygulaması

Mehmet NACAROĞLU

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

Yönetim Bilişim Sistemleri Anabilim Dalı

Yönetim Bilişim Sistemleri Programı

Teknolojinin ve ulaşım araçlarının çok hızlı bir şekilde geliştiği dünyamızda, insanlar dünyanın farklı noktalarında yapılan toplantı, seminer, söyleşi, sempozyum, çalıştay, brifing, fuar vb. yerlere hızlı bir şekilde katılım sağlayabilmektedir. Bu katılımlar internet üzerinden çevrimiçi veya fiziki olarak sağlanabilmektedir.

Fiziki katılım sağlanan, özellikle herkese açık olmayan, güvenlik önlemlerinin üst düzey olduğu kurumlarda icra edilen toplantılarda dünyanın farklı noktalarından gelen yerli ve yabancı katılımcıların giriş güvenliğinin sağlanması önemli bir sorun haline gelmiştir. Giriş kontrollerinde görev yapan güvenlik personelleri katılımcıları daha önceden hiç tanımadıkları ve görmedikleri için gelen gerçek katılımcıların dışında, sahte kimliklerle art niyetli kişiler tarafından yetkisiz girişler yapılabilmekte, amaçlarına göre bilgi casusluğu, terörizm amaçlı saldırı vb. eylemlerde bulunabilmektedirler.

Tez kapsamında, kurumlarda katılımcı güvenliğini en üst seviyeye çıkarabilmek, yetkisiz girişleri önleyebilmek ve katılımcıların kontrolünü kolaylıkla sağlanabilmesi için siber güvenlik tabanlı ziyaretçi kontrol sistemi tasarlanmıştır.

Ziyaretçi Kontrol Sistemi, Raspberry Pi 3 kullanarak geliştirilmiş olup katılım yapacak olan ziyaretçilerin bilgileri resimleri ile sisteme yüklenmektedir. Siber güvenlik önlemleri kapsamında sahte kimlik veya giriş

kartlarını engellemek üzere ziyaretçilere QR kod ile oluşturulmuş üzerlerinde isimlerinin bulunduğu Ziyaretçi Giriş Kartı katılımcılara toplantı, seminer, söyleşi, sempozyum, çalıştay, brifing, fuar vb. programların tarihlerinden günler önce ulaştırılarak bu kartlarla giriş yapması istenmektedir.

Kurumlarda giriş noktalarında güvenlik görevlileri tarafından katılımcıların Ziyaretçi Giriş Kartı sorgulanmakta ve kamera yardımıyla kart üzerindeki QR kodu okutularak ziyaretçin yetkili olup olmadığı teyit edilmektedir. Güvenlik personeli tarafından sistemden kişinin fotoğrafı ile birebir aynı olduğu teyit edildikten sonra girişine müsaade edilmektedir.

Anahtar Kelimeler: Raspberry Pi, QR Kod, Ziyaretçi Kontrol Sistemleri, Siber Güvenlik, Kurumlarda Giriş Sistemleri, Yetkisiz Giriş Önleme Sistemleri.

ABSTRACT

Master'sThesis

Cyber Security BasedVisitor

Control System Design andImplementation in Institutions

Mehmet NACAROĞLU

Dokuz Eylül University

Graduate School of SocialSciences

Department of Management Information Systems

Management Information SystemsProgram

In our world where technology and means of transportation develop very rapidly, people attend meetings, seminars, conversations, symposiums, workshops, briefings, fairs, etc. held in different parts of the world can quickly participate in places. These participations can be provided online or physically over the internet.

Ensuring the entrance security of local and foreign participants from different parts of the world has become an important problem in the meetings held in institutions where physical participation is provided, especially in institutions that are not open to everyone and where security measures are at a high level. Since the security personnel working at the entrance controls do not know or see the participants before, unauthorized entries can be made by malicious people with fake identities, apart from the real participants, and they can engage in acts such as information espionage, terrorist attacks, etc.

In this thesis, a cyber security-based visitor control system has been designed in order to maximize participant security in institutions, to prevent unauthorized access, and to easily control participants.

The Visitor Control System has been developed using Raspberry Pi 3 and the information of the visitors who will participate is uploaded to the system along with their pictures. Within the scope of cyber security measures, the Visitor Entry Card, which is created with a QR code to prevent fake ID or entrance cards, is sent to the participants days before the dates of programs

such as meetings, seminars, interviews, symposiums, workshops, briefings, fairs, and they are requested to enter with these cards.

At the entrance points of the institutions, the visitors' Visitor Entry Card is questioned by the security guards and the QR code on the card is scanned with the help of the camera to confirm whether the visitor is authorized or not. After it is confirmed by the security personnel that it is exactly the same as the person's photo, it is allowed to enter.

Keywords: Raspberry Pi, QR Code, Visitor Control Systems, Cyber Security, Entry Systems in Institutions, Intrusion Prevention Systems.

KURUMLARDA SİBER GÜVENLİK TABANLI ZİYARETÇİ KONTROL SİSTEMİ TASARIMI VE UYGULAMASI

İÇİNDEKİLER

ÜÇÜNCÜ BÖLÜM

ZİYARETÇİ KONTROL SİSTEMİ TASARIMI VE UYGULAMASI

KISALTMALAR

CSI	Kamera Seri Arayüzü (Camera Serial Interface)
CPU	Merkezi İşlem Birimi (Central Process Unit)
GPIO	Genel Amaçlı Giriş/Çıkış (General purpose Input Output)
GPU	Grafik İşlemci Birimi (Graphics Processing Unit)
IoT	Nesnelerin İnterneti (Internet of Things)
LCD	Sıvı Kristal Ekran (Liquid Crystal Display)
NFC	Yakın Alan İletişimi (Near Field Communication)
OPTS	Otomatik Parmak İzi Tanıma Sistemi
PCB	Baskılı Devre Kartı (Printed Circuit Board)
OS	İşletim Sistemi (Operating System)
QR	Çabuk Tepki (Quick Response)
RAM	Rastgele Erişimli Bellek (Random Access Memory)
RFID	Radyo Frekansla Kimlik Tanımlama (Radio Frequency Identification)
s.	Sayfa
SBC	Tek Kart Bilgisayar (Single Board Computer)
SD	Güvenli Dijital (Secure Digital)
SDLC	Sistem Geliştirme Yaşam Döngüsü(Systems Development Life Cycle)
USB	Evrensel Seri Veriyolu (Universal Serial Bus)
VNC	Sanal Ağ üzerinden Bilgisayar Kontrolü(Virtual Network Computing)

ŞEKİLLER LİSTESİ

GİRİŞ

Bilim ve teknolojinin hızla gelişmesi ile bilgisayar teknolojileri hayatın birçok alanında vazgeçilmez hale gelmiştir. İnsan yaşantısını büyük oranda etkileyerek geleneksel fiziki olarak bir araya gelme alışkanlıkları neredeyse ortadan kalkmıştır. Dünyanın farklı yerlerinde birçok seminer, söyleşi, sempozyum, çalıştay, brifing ve fuar gibi bir araya gelme faaliyetleri yapılmaktadır. Gelişen teknoloji ile birlikte zamanın daha değerli hale gelmesi, salgın hastalıklar gibi nedenlerle fiziksel olarak katılımın ihtiyaç duyulduğu kurumlarda bu faaliyetler alternatif olarak çevrimiçi (online) gerçekleşmektedir.

Çevrimiçi katılımların yetersiz kaldığı fiziki katılımların zorunlu olduğu durumlarda katılımcı/ziyaretçi giriş kontrol sistemlerinin güvenirliliği son zamanlarda çok daha önemli bir kriter haline gelmiştir. Bunun sonucunda organizatörler icra ettikleri toplantı, fuar, seminer gibi organizasyonlarda katılımcıların güvenliğini artırmak maksadıyla yetkisiz katılımcıları engellemek üzere birçok farklı güvenlik önlemlerine başvurmaktadır. Bunlardan bazıları; güvenlik görevlisi, kimlik kontrol, parmak izi kontrol, giriş kartı, bilet gibi yetkisiz katılımları engelleyici önlemlerdir. Ancak bahsedilen güvenlik önlemleri daima içeriğinde bir güvenlik açığı barındırmaktadır. Örneğin; sahte bilet, sahte kimlik, sahte parmak izi gibi.

Kurumlar, siber saldırılara karşı sistemlerini korumak için siber güvenlik önlemleri almaktadırlar. Ancak, buna rağmen birçok kurum ziyaretçi kontrol süreçlerinde yetersizlikler yaşamaktadır. Ziyaretçi kontrolü, kurumun güvenlik bariyerini oluşturan ilk adımdır ve bu sürecin etkin bir şekilde yönetilmesi önemlidir. Geleneksel ziyaretçi kayıt sistemleri, güvenlik açıklarına neden olabilir ve ziyaretçi verilerinin kötü niyetli kişilerin eline geçmesi riskini artırabilir. Bu nedenle, kurumlar siber güvenlik tabanlı ziyaretçi kontrol sistemlerine ihtiyaç duymaktadırlar.

Buna karşın güvenlik personelinin katılımcıların açıkça üzerinde ne yazdığını bilmediği hızlı cevap (quickresponse) (QR) kod ile oluşturulmuş kişiye özel giriş kartları ekstra katılımcı güvenliği sağlamaktadır. QR kod 1994 yılında bir Japon firması tarafından geliştirilerek günümüze kadar ulaşmıştır. QR kodlar kolay kullanılabilirliğinin yanı sıra yüksek veri işleme yeteneğine sahiptirler. (Hampton,

Peach ve Rawlins,2011: 75; Dou ve Li, 2008: 62). Japonya'da ilk olarak otomotiv endüstrisinde kullanılmak üzere geliştirilmiştir. Siyah noktalar ve çizgilerden oluşan QR kodlar, bir mobil cihazın kamerasına okutulduğunda, internette yer alan veya bir serverda depolanmış dijital bilgi kaynağına doğrudan erişim sağlanabilmektedir (Chen vd., 2010: 202).

Bu tez kapsamında, kurumlarda katılımcı güvenliğinin en üst seviyeye çıkarabilmek ve yetkisiz girişleri önleyebilmek, katılımcıların kontrolünü kolaylıkla sağlanabilmesi için siber güvenlik tabanlı ziyaretçi kontrol sistemi tasarlanmıştır. Tasarlanan ziyaretçi kontrol sistemi, Raspberry Pi 3 donanımı ve programlama dili olarak Python kullanılarak geliştirilmiştir. Kurumlarda katılım yapacak olan ziyaretçilerin bilgileri resimleri ile sisteme yüklenmekte ziyaretçilere sadece kişiye özel olarak hazırlanmış QR koda sahip bir ziyaretçi giriş kartı verilmektedir. Ziyaretçiler/katılımcılar tarafından kurumlara girişte kendilerine verilen üzerinde giriş kartı sisteme okutulduğunda kişinin yetkili katılımcı olup olmadığı güvenlik görevlileri tarafından tespit edilebilmektedir. Güvenlik görevlisi ekranda kişinin fotoğrafından diğer tanımlayıcı kişisel bilgilerine kadar her şeyi kontrol ederek katılımcının geçişine izin vermektedir. QR kod teknolojisi ile hazırlanmış sahte giriş kartları ile giriş yapılmaya çalışıldığında ise ekranda yetkisiz giriş uyarısı ile herhangi bir fotoğraf görüntülenmediği için katılımcının girişine güvenlik personeli tarafından izin verilmeyecektir. Siber güvenlik tedbirleri kapsamında ise sistemin offline (çevrimdışı)olarak çalışması olası bir siber saldırı, sisteme sızma, sahte kimlik veya ziyaretçi bilgilerinin değiştirilmesi ya da sahte QR kod üretilmesi vb.durumların önlenebilmesi açısından avantaj sağlamaktadır.

BİRİNCİ BÖLÜM
LİTERATÜR ARAŞTIRMASI

1.1. GEÇİŞ KONTROL SİSTEMLERİ

Geçiş güvenliğine ihtiyaç duyulan her yerde birbirinden farklı teknolojilere sahip geçiş kontrol sistemleri kullanılmaktadır. Bu teknolojilerden şifre kullanımı, radyo frekansla kimlik tanımlama (FrequencyIdentification) (RFID) kart kullanımı, manyetik kart kullanımı ile biyometrik önlemler (parmak izi, iris tarayıcı, retina tarayıcı, ses tanıma, yüz algılama vb.) günümüzde çok sık kullanılmaktadır. Bunlarla birlikte son yıllarda kullanımı çok yaygın hale gelen QR kod sisteminde kullanılmaktadır. Ancak QR kod sistemi sadece kimlik doğrulama amaçlı değil internet adresi, stok sorgulama, banka hesap bilgileri paylaşımı, kartvizit yerine kullanım, adres tarifi, restoranlarda elektronik menü gösterimi vb. ihtiyaçlara da cevap verecek şekilde kullanılmaktadır. Bahsedilen bu teknolojilerin dünyada gün geçtikçe çok hızlı bir şekilde artış gösteren siber saldırılara karşı güvenirliliği daha önemli bir konu haline gelmektedir. Bu kapsamda hali hazırda dünyada kullanılan birbirinden farklı teknolojilere sahip geçiş kontrol sistemlerine yönelik literatür taraması gerçekleştirilmiştir.

Karaca (2010), anlık Personel Takip Sistemi geliştirmek için RFID sistemini kullanmıştır. Kullanılan RFID sistemi ile personelin giriş-çıkış saatlerinin ve güncel konum bilgilerini göz önünde bulundurularak, kısıtlı katılımcı ile gerçekleştirilen gizli toplanmalarda güvenliğin de önemi göz önünde bulundurulduğunda yetkisiz katılımların takip edilmesi ve müdahale edilmesi sağlanarak güvenlik seviyesinin arttırılması, güncel personel katılım listesi işlenerek kurumların/kuruluşların personel takibini kolaylıkla yapması hedeflenmiştir.

Mamak vd. (2020), işyerlerinde personelin mesai giriş ve çıkış işlemlerini hızlı, etkin ve doğru bir şekilde takip edilebilmesi amacıyla, yüz tanıma tabanlı personel kontrol ve takip sistemi tasarımı gerçekleştirilmiştir. Geliştirilen sistemde, işyerinin giriş ve çıkışlarına kamera sistemi kurularak personelin görüntüleri alınmıştır. Alınan görüntüler personelin yüz bölgeleri tespit edilip personel eşleştirilerek fisheryüz, özyüz ve yerel ikili örüntü histogramı yöntemleriyle

tanımlanan yüz bölgelerinin kime ait olduğu bulunmaktadır. Bulunan personele ait giriş-çıkış verileri ekranda verilerek personel şahsi veritabanına işlenerek arşivlenmesi sağlanmıştır.

Genli (2005) Kartlı geçiş sistemlerinde kart sahibinin bina içerisinde herhangi bir odaya ya da bölüme girmek istediğinde giriş yetkisi yoksa bu kart kullanımını sisteme alarm olarak rapor edecek ve odaya girişi yada turnikeden geçişi engelleyecek bir uygulama geliştirilmiştir. Eğer hiçbir giriş yetkisi yoksa sistemin direkt olarak alarm üretmesi sağlanmıştır.

MusayevaveYahyayev (2014), parmak izi tanıma teknolojisi ile ilgili olarak her insan elinin farklı deri yapısında olduğunu, parmak uçlarının derisinde girintili çıkıntılı kabartılar mevcut olduğunu ve bu kabartılı yapıların teması sonucu yüzeylerde bıraktığı izi parmak izi olarak tanımlamışlardır. İnsanlardaki parmak izinin benzersiz ve değişmeyen nitelikte biyometrik ölçülere sahip olduğunu belirtmişlerdir.

Özkaya ve Sağıroğlu (2014), kimlik doğrulamasında parmak izi teknolojisinin kullanımı çok eskilere dayandığı belirtilmiştir. Otomatik Parmak İzi Tanıma Sistemi (OPTS) geçmişi ise parmak izi mürekkebine dayanmaktadır. OPTS güvenli bir sistem olarak bilinse de art niyetli kişiler parmak kalıplarını kullanarak taklit etmeyi başarmış olduklarını belirtmişlerdir. Buna karşın taklit edilmiş bir parmak izi kalıbının parmağın canlı gerçek parmak olup olmamasını kontrol eden sistemler ile bu sorunu ortadan kaldırmanın mümkün olduğunu belirtmişlerdir. OPTS'nin parmak izini tanılama yaparken geçekleştirdiği işlemler:

-Alınan parmak izlerinin sayısal koda çevrilmesi

-Parmak izlerinde bilgi olan, önemli kısmın arka plandan ayrılması.

-Referans noktaların elde edilmesi

-Ortaya çıkan referans noktalarının ikili resme çevrilmesi.

-İkili resmin inceltilmesi,

-Özellik noktalarından parametrelerinin elde edilmesi.

-Yanlış özellik noktalarının çıkarılması.

-Karşılaştırma işleminin gerçekleştirilmesi.

Şamlı ve Yüksel (2009), parmak izi sistemlerinin en büyük dezavantajının bazı insanlarda uzuv eksikliği, yanma, cilt hastalıkları vb. durumlar mevcut olduğundan kullanılamaması olduğunu belirtmişlerdir.

Noma-Osaghae vd. (2017), biyometrik kimlik doğrulama sistemlerinin erişimi sınırlamak için benzersiz fizyolojik ve davranışsal özellikler kullandığını belirtmişlerdir. Bu genellikle bireyin benzersiz fiziksel özelliğinin bir görüntüsünü elde etmeyi ve bunu bir veritabanında önceden depolanmış şablonlarla karşılaştırmayı içerir. Birden fazla olan yüz, parmak izi, ses, iris vb. biyometrik kimlik doğrulama sistemlerinden iris tanıma sistemi insanda bireysel tanımlama için kullanılabilecek en güvenilir sistemlerden biridir. İris, gözbebeği ve sklera ile çevrilidir. Bireysel tanımlama için kullanılabilecek en güvenilir fiziksel özelliklerden biridir. İrisin kararlı, değişmez ve benzersiz doğası, kendi özel sınıfındadır. Diğerlerine kıyasla daha kararlı bir biyometrik özelliktir. İris o kadar benzersizdir ki aynı kişinin (hatta ikizlerin bile) sağında ve solunda farklıdır. İris tanıma sisteminin çalışma prensibini ise şu şekilde açıklamışlardır: Sisteme bir kişi tanımlandıktan sonra, kullanıcıya erişim izni verilir. Tanımlama, bir tanımlama aracı olarak kullanıcının irisinin sağlanmasını gerektiren bire çok eşleşme anlamına gelir. Kamera yardımıyla sağlanan iris örneği, veritabanında önceden saklanan iris örneklerinin bilgileriyle karşılaştırılır. Kayıtlı iris modeliyle bir eşleşme varsa, erişime izin verilir ve kapı açılır. Aksi takdirde, erişim reddedilir. Ancak bahsedilen bu iris tanıma sisteminin uzaktan tanımlama yeteneği bulunmamaktadır. Tanımlama yapılacak her bireyin sistemin kamerasına doğru bir şekilde bakarak iris özelliklerinin kaydedilmesi gerekir.

Wahyudi ve Syazilawati (2007), güvenli binaların çeşitli cihazlar tarafından yetkisiz erişime karşı korunmakta olduğunu belirtmişlerdir. Sistem güvenliğini garanti etmek için PIN kodları hem geleneksel hem de elektronik anahtarlar, kimlik kartları, kriptografik ve ikili kontrol prosedürleri gibi birçok türde cihaz olmasına rağmen, insan sesinin de kullanılabilir olduğunu açıklamışlardır. Konuşmayı veya konuşmacı doğrulamayı analiz ederek bir konuşmacının kimliğini doğrulama yeteneği, önemli veya güvenli bir yere giriş için güvenlik sağlamanın çekici ve nispeten göze çarpmayan bir yolu olduğunu, bir kişinin sesi çalınamaz, kaybolamaz, unutulamaz, tahmin edilemez veya tam olarak taklit edilemez olduğunu öne

sürmüşlerdir. Bu avantajlar nedeniyle bina güvenliği için ses tabanlı bir kapı erişim kontrol sisteminin tasarlamışlardır. Önerdikleri sistemde, sisteme bağlı bir mikrofona konuşan kayıtlı bir kullanıcı aracılığıyla erişim yetkilendirilebilir. Veritabanına bir mikrofon yardımıyla yetkilendirilecek kişilerin sesleri kaydedilir. Kaydedilen seslerden kişiye özel ses öznitelikleri çıkarılır. Ardından erişim yapmak isteyen kullanıcıdan sistem bir giriş kodu ya da kimlik numarası tuşlaması talep edilir. Ardından sistem kişiden konuşmasını talep eder ve örnek bir cümle söylemesini ister; örneğin, adınız ve soyadınız gibi. Sonrasında kapıdaki mikrofon yardımıyla istenen ses cümlesi veritabanındaki seslerle karşılaştırılır. Sistemin sesten çıkarılan özelliğin talep edilen kişinin ses modeliyle eşleşip eşleşmediğine karar verdiği bir süreç vardır. Kesin bir erişim kabulü veya reddi yanıtı vermek için bir eşik belirlenir. Belirli bir ses ile model arasındaki benzerlik derecesi eşikten büyük olduğunda, giriş onaylanır ve kapı açılır. Eğer kişi tarafından söylenen ses, giriş kodu ya da kimlik numarasıyla eşleşmiyorsa girişinin reddedildiği tespit edilmiştir.

1.2. SİBER GÜVENLİK VE GÖMÜLÜ BİLGİSAYAR

Aslay (2017), dünyada bilişim teknolojilerinin hızla gelişmesine bağlı olarak bilgisayar ve internet kullanımının hayatın vazgeçilmez bir unsuru haline geldiği belirtilmiştir. Ancak internetin dünya genelinde çok hızlı yaygınlaşması kullanıcılara büyük kolaylıklar ve özgürlükler sağlarken bununla birlikte ortaya çıkan güvenlik açıkları sebebiyle de sistemlerin kötüye kullanılmasına sebebiyet verdiği belirtmişlerdir. Bu güvenlik açıkları kişileri veya büyük sistemleri hedef alabilmektedir. Cihazların birbirleriyle iletişime geçmesi yani Nesnelerin İnterneti (Internet of Things, IoT) ile internete bağlı olan cihazların sayısında tahmin edilemeyecek kadar artış olması siber güvenlik problemlerini de beraberinde getirecektir.

Siber kavramı, bilgisayar ve ağlarını içeren kavram veya varlıkları tanımlamak için kullanılmaktadır. Siber uzay (cyber space) kelimesi de birbiriyle bağlantılı donanım, yazılım, sistemler ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır. Siber Saldırı kavramı ise “hedef seçilen kişi, şirket, kurum ve devlet gibi yapıların bilişim

sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar" şeklinde tanımlanmıştır.

Gelişen teknoloji ile birlikte gömülü bilgisayarlar başka bir deyişle gömülü sistemler günümüzde yaşamın birçok alanında kullanılmaktadır. Gömülü bilgisayarlar; mobil cihazlarda, araçlarda, banka atmlerinde, televizyonlarda, beyaz eşyalarda, oyuncaklarda, yazıcılarda, akıllı ev sistemlerinde, fabrikalarda, işyerlerinde, güvenlik noktalarında vb. daha birçok yerde her ihtiyaca hizmet verecek şekilde yapılandırılmakta ve kullanılmaktadır.

Türk ve Lüy (2021) Gömülü sistemleri, bağımsız veya daha büyük bir sistemin parçası olarak belirli bir görevi icra eden aynı zamanda kendine özel yazılıma sahip mikroişlemci tabanlı bilgisayar donanım sistemleri olduğunu belirtmişlerdir. Gömülü bilgisayarlar; GPU (Graphics Processing Unit) teknolojisi, dijital sinyal işlemcileri, mikro denetleyiciler veya uygulamaya özel bütünleşmiş devreler, vb. sistemler üzerinde kullanılmaktadır.

Gömülü bilgisayarlarda kullanılan program dizeleri sistemin yazılım mimarisini oluşturmaktadır. Basit bir endüstriyel mikrodenetleyici belirli görevleri yerine getirmek üzere tasarlandığı için güç tüketimi, boyut, güvenilirlik ve performansı ayarlamak son derece önemlidir. Bu temel cihazlar CPU(Central Process Unit)'nun makine kodu vasıtasıyla programlanır. Yazılımları C, C++, Java veya benzeri programlama dilleri ile gerçekleştirilir. Gömülü bilgisayarlar çoğu zaman, gerçek zamanlı işletim ortamları ile birlikte, gömülü kullanıma uygun ara yüz veya dil platformlarını kullanmaktadırlar. Bunlara örnek olarak Linux, Windows IoT ve Embedded Java gösterilebilir.

Bununla birlikte gömülü bilgisayarlara veya başka bir deyişle programlanabilir basit bilgisayarlara örnek vermek gerekirse; Arduino veya Raspberry Pi örnek verilebilir.

Arduino basit ve kolay entegre, kodlama dili ile en düşük seviyeden mühendislik seviyesine kadar birçok kullanıcıya hitap eden geliştirme kartı çeşididir. Arduino aynı zamanda açık kaynak kodlu yazılım ve donanıma sahip bir mikrodenetleyici platformudur; örneğin Arduino kullanarak sensörlerden gelen verileri okuyabilir ve bu verilere göre elektronik sistemleri kontrol edebilir ya da ışıkları yakıp söndürebilir ya da motoru çalıştırabilir.

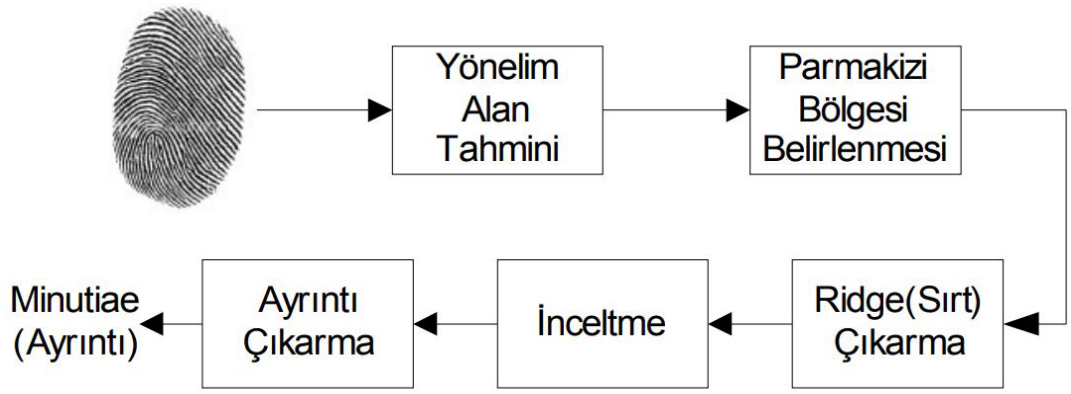
Raspberry Pi ise bir monitöre, televizyona veya kendine özel ekrana takılabilen, standart bir klavye ve fare kullanan, düşük maliyetli kredi kartı boyutunda küçük bir bilgisayardır. Arduino sistemine benzerlik göstermekle birlikte her seviyeden kullanıcıya hitap eden Scratch ve Python gibi dillerde programlamayı öğrenmesini sağlayan bir platformdur. Raspberry Pi üzerinde barındırdığı mikroişlemci, RAM (Random Access Memory), GPIO (General purpose Input Output) pinleri ve bir bilgisayar için gerekli tüm özelliklere sahip olan tek bir devre kartı PCB (Printed Circuit Board) üzerinde oluşturulmuştur. Bu tip bilgisayarlar Tek Kart Bilgisayar yani SBC (Single Board Computer) olarak da adlandırılır. Günlük hayatta kullandığımız bilgisayarlardan farklı olarak SBC'ler daha az güç tüketirler ve daha küçük boyuta sahiptirler. Raspberry Pi normal bir bilgisayarın yapabildiği çoğu görevi yerine getirmekle birlikte üzerinde bulunan GPIO pinleri sayesinde de birçok farklı elektronik sistemi programlayarak kontrol edebilme yeteneğine sahiptir.

İKİNCİ BÖLÜM
KURUMLARDAKİ MEVCUT GEÇİŞ KONTROL SİSTEMLERİ

2.1. PARMAK İZİ TEKNOLOJİSİ GEÇİŞ SİSTEMİ

Günümüzde maliyet göz önünde bulundurulduğunda farklı alanlarda farklı giriş sistemleri ile ilgili uygulamalar bulunabilir. İşletmeler ve bireysel önlemler, teknolojik birçok giriş yöntemi kullanarak geleneksel sistemlere kıyasla daha hızlı ve daha etkin giriş-çıkış kontrolü sağlamaktadır. Birçok güvenlik kontrol sistemleri başarılı bir şekilde kullanılmaktadır. Bunlardan yaygın olarak kullanılanlardan biri de parmak izi tabanlı güvenlik kontrol sistemidir. Parmak izi teknolojisinin güvenlik maksatlı giriş-çıkış sistemlerinde temelde anahtar olarak kullanılması parmak izinin spesifik özelliğe sahip olmasındandır. Bu özellik sayesinde maksimum güvenlik sağlanabilir. Parmak izinin giriş-çıkış sistemlerinde kontrol aracı olarak Minutiae (Ayrıntı) Eşleştirme Algoritması ile kullanılması işlemi Şekil 1'de verilmiştir. (Merkepçi, 2009:1; Pehlivanoğlu, 2017:1; Boydak, 2017:2).

Şekil 1. Minutiae (Ayrıntı) Eşleştirme Algoritması



Kaynak: (Merkepçi &Özyazıcı, 2009).

Parmak izi tanıma sistemlerinin çalışması için özel bir yazılıma gerek vardır. Parmak izi tanıma algoritmaları, bu yazılımın temelini oluşturur. Algoritmalar kullandığımız tüm yazılıma dayanan cihazların temelini oluşturur. Personel parmak

izi okuyucu sistemlerinde donanım ve yazılım bir arada çalışır. Parmak izi okuma cihazı, parmağı tarayarak parmak izini tespit eder. Daha sonra algoritma yani yazılım tarafı parmak izini eşleştirmek için devreye girer. Parmak izi eşleştiğinde giriş onaylanır ve kilit açılır. Başka bir şekilde açıklamak gerekirse parmak izi taranır. Bu tarama işlemi aslında fotoğraf çekme işlemidir. Kamera ve optik, cihaza yerleştirilen parmağın fotoğrafını çeker. Süreç elektronik olarak tamamlanır. Parmak izi algoritmaları, elde edilen bu fotoğrafı özel bir sayısal modele dönüştürür. İzde bulunan girintiler ve çıkıntılar, sayısal modelin oluşturulmasında kullanılır. Elde edilen sayısal model, bilgisayarda bulunan veri tabanı ile karşılaştırılır. Veri tabanında eşleşme olması durumunda parmak izi doğrulama işlemi gerçekleşmiş olur. Bu süreç hem personel takip sistemi hem de kapı kilidi açma sistemi gibi farklı alanlarda uygulanabilir.

Şekil 2. Parmak İzi Okuyucu Geçiş Sistemi

Kaynak: (geciskontrolmerkezi.com, 2023).

Şekil 2'de gösterildiği üzere parmak izi teknolojisine sahip geçiş sistemleri sayesinde şifre veya kart paylaşımı yöntemi kullanılarak yetkisiz geçişlerin engellenmesi sağlanmıştır. Buna karşın geçiş yetkisine sahip kişilerin sahte parmak izleri çeşitli teknikler kullanılarak yapılabilir. Bu sayede yetkisi olmayan kişilerinde geçişi gerçekleşebilir.

2.2. KARTLI GEÇİŞ SİSTEMİ

Kartlı geçiş sistemleri; kişilere verilen kart ve bu kartların sisteme okutularak kişilerin, çalışanların, ziyaretçilerin ya da otoparka giriş sağlayan araçların giriş-çıkış saatlerini kayıt altına alan turnike, kapı ya da bariyerlerin açılıp kapanmasını sağlayan sistemlerdir. Kartlı geçiş kontrol sistemleri personel takip yapmak amacı ile de sıklıkla tercih edilen kontrol sistemlerindendir. Bu sistemler access kontrol sistemi, erişim kontrol sistemi ve geçiş kontrol sistemi olarak da adlandırılmaktadır.

Baykara ve Sherzad (2020), RFID Kartlı Giriş Sistemleri, bir yere ana kapıdan girmek isteyen kişiler veya ziyaretçiler için bilgi ve erişimi yönetmek için kullanılan bir tekniği tanımlamışlardır. Buna göre geliştirdikleri sistem herhangi bir eve erişim sağlamadan önce girişi kontrol etmek için güvenli bir alandaki sakinlerin veya ziyaretçilerin hareketlerine ilişkin bilgileri korumak için bir veri tabanına bağlı bir web uygulaması olarak tasarlanmıştır. Bina sakinleri için bir güvenlik önlemi sağlar ve yetkisiz erişim riskini en aza indirmeye, güvenliği artırmaya, hırsızlık ve kazaları azaltmaya ve hassas bilgileri güvence altına almaya yardımcı olabileceğini bildirmişlerdir.

Kartlı geçiş kontrol sistemleri personel takip sistemlerinin atası olarak kabul edilmektedir. Şekil 3'te gösterilen kartlı geçiş sistemleri sayesinde kurumlarda veya işletmelerde personeli kontrol altında tutmak, giriş çıkış saatlerini kayıt altına almak ve işletmelerde belirli alanlara sadece yetkilendirilmiş kişilerin erişmesini sağlamak ve onların dışındaki herkesin giriş yapmasını engellemek için kullanılan sistemlerdir.

Kartlı geçiş kontrol sistemleri oldukça pratik, kullanışlı ve düşük maliyetlidir. Ayrıca kartlı geçiş sistemlerinin yetkilendirme özelliği sayesinde belirli kişilerin izin verilen alanlardan güvenli bir şekilde geçmesi sağlanmaktadır.

Ancak kartlı geçiş sistemlerinin en büyük dezavantajı belir bir bölge veya alana geçiş için yetkilendirilmiş olan kişilerin kartları istemli yada istemsiz olarak başka kişiler tarafından kullanılması sonucunda yetkisiz girişlerin yapılması güvenlik zafiyeti oluşturmaktadır (komsek.com.tr, 2023).

Şekil 3. Kartlı Geçiş Sistemleri


Kaynak: (karel.com.tr, 2023).

2.3. ŞİFRELİ GEÇİŞ SİSTEMİ

Şifreli geçiş sistemleri, turnikelerin, kapıların şifre yardımı ile açılmasına imkân tanıyan sistemlerdir. Şekil 4'te gösterilen piyasada yüzlerce farklı modeli olan şifreli geçiş sistemleri genellikle bina girişlerinde, ofis odalarında, hastanelerde, özellikle ameliyat ve yoğun bakım ünitelerinin girişlerinde, asansörlerde, depolarda vb. yerlerde kullanılmaktadır. Şifreli geçiş sistemleri çalışma prensibi olarak geçiş yapmak isteyen kullanıcının doğru şifreyi bilmesi prensibine dayanmaktadır. Kullanıcı doğru şifreyi tuşladığında sistem kendi elektronik devresi üzerinde kilit sistemindeki devreyi tamamlar kapı içerisinde bulunan kilit sistemine voltaj anlık olarak gönderilir ve kapı kilidi açılmaktadır (perkotek.com, 2023).

Kolekar vd. (2022), şifre tabanlı kapı giriş sistemlerini 8051 mikrodenetleyici kullanılarak tasarlamıştır. Sistemin bir tuş panelinden tuşlanan rakamların daha önceden 2 Kilobyte kapasiteli hafızasına kaydedilen şifreyle eşleşmesi prensibi ile çalıştığını belirtmişlerdir. Şifrenin doğru girilmesi sonucunda mikrodenetleyiciye bağlı olan motor arabiriminin devreye girmesi ile motorun ileri veya geri döndürülmesiyle kapı kilidinin açılması veya kapanmasını sağlamışlardır.

Şifreli geçiş sistemlerinde gelişen teknoloji ile şifre girişi buton yerine dokunmatik tuşlar ya da panel olarak da günümüzde kullanılmaktadır. Ayrıca dokunmatik şifreli geçiş sistemlerinde manyetik kart ile de geçiş sağlamak mümkündür.

Ancak bu sistemin en büyük dezavantajı şifrenin ifşa olması durumunda yani şifrenin yetkili olmayan birisine verilmesi ya da yetkili birinin şifreyi tuşlarken arkadan izleyerek öğrenmesi güvenlik zafiyetini oluşturacaktır.

Bununla birlikte elektronik teknik bilgisi iyi olan bir hırsız veya art niyetli birisi, şifre paneli çok güvenli bir şekilde montaj edilmediyse eğer paneli kolaylıkla sökebilir. Şifreyi bilmese dahi güç kaynağından gelen kabloyu kapı kilidine giden kabloları kısa devre yapacak şekilde bağlayarak kapıyı kolaylıkla açabilir.

Şekil 4. Şifreli Geçiş Sistemi

Kaynak: (asyakapisistemleri.com.tr, 2023).

2.4. BARKODLU GEÇİŞ SİSTEMİ

Teknolojinin çok hızlı bir şekilde geliştiği dünyamızda gündelik hayatta kullandığımız emniyet amaçlı kilit ve geçiş sistemleri de birçok değişikliğe maruz kalmıştır. Kartlı geçiş sistemleri gündelik hayatımızda her alanında kullanılmaktadır. Hali hazırda kamu kurumları, otobüsler, üniversiteler, hastaneler, yemekhaneler, eğlence merkezleri, oteller vb. birçok yerde kartlı geçiş sistemi teknolojisi kullanılmaktadır.

San Hlaing ve San Lwin (2019) kartlı geçiş sistemlerinin kilit ve anahtara gerek olmadan RFID kapı kilit mekanizmalarının üzerine bir miktar voltaj elektrik uygulandığında girişe izin veren sistemler olduğunu belirtmişlerdir.

Bu teknoloji hem geçmişte hem de günümüzde uygun fiyatlı aynı zamanda kullanıcılar için güvenilir bir çözüm olarak bilinmektedir. Fakat geçmiş yıllarda tüm dünyayı etkisi altına alan pandemi salgını bize kullanımı alışılagelmiş kartlara alternatif sistemler kullanmaya mecbur bırakmıştır. Bu sebeplerle son zamanlarda toplu alanlarda fiziksel temasın en aza indirgenebilmesi için özellikle geçiş kontrol noktalarında hem güvenli hem de temas gerektirmeyen çözümler daha çok tercih edilmektedir.

Teknolojinin gelişmesi ile RFID kartları okuyan aynı zamanda QR kodu veya barkodunu da tarayabilen geçiş sistemleri pazarında yerini almaya başlamıştır. Bazı güvenlik teknolojileri şirketleri mevcut kartlı geçiş sistemlerine sahip kamu kurumları, binalar, işletmeler vb. yerlerde mevcut alt yapısal sistemlerine zarar vermeden Şekil 5'te gösterilen QR veya barkod teknolojisine sahip geçiş sistemlerine dönüşümünü gerçekleştirmektedirler.

Şekil 5. Barkodlu Geçiş Sistemi

Kaynak: (barfas.com, 2023).

Ancak bu sistemler kartlı geçiş sistemlerinde olduğu gibi QR veya barkod teknolojisine sahip kartlarında olduğu gibi istemli ya da istemsiz olarak gerçek

sahipleri dışında kullanılması sonucunda yetkisiz geçişlerin yapılması buda söz konusu kurum ve işletmeler için güvenlik zafiyeti oluşturmaktadır. (barfas.com, 2023).

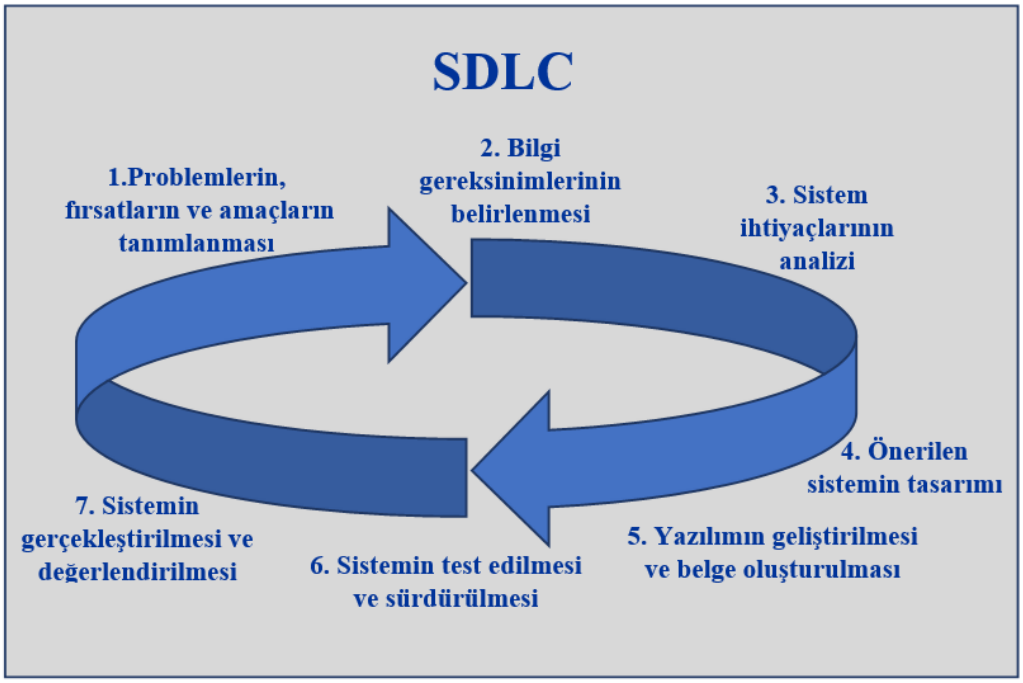
ÜÇÜNCÜ BÖLÜM
ZİYARETÇİ KONTROL SİSTEMİ TASARIMI VE UYGULAMASI

Ziyaretçi kontrol sistemi tasarımı ve uygulanması bölümünde ilk olarak Sistem Geliştirme Yaşam Döngüsü konusu ele alınacaktır. Bu kapsamda Sistem Geliştirme Yaşam Döngüsü adımları ayrıntılandırılacaktır. Üçüncü Bölüm'de aktarılacak diğer konu Ziyaretçi Kontrol Sistemi Tasarımı ve Uygulamasıdır. Uygulamanın donanımsal ve yazılımsal gereksinimleri ile ilgili detaylar anlatılmıştır.

3.1. SİSTEM GELİŞTİRME YAŞAM DÖNGÜSÜ (SDLC)

Ziyaretçi Kontrol Sistemi tasarım geliştirme sürecinde Şekil 6'da gösterilen SDLC (Systems Development Life Cycle)olarak adlandırılan Sistem Geliştirme Yaşam Döngüsü (SGYD) adımları izlenmiştir (Dönerçark ve Tecim, 2020: 93).

Şekil 6. Sistem Geliştirme Yaşam Döngüsü (SGYD)



Kaynak: (Dönerçark ve Tecim, Sistem Geliştirme Yaşam Döngüsü, 2020).

Sistem Geliştirme Yaşam Döngüsünde toplamda yedi süreçten oluşmaktadır. SGYD bulunan bu süreçler sırasıyla;

1. Problemlerin, Fırsatların ve Amaçların Tanımlanması,
2. Bilgi Gereksinimlerinin Belirlenmesi,
3. Sistem İhtiyaçlarının Analizi,
4. Önerilen Sistemin Tasarımı,
5. Yazılımın Geliştirilmesi ve Belge Oluşturulması,
6. Sistemin Test Edilmesi ve Sürdürülmesi,
7. Sistemin Gerçekleştirilmesi ve Değerlendirilmesi, olarak tanımlanmıştır.

3.1.1. Problemlerin, Fırsatların ve Amaçların Tanımlanması

Kurumlarda katılımcı/ziyaretçi giriş kontrol sistemlerinin güvenirliliği hızla gelişen teknoloji ile çok önemli bir problem haline gelmiştir. Geleneksel ziyaretçi kontrol sistemleri uygulandığında; art niyetli davranışlar sergileyen kimselerin bazı durumlarda sahte kimlik, sahte bilet, başkasına ait manyetik kart, paylaşılan şifre vb. birçok farklı yöntemlerle kayıtlı ya da yetkisi olmayan katılımcıların, ziyaretçilerin giriş yapabildiği bilinmektedir. Bu durum ise kurumlarda güvenlik açığına sebebiyet vermektedir.

Günümüzde dünyadaki tüm bilgi sistemleri hedef alan siber saldırıların katılımcı/ziyaretçi giriş kontrol sistemlerine de zarar verebildiği bilinmektedir. Söz konusu siber saldırıların kurumlardaki giriş kontrol sistemlerine etki etmesi durumda katılımcı/ziyaretçi bilgileri değiştirilebilmekte kayıtlı olmayan kişilerinde girişine izin verilmektedir. Toplantı, fuar, seminer, söyleşi, sempozyum, çalıştay, fuar vb. organizasyonların düzenlendiği bina girişlerinde bulunan güvenlik görevlilerinin dünyanın farklı yerlerinden gelen katılımcıları daha önce hiç görmedikleri ve tanımadıkları için gerçek yetkili katılımcı olup olmadıkları konusunda hata yapabilme olasılığı bulunmaktadır.

Tez kapsamında yapılan çalışmada ise bu sorunların önüne geçilmesi amacıyla Ziyaretçi Kontrol Sistemi geliştirilmesi amaçlanmıştır. Ziyaretçi Kontrol Sistemi ile katılım yapacak olan ziyaretçilerin bilgileri günler öncesinden resimleri ile sisteme yüklenmesi amaçlanmıştır. Bununla birlikte katılımcı/ziyaretçilere

toplantı, seminer, söyleşi, sempozyum, çalıştay, brifing, fuar vb. programların tarihlerinden günler öncesinde siber güvenlik önlemleri kapsamında sahte kimlik veya giriş kartlarını engellemek üzere QR kod ile oluşturulmuş üzerlerinde isimlerinin bulunduğu Ziyaretçi Giriş Kartı ulaştırılarak bu kartlarla giriş yapması amaçlanmıştır.

Bu sayede kurumlarda giriş noktalarında güvenlik görevlileri tarafından Ziyaretçi Kontrol Sistemi ile katılımcıların Ziyaretçi Giriş Kartı sorgulanmakta ve kamera yardımıyla kart üzerindeki QR kodu okutularak ziyaretçin yetkili/kayıtlı kullanıcı olup olmadığı teyit edilmesi hedeflenmiştir. Güvenlik personeli tarafından sistemden kişinin fotoğrafı ile birebir aynı olduğu teyit edildikten yani çifte kontrol yapıldıktan sonra girişine müsaade edilebilmesi amaçlanmıştır.

3.1.2. Bilgi Gereksinimlerinin Belirlenmesi

Ziyaretçi Kontrol Sistemi tasarlanırken hali hazırda kurumlarda kullanılan geçiş kontrol sistemleri incelenmiştir. Bu sistemlerin çalışma prensipleri, tasarımları ve güvenlik zafiyetleri ayrıntılı olarak tespit edilmiştir. Bu sistemlerden ilk olarak incelenen şifreli geçiş sistemleridir. Şifreli geçiş sistemleri belirli bir sayıda rakamın doğru bir şekilde sırayla tuşlanmasıyla geçişe izin veren sistemlerdir. Ancak güvenlik açısından çok uygun bir sistem değildir. Çünkü şifreyi bilen ya da ele geçiren herhangi bir kişinin geçiş yapması çok kolaydır.Düşük maliyetli olmakla birlikte genellikle apartman, bina, kurum içi kapılarda, okullarda, hastanelerde vb. yerlerin girişlerinde kullanılmaktadır.

Kartlı geçiş sistemleri incelendiğinde ise karta sahip olan kişilerin sisteme RFID özellikli kartı yakınlaştırdığında kapının ya da geçiş turnikesinin açılması prensibine dayalı bir sistemdir. Ancak bu sistemin en büyük zafiyeti ise kartın bir başkasına verilmesi ya da kaybedilmesi çalınması durumunda yetkisi olmayan birisinin kartı sisteme okutarak geçiş yapmasına olanak tanımasıdır. Kartlı geçiş sistemi de tıpkı şifreli geçiş sisteminde olduğu gibi apartman, bina, kurum içi kapılarda, okullarda, hastanelerde vb. yerlerin girişlerinde kullanılmaktadır.

Parmak izi Okuyucu geçiş sistemlerinde ise bahsedilen şifreli ve kartlı geçiş sistemlerine göre güvenirlilik açısından bir adım daha öndedir. Kişilerin daha

önceden fiziki olarak parmaklarını sisteme tanıtması ve daha sonra geçiş yapmak istemeleri durumda sisteme parmak izlerini okutması ardından kapı ya da turnikenin açılması prensibine dayalıdır. Şifreli veya kartlı geçiş sistemlerine göre güvenirlilik açısından daha iyi olmasına rağmen geçiş yetkisine sahip kişilerin sahte parmak izleri çeşitli teknikler kullanılarak taklit edilebilir. Bununla birlikte yetkisi olmayan kişilerin geçişi gerçekleşebilir.

Barkodlu geçiş sistemleri ise katılımcı/ziyaretçiye verilen bilet yada kartın sisteme okutulması suretiyle geçiş yapılmasına olanak sağlar. Ancak bu sistem tek başına kullanıldığında kartlı geçiş sistemlerinde olduğu gibi biletin başkasına verilmesi ya da kaybedilmesi durumunda yetkisi olmayan kişilerin geçiş yapmasına olanak sağlamakta güvenlik zafiyeti oluşturmaktadır.

Ziyaretçi Kontrol Sistemi tasarlanırken bahsedilen geçiş kontrol sistemlerinin güvenlik zafiyetleri incelenmiş olup buna zafiyetleri ortadan kaldırabilecek bir sistem geliştirmiştir. Sistemin bilgi gereksinimleri kapsamında katılımcı ya da ziyaretçilerin gerçek fotoğraflarının sisteme günler öncesinden yüklenmesi için kişilerin fotoğraf ve kimlik bilgilerine ihtiyaç duyulmaktadır. Kişilerin verdiği fotoğraflar ve bilgiler çerçevesinde katılımcı veya ziyaretçiye üzerinde sadece QR kod ve ziyaretçi isminden başka bir şey bulunmayan Ziyaretçi Giriş Kartı hazırlanmaktadır. Ziyaretçi Giriş kartı sisteme okutulduğunda ise güvenlik görevlisi tarafından gelen katılımcı/ziyaretçi sistemde çıkan fotoğraf kontrol edilmekte eğer sistemde görüntülenen fotoğrafla katılımcı/ziyaretçi eşleşiyor ise geçişine izin verilmekte aksi halde reddedilmektedir. Bu sayede yaşanabilecek güvenlik zafiyetlerinin önüne geçilebilmektedir.

3.1.3. Sistem İhtiyaçlarının Analizi

Ziyaretçi Kontrol Sistemi tasarlanırken sistemin ihtiyaç duyduğu donanım ve yazılımlar geleneksel geçiş kontrol sistemlerine göre farklılık göstermektedir. Piyasada fazlaca bulunan geleneksel geçiş kontrol sistemlerinde genellikle sabit kartlar ve gömülü yazılımlar bulunmaktadır. Ancak Ziyaretçi Kontrol Sistemi tasarımda bir bilgisayarla aynı işlevi gören ancak hacim ve boyut olarak çok küçük olan Raspberry Pi, Raspberry Pi LCD Dokunmatik Ekran, Raspberry Pi Kamera, güç

Kaynağı ve yazılım olarak ise Python programlama dili kullanılması planlanmıştır. Raspberry Pi kullanılmasının planlanmasındaki amaç maliyetinin diğer bilgisayar kontrollü ya da gömülü sistemlere göre boyut olarak çok daha küçük olması ve maliyetinin diğerlerine göre az olması olarak değerlendirilebilir.

3.1.4. Önerilen Sistemin Tasarımı

Sistem Geliştirme Yaşam Döngüsünün (SGYD)'nin dördüncü süreci olan Önerilen Sistemin Tasarımın sürecinde Ziyaretçi Kontrol Sistemini oluşturan ekran, kamera vb. donanım parçalarının montajından kullanılacak olan işletim sisteminin belirlenmesi sağlanmıştır. Ziyaretçi Kontrol Sistemi Uygulaması Raspberry Pi işletim sistemi üzerinde Python programlama dili ve uygulama için gerekli kütüphaneler kullanılarak geliştirilmesi planlanmıştır.

3.1.5. Yazılımın Geliştirilmesi ve Belge Oluşturulması

Ziyaretçi Kontrol Sistemi uygulaması geliştirilirken Python programlama dili kullanılmıştır. Tasarımda kullanılacak olan kodların ve fonksiyonların sorunsuz çalışabilmesi için gerekli olan kütüphanelerin yüklenmesi gerekmektedir. Ziyaretçi Kontrol Sistemini uygulamasına ilişkin kodlar detaylı olarak "*3.9.Raspberry Pi Üzerinde Uygulama Kodlarının Gösterilmesi"* başlığı altında kodların ne işe yaradığının açıklamalarıyla birlikte anlatılmıştır.

3.1.6 Sistemin Test Edilmesi ve Sürdürülmesi

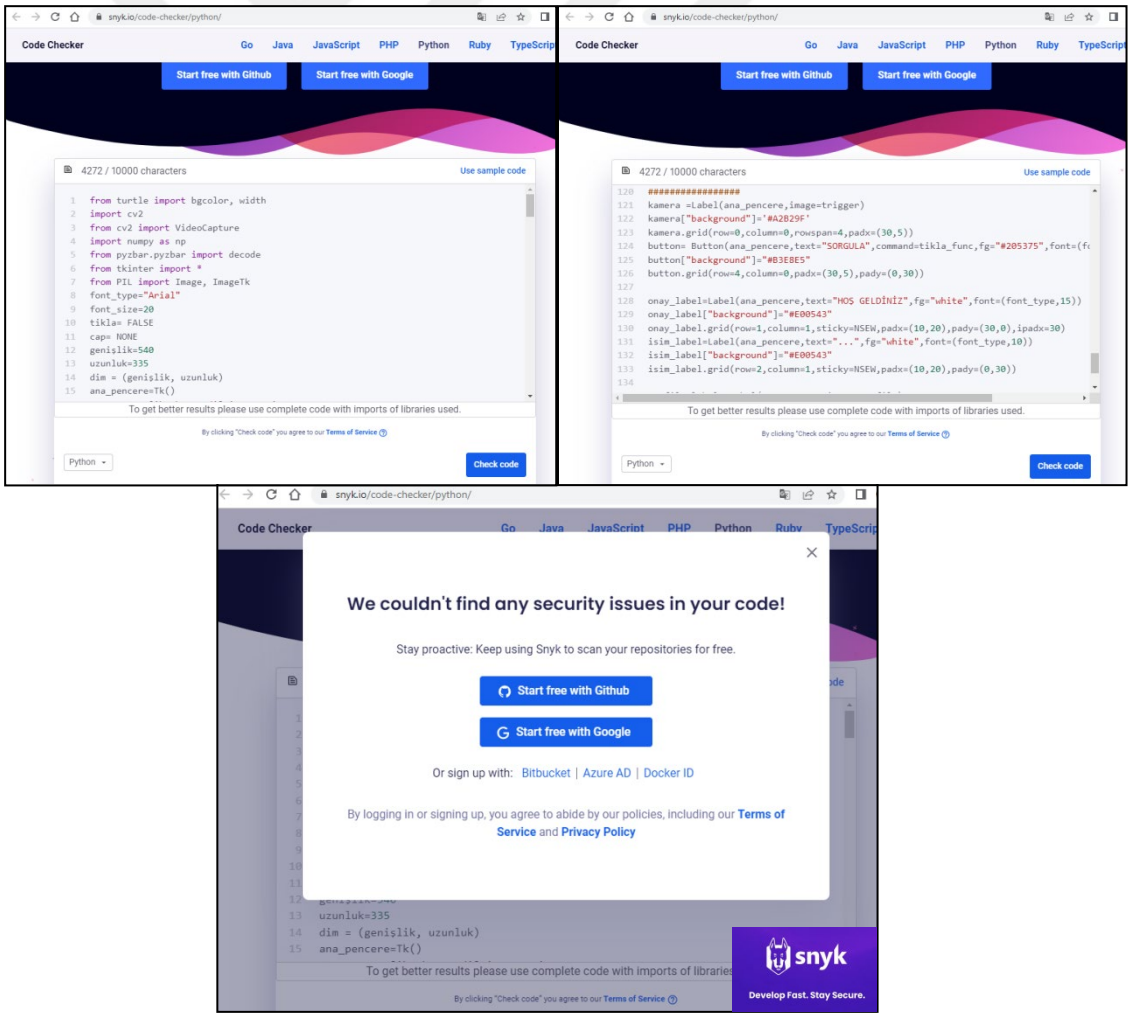
Ziyaretçi Kontrol Sistemi uygulamasının yazılımın geliştirilmesi süreci de tamamlandıktan sonraki süreçte sistemin testi gerçekleştirilmiştir. Ziyaretçi Kontrol Sistemini testine ilişkin detaylı olarak "*3.11.Ziyaretçi Kontrol Sistemi Uygulamasının Çalıştırılması"* başlığı altında anlatılmıştır.

Sistemin testi gerçekleştirilirken sisteme örnek olarak birkaç ziyaretçi fotoğrafları ve kimlik bilgileri yüklenmiştir. Sonrasında ise üzerinde QR kod ve katılımcı/ziyaretçi bilgileri bulunan Ziyaretçi Giriş Kartı sisteme okutulmuştur.

Sistem tarafından okunan QR kod tarafından bilgiler kontrol edilmiştir. Sorgulama sonucunda katılımcı/ziyaretçi eğer kayıtlı ya da yetkili ise fotoğrafı ile birlikte güvenlik görevlisine görüntülenmiş olup geçişi onaylanmıştır. Eğer sorgulama sonucunda QR kod kayıtlı ya da yetkili değilse girişi onaylanmayarak geçişi engellenmiştir. Ziyaretçi Kontrol Sistemini testine ilişkin onaylama ve reddetme durumlarına ilişkin olarak "*3.12.Ziyaretçi Kontrol Sistemi Uygulamasının Ekran Alıntıları*" başlığı altında gösterilmiştir.

Ziyaretçi Kontrol Sistemi uygulaması geliştirilirken python programlama dili kullanılmış olup kodların testi *https://snyk.io/code-checker/python/* web sitesi üzerinden çevrimiçi olarak gerçekleştirilmiştir. Test ve sonuçlarına ilişkin ekran alıntıları Şekil 7'de gösterilmiştir.

Şekil 7. Uygulama Kodlarının Test Sonucu Ekran Alıntıları



Kaynak: (snyk.io/code-checker/python/, 2023).

Çevrimiçi gerçekleştirilen test sonucunda Ziyaretçi Kontrol Sistemi Uygulamasının kodlarında herhangi bir güvenlik problemi olmadığı tespit edilmiştir. Bununla birlikte Ziyaretçi Kontrol Sistemi Uygulaması çevrim dışı olarak çalışan bir sistem olması sebebiyle internet üzerinden yapılabilecek siber saldırılara karşı güvenli bir uygulamadır.

3.1.6 Sistemin Gerçekleştirilmesi ve Değerlendirilmesi

Ziyaretçi Kontrol Sistemi herhangi bir ağa bağlı olmadan veya internetten bağımsız olarak çalışabilmekte LCD Dokunmatik ekranı sayesinde herhangi bir klavye vb. donanıma ihtiyaç duymadan bir tablet gibi kullanılabilir olduğu tespit edilmiştir. Sistem içerisine mobil güç kaynakları powerbank vb. cihazlar ile desteklendiğinde istenen her ortamda elektrik kesintilerine ve siber saldırılara maruz kalmadan işlevini yerine getirebilme kabiliyetine sahip olduğu tespit edilmiştir.

3.2. KISITLAR

Bu çalışmada Ziyaretçi Kontrol Sistemi Uygulaması Raspberry Pi 3 üzerinde kartı üzerinde tasarımı gerçekleştirilmiştir. Uygulamanın başka markalar ait donanımlar veya işletim sistemleri üzerinde nasıl çalışacağı aynı fonksiyonları yerine getirip getiremeyeceği bilinmemektedir. Buna Ziyaretçi Kontrol Sistemi Uygulaması sisteminden en basit örnek vermek gerekirse geliştirilen uygulama arayüzü Raspberry Pi 7 inç LCD Dokunmatik ekran boyutuna (800 x 480 piksel) uygun olarak geliştirilmiştir. Farklı bilgisayar ve ekranlarda uygulama arayüzünün aynı şekilde çalışmayabileceği ekran boyutlarından dolayı sistemi kullanım zorluğu yaşanabilme ihtimali bulunmaktadır.

Ziyaretçi Kontrol Sistemi QR kod içeren Ziyaretçi Giriş Kartı ile çalışmaktadır. Sistem internetten ya da herhangi bir ağdan bağımsız olarak çalışmaktadır. Bu nedenle uzaktan yapılacak siber saldırılara ya da katılımcı/ziyaretçi bilgilerinin uzaktan değiştirilmesine olanak vermemektedir. Ancak bununla birlikte sisteme fotoğraf ve kimlik bilgilerini yükleyecek olan personelin güvenirliliği çok kritiktir. Çünkü bu işleri yapmak üzere görevlendirilecek personelin art niyetli

davranması sonucunda istenmeyen kişilerin geçişleri sağlanacak ve bu da güvenlik zafiyeti oluşturabilecektir.

Tasarımı gerçekleştirilen Ziyaretçi Kontrol Sistemine geçiş onaylandığında ek olarak turnike sistemlerinin kontrolü de entegre edilebilir. Bu durum sistemin Raspberry Pi ile uygulama geliştirmenin birçok olanağını bizlere sunmaktadır. Sistemin geliştirilmesiyle giriş yapan katılımcı/ziyaretçi istatistik bilgileri ile girişi reddedilen kişilerin kayıtları tutulabilir. Bununla birlikte Türkiye'de kullanıma verilen yeni kimlik kartlarının NFC özelliği de sisteme entegre edilerek ile katılımcı/ziyaretçi güvenlik seviyesi daha üst seviyelere çıkarılabilir.

3.3. ZİYARETÇİ KONTROL SİSTEMİNDE KULLANILAN DONANIMLAR

Ziyaretçi Kontrol Sisteminde kullanılan donanımlar aşağıda listelenmiştir;

- Raspberry Pi 3
- Raspberry Pi Kamera
- 16 GB Micro SD Kart
- Raspberry Pi 7 inchLCD Dokunmatik Ekran
- 2 x Güç Adaptörü

3.3.1. Raspberry Pi 3 Donanımı

Raspberry Pi, Raspberry Pi vakfı tarafından Birleşik Krallık'ta geliştirilen, bir bilgisayar monitörüne veya TV'ye takılan ve standart bir klavye ve fare kullanan, düşük maliyetli, kredi kartı boyutunda bir bilgisayardır. Tüm dünya da çocukların kodlama ve elektroniği sevmesi için geliştirilen Raspberry Pi maliyet açısından düşük ve açık kaynak kodlu bir bilgisayar olması nedeniyle popüler hale gelmiştir. Şekil 8'deRaspberry Pi serisinin Raspberry Pi 3 modeli gösterilmiştir.

Raspberry Pi, Her yaştan insanın bilgi işlemi keşfetmesini ve Scratch ve Python gibi dillerde programlamayı öğrenmesini sağlayan yetenekli küçük bir bilgisayardır. İnternette gezinmekten yüksek çözünürlüklü video oynatmaya, elektronik tablolar oluşturmaya, kelime işlemeye ve oyun oynamaya kadar bir

masaüstü bilgisayardan beklenen her şeyi yapabilir kabiliyete sahiptir (raspberrypi.org, 2023).

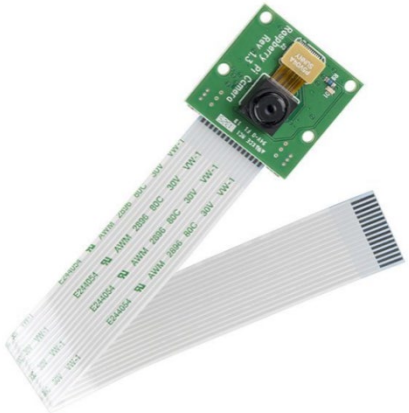
Şekil 8. Raspberry Pi 3

Kaynak:(tr.farnell.com, 2023).

3.3.2. Raspberry Pi Kamera

Ziyaretçi Kontrol Sisteminde ziyaretçiler tarafından Qr Kod gösterildiğinde sistemin QR kodu okuyabilmesi için bir kameraya ihtiyaç duymaktadır. Şekil 9'da gösterilen Raspberry Pi Camera Modülü, Raspberry Pi üzerindeki CSI (Camera Serial Interface) konektörüne direk bağlanabilir.

Şekil 9. Raspberry Pi Kamera



Kaynak:(direnc.net, 2023).

Bu cihaz 5 Mega piksel çözünürlüklü kamera modülü 1080p video ve sabit fotoğraf çekme kapasitesine sahiptir ve Raspberry Pi'yeözel film kablo ile doğrudan bağlanabilecek şekilde tasarlanmıştır (robocombo.com, 2023).

3.3.3. Micro SD Kart

Micro SD Kart Raspberry Pi'nin işletim sisteminin yüklenebilmesi için gereklidir. Bununla birlikte istenen program yada geliştirilen uygulamaların tamamı da bu kart üzerinde çalıştırılmaktadır. SD Kart (Secure Digital Memory Card)'ın kısaltılmışı olup 2001 yılında SanDisk firması tarafından çıkarılmıştır. Aynı zamanda SanDisk'in ürettiği MMC kartının geliştirilmesiyle ortaya çıkmış hafıza kartı standardıdır. SD kart, bilgisayarımızdaki resimleri, fotoğrafları, dokümanları güvenli bir şekilde saklamamıza yarar. SD karta Secure Digital denmesinin sebebi donanımında Digital Rights Management fonksiyonu bulundurmasından dolayıdır (iienstitu.com, 2023).

Ziyaretçi Kontrol Sistemi uygulaması geliştirilirken kullanılan Raspberry Pi işletim sistemi, Python programlama uygulaması ve yazılan kodların tamamı Şekil 10'da gösterilen Micro SD Karta yüklenmiştir.

Şekil 10. Micro SD Kart

Kaynak:(robotistan.com, 2023).

3.3.4. Raspberry Pi 7 inçLCD Dokunmatik Ekran

Raspberry Pi 7 inç LCD Dokunmatik ekranı Raspberry Pi'ye uygun olarak tasarlanmış ve üretilmiştir. Bu sayede ekran donanımı Raspberry Pi kartına 4 adet vida ile çok kolay bir şekilde montajı yapılabilmektedir. Raspberry Pi 7 inç LCD Dokunmatik ekranın Raspberry Pi'ye bağlantısı yapılması durumunda harici bir monitör, klavye ve fareye ihtiyaç kalmayacaktır. Bu sayede Raspberry Pi dokunmatik bir bilgisayara veya tablete dönüşecektir. Raspberry Pi 7 inç LCD dokunmatik ekran Raspberry Pi'ye bağlantısı yapıldığında Raspberry Pi işletim sistemlerinde otomatik olarak tanınmakta ve çalışmaktadır.

Raspberry Pi 7 inç LCD dokunmatik ekrana harici bir güç adaptörü ile microUSB girişinden ekrana güç verilebilmektedir. Bunun haricinde ekran Raspberry Pi üzerinden de beslenebilmektedir. Raspberry Pi'nin micro USB güç girişinden, sürücü kartı üzerindeki USB A tipi konnektöre bağlantı ile gerçekleştirilebilmektedir. Ayrıca Raspberry Pi üzerindeki GPIO pinlerinden 5V ve GND pinlerini doğrudan ekranın güç pinlerine bağlayarak besleme yapılabilmektedir (robolinkmarket.com, 2023).

Şekil 11. Raspberry Pi 7 inch Dokunmatik Ekran

Kaynak:(robolinkmarket.com, elektronikport.com, 2023).

Ziyaretçi Kontrol Sistemi tasarlanırken Raspberry Pi kartı üzerine Şekil 11'de gösterilen Raspberry Pi 7 inch LCD Dokunmatik Ekran monte edilmiş olup sistem kullanıldığında herhangi bir monitör klavye ya da fare kullanımı ihtiyacı ortadan kalkmıştır.

3.4. ZİYARETÇİ KONTROL SİSTEMİNDE KULLANILAN YAZILIMLAR

Raspbian Desktop Operating System (OS): Raspberry Pi içinde bir işletim sistemi ile gelmemektedir. Bu nedenle Raspberry Pi'yi kullanabilmek için işletim sistemi yüklememiz gerekmektedir.Bu çalışmadaRaspberry Pi için Raspian Desktop işletim sistemi kullanılmıştır.

SD CardFormatter: SD kartın üzerine işletim sistemini yazdırmadan önce format atılması gerekmektedir. Bunun için SD CardFormatter yazılımı kullanılmıştır.

Win32DiskImager: Format atılmış olan SD kartın üzerine Raspian Desktop işletim sistemini kurmak için Win32DiskImager programını kullanılmıştır.

VNC Viewer: Raspberry Pi'ye uzaktan bağlantı sağlayabilmek ve kontrol edebilmek için VNC Viewer programı kullanılmıştır.

3.5. DONANIM BAĞLANTILARININ YAPILMASI

Raspberry Pi başka bir bilgisayardan ya da herhangi bir monitörden bağımsız olarak kullanabilmek için Raspberry Pi'ye özel dokunmatik ekran geliştirilmiştir. Raspberry Pi'ye özel olarak tasarlanan LCD (Liquid CrystalDisplay) dokunmatik ekranın elektronik devresi ve güç beslemesi, ölçülerinin aynı boyutta olması birebir uyum sağlanmasına güç paylaşımı yapılabilmesine ve direkt olarak üzerine montaj yapılmasına olanak sağlamaktadır. Şekil 12'de Raspberry Pi'ye Raspberry Pi 7 inch Dokunmatik LCD Ekran bağlantısı ekran kutusu içerisinden çıkan Flex kablo yardımı ile yapılmaktadır.

Raspberry Pi'nin LCD ekran üzerine sabitlenmesi ise 4 adet vida yardımı ile yapılmaktadır. LCD ekranın güç beslemesi ise Raspberry Pi ile aynı adaptör uyumlu ancak tek adaptör ile ikisini birden çalıştırmak istenirse adaptör öncelikle ekranın güç girişine bağlanmalı sonrasında LCD dokunmatik ekran üzerindeki USB (Universal

SerialBus) portundan Raspberry Pi'nin güç girişine özel olarak tasarlanan kablo ile bağlantı yapılmalıdır. Ancak bu şekilde bağlantı yapıldığında bazen düşük voltaj hatası verebilmektedir.

Şekil 12. Raspberry Pi'ye Raspberry Pi 7 inch Dokunmatik Ekran bağlantısı

Kaynak: Yazar tarafından derlenmiştir.

Şekil 13. Raspberry Pi'ye Raspberry Pi Kamerasının bağlantısı

Kaynak: Yazar tarafından derlenmiştir.

Raspberry Pi'ye kamera bağlanabilmesi için Raspberry Pi'ye özel olarak üretilmiş Raspberry Pi kamera kullanılmıştır. Raspberry Pi kamerası flexi kablo ile Raspberry Pi'nin anakartına Şekil 13'deki gibi bağlanmaktadır.

Raspberry Pi'ye ve Raspberry Pi 7 inch Dokunmatik Ekrana güç bağlantıları Şekil 14'teki gibi bağlanmaktadır. Raspberry Pi donanımına uygun olarak 5V 2.5A olarak Raspberry Pi adaptörü kullanılmıştır. Ancak İki farklı donanımın tek bir güç kaynağı üzerinden beslenmesi durumunda Raspberry Pi düşük voltaj hatasına sebep olduğundan dokunmatik LCD ekranı ve Raspberry Pi'yi ayrı güç adaptörlerinden beslenmesi daha verimli çalışmasına sağlayacaktır.

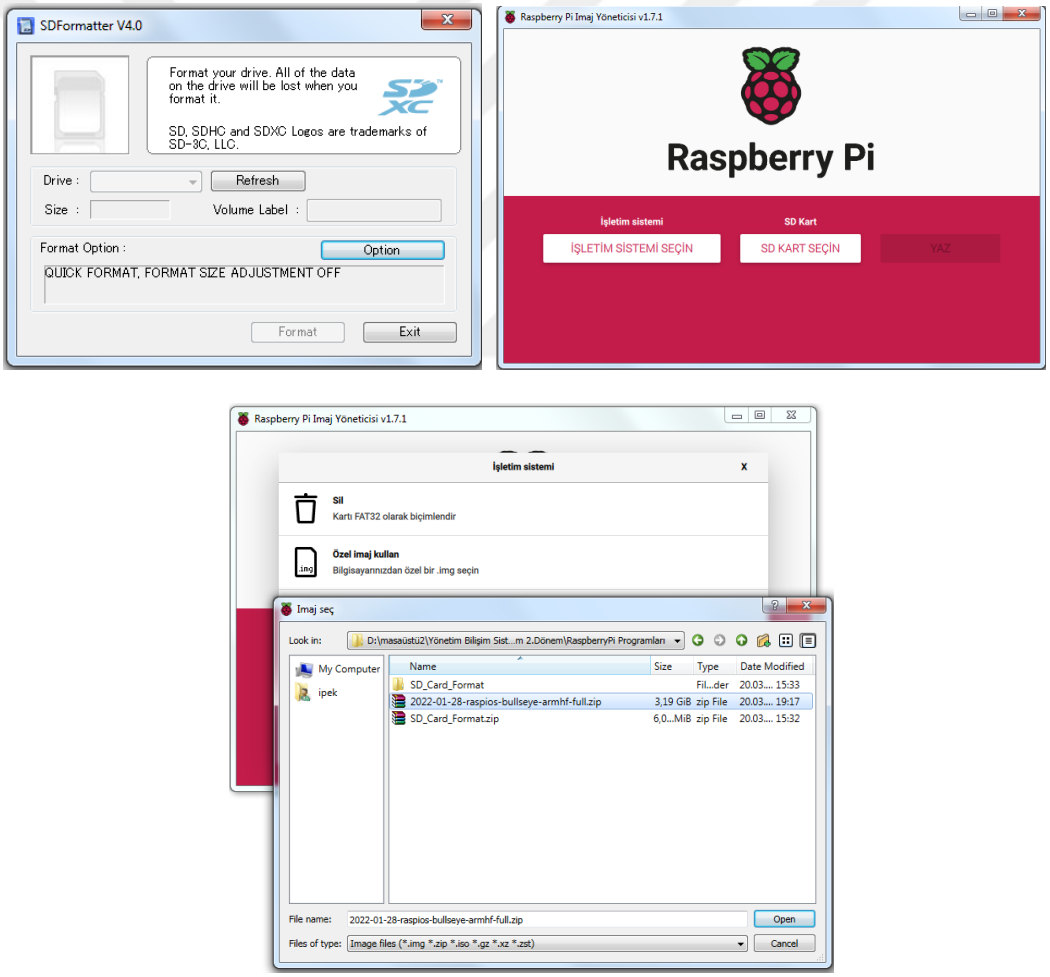
Şekil 14. Raspberry Pi ve LCD ekranın güç bağlantısı

Kaynak: Yazar tarafından derlenmiştir.

3.5.1. Raspberry Pi İşletim Sisteminin Micro-Sd Karta Kurulması

Bu aşamada öncelikle gerekli olan SD CardFormatter, Raspberry Pi İmaj Yöneticisi ve Raspberry Pi OS imajının indirilmesi gerekmektedir. Şekil 15'deki gibi SD Formatter V4.0 programı ile SD kartı formatlanır ve Raspberry Pi İmaj Yöneticisi programını kullanarak Raspberry Pi OS işletim sistemini SD kart üzerine yazdırılır. Sonra Raspberry Pi'ye SD kartı yerleştirip işletim sistemi kurulumu tamamlanacaktır.

Şekil 15. Raspberry Pi İşletim Sisteminin Micro-Sd Karta Kurulması



Kaynak: Yazar tarafından derlenmiştir.

3.5.2. Raspberry Pi Kamerasının Raspberry Pi 3 Üzerinden Aktif Edilmesi

Raspberry Pi'ye Raspberry Pi Kamerası bağlantısı yapıldığında kamera kendiliğinden aktif olmamaktadır. Şekil 16'daki gibi Raspberry Pi Software Configuration Tool üzerinden aktif edilmesi gerekmektedir.

Şekil 16. Raspberry Pi Kamerasının Sistem üzerinden aktif edilmesi

Kaynak: Yazar tarafından derlenmiştir.

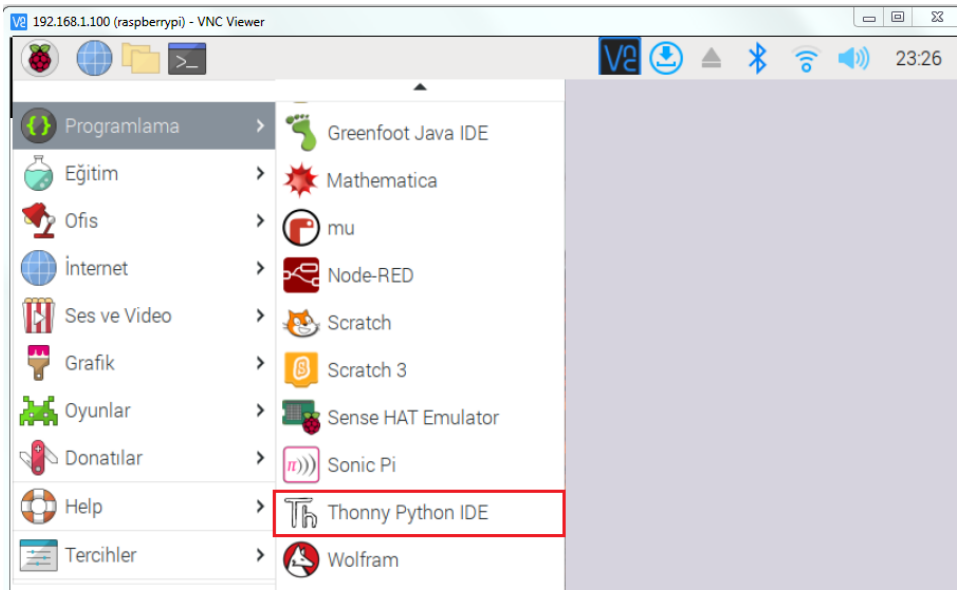
3.5.3. VNC Viewer ile Raspberry Pi'ye Uzaktan Bağlantı Yapılması

Raspberry Pi teknolojisi ile kurulmuş sistemlerde Raspberry Pi'yi yönetebilmek için sürekli olarak kablo bağlantısına yada harici ekranlara ihtiyaç duyulmamaktır. VNC Viewer ile Raspberry Pi ye uzaktan bağlantı yapılabilmesi için öncelikle Raspperry Pi'nin internet bağlantısının olması gerekmektedir. Bununla birlikte Şekil 18'deki (s. 33'de gösterilmiştir) gibi Raspberry Pi yapılandırılması arayüzünde bulunan VNC'ye izin verilmesi ve ayrıca bağlantının her zaman sağlanabilmesi için değişmeyen statik bir ip belirlenmesi gerekmektedir (youtube.com, 2023).

3.5.4. Raspberry Pi Üzerinde Uygulamayı Çalıştıran Kodlar ve Açıklaması

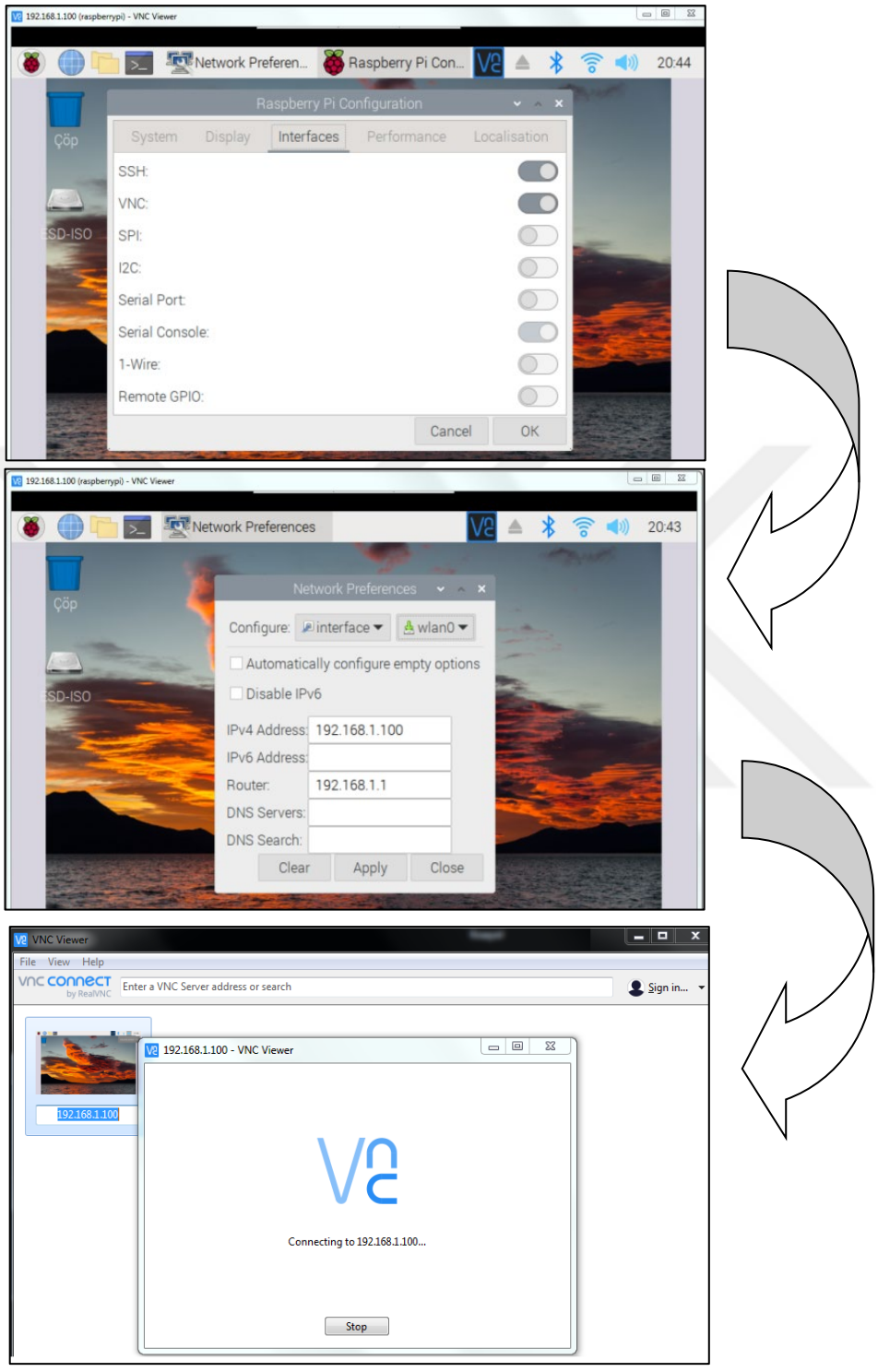
Ziyaretçi Kontrol Sistemi Uygulamasının geliştirilmesi için Şekil 17'de gösterilen Raspberry Pi üzerinde bulunan Thonny Python programlama dili kullanılmıştır.

Şekil 17. Raspberry Pi üzerinde bulunan Thonny Python programlama dili



Kaynak: Yazar tarafından derlenmiştir.

Şekil 18. Raspberry Pi VNC özelliğinin aktif edilmesi

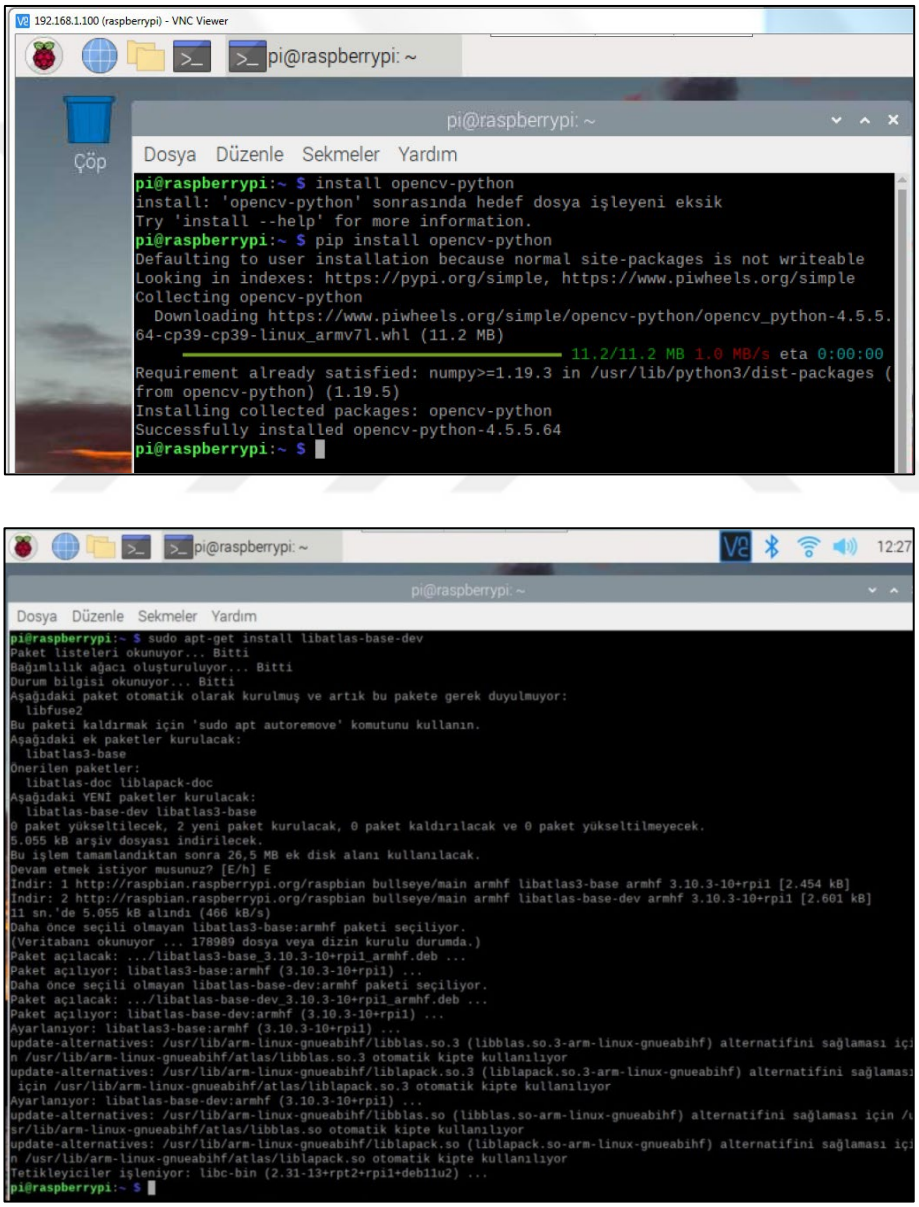


Kaynak: Yazar tarafından derlenmiştir.

3.5.5. Kodlamada Kullanılacak OpenCv ve Diğer Kütüphanelerin Yüklenmesi

Ziyaretçi Kontrol Sistemini uygulaması geliştirilirken kullanılacak kodların ve kütüphanelerin Raspberry Pi üzerinde Şekil 19'da gösterildiği gibi yüklenmesi gerekmektedir.

Şekil 19. Raspberry Pi'ye kodların ve kütüphanelerin yüklenmesi



Kaynak: Yazar tarafından derlenmiştir.

3.5.6.Raspberry Pi Üzerinde Uygulama Kodlarının Gösterilmesi

Ziyaretçi Kontrol Sistemi uygulaması geliştirilirken kullanılan kodlar Şekil 20'de gösterilmiştir. Bu kodlar Raspberry Pi üzerinde bulunan Thonny uygulaması üzerinde yazılmıştır. Programlama dili olarak Python kullanılmıştır.

Şekil 20. Ziyaretçi Kontrol Sistemi Uygulama kodları

```
            myOutput = 'Yetkisiz'
            myColor = (0, 0, 255)
            onay_label.configure(text="GİRİŞ ONAYLANMADI")
            onay_label["background"]="#E00543"
            isim_label["background"]="#E00543"
            isim_label.configure(text="")
            profile=ImageTk.PhotoImage(Image.open("profile.jpg").resize((150,150)))
            profile_label.configure(image=profile)
        pts = np.array([barcode.polygon],np.int32)
        pts = pts.reshape((-1,1,2))
        cv2.polylines(img,[pts],True,myColor,5)
        pts2 = barcode.rect
        cv2.putText(img,myOutput,(pts2[0],pts2[1]),cv2.FONT_HERSHEY_SIMPLEX,0.9,myColor,2)
        tikla=not tikla
    cv2image= cv2.cvtColor(img,cv2.COLOR_BGR2RGB)
    img1 = Image.fromarray(cv2image)
    imgtk = ImageTk.PhotoImage(image = img1)
    kamera.imgtk = imgtk
    kamera.configure(image=imgtk,width=genişlik,height=uzunluk)
    kamera.after(20, show_frames)
def tikla_func():
    global cap, tikla
    tikla= not tikla
    if tikla:
        print("tiklandi")
        cap=cv2.VideoCapture(0)
        show_frames()
ana_pencere.columnconfigure(0,weight=5)
ana_pencere.columnconfigure(1,weight=1)
#ana_pencere.rowconfigure(0, weight=1)
ana_pencere.rowconfigure(0, weight=1)
ana_pencere.rowconfigure(1, weight=4)
ana_pencere.rowconfigure(2, weight=4)
ana_pencere.rowconfigure(3, weight=4)
ana_pencere.rowconfigure(4, weight=1)
####################
icon1=Label(ana_pencere,image=icon)
icon1["background"]="#A2B29F"
icon1.grid(row=0,column=1,sticky=NSEW,padx=(10,20),pady=(20,0))
##################
kamera =Label(ana_pencere,image=trigger)
kamera["background"]='#A2B29F'
kamera.grid(row=0,column=0,rowspan=4,padx=(30,5))
button= Button(ana_pencere,text="SORGULA",command=tikla_func,fg="#205375",font=(font_type,13,"bold"))
button["background"]="#B3E8E5"
button.grid(row=4,column=0,padx=(30,5),pady=(0,30))
onay_label=Label(ana_pencere,text="HOŞ GELDİNİZ",fg="white",font=(font_type,15))
onay_label["background"]="#E00543"
onay_label.grid(row=1,column=1,sticky=NSEW,padx=(10,20),pady=(30,0),ipadx=30)
isim_label=Label(ana_pencere,text="...",fg="white",font=(font_type,10))
isim_label["background"]="#E00543"
isim_label.grid(row=2,column=1,sticky=NSEW,padx=(10,20),pady=(0,30))
profile_label =Label(ana_pencere,image=profile)
profile_label["background"]='#A2B29F'
profile_label.grid(row=3,rowspan=2,column=1,sticky=NSEW,padx=(10,20),pady=(0,30))
mainloop()

```

Kaynak: Yazar tarafından derlenmiştir.

3.5.7.Ziyaretçi Kontrol Sistemi Uygulamasında Kullanılan Kodların Açıklamaları ile Birlikte Gösterimi

Ziyaretçi Kontrol Sistemi uygulaması geliştirilirken kullanılan kodların satır satır ne işe yaradığı hangi kodun hangi fonksiyonları yerine getirdiği aşağıda ayrıntılı bir şekilde açıklanmıştır.

```
turtle import bgcolor, width
```
**Turtle: Kullandığımız renk kodlarını ve uzunluk birimlerini pythonın derleyicisinin anlamlandırmasını sağlayan kütüphanedir.*

```
import cv2
from cv2 import VideoCapture
```
**Cv2: Görüntü işleme, kaydetme ve değiştirmeye yönelik işlemleri yapmaya yönelik kütüphanedir.*

```
import numpy as np
```
**Numpy: Görüntü verilerini matris verisine dönüştürerek görüntü işleme operasyonlarında kullanılmasını sağlar.*

```
from pyzbar.pyzbar import decode
```
**Pyzbar: Görüntülerden barcode ve qrcode çözümlenmesi sağlar.*

```
from tkinter import *
```
**Tkinter: Python ekosisteminde işletim sistemlerinde var olan widgetları manüpüle ederek yazılımlara görsel arayüz oluşturmayı sağlar.*

```
from PIL import Image, ImageTk
```
**Pillow: Harddiskten ram'e görüntülerin yüklenmesini ve numpy kütüphanesinde matris yapısına dönüştürdüğümüz görüntüleri tekrar jpg ve png formatlarına çevirerek tkinter ile oluşturduğumuz görsel arayüze işlenmiş fotoğraf karnelerini görüntülenebilmesini sağlar.*

```
font_type="Arial"
font_size=20
tikla= FALSE
cap= NONE
genişlik=640
uzunluk=480
dim = (genişlik, uzunluk)
```
**Görsel arayüzde kullanılan stiller ve global olarak kullanılacak değişkenler tanımlanmıştır.*

```
ana_pencere=Tk()
```
**Tkinter kütüphanesindeki Tk classından ana_pencere nesnesi üretilerek program arayüzünü çalıştıracak ana widget oluşturulmuştur*

```
ana_pencere['background']='#A2B29F'
ana_pencere.title('Ziyaretçi Giriş Kontol Sistemi')
ana_pencere.geometry("800x480")
```
**ana_pencere widgetınaarkaplan rengi, program etiketi ve program ilk yüklendiğindeki boyutları ayarlanmıştır.*

```
trigger= ImageTk.PhotoImage(Image.open("trigger.png").resize(dim))
icon = ImageTk.PhotoImage(Image.open("icon.jpg").resize((150,150)))
profile=ImageTk.PhotoImage(Image.open("profile.jpg").resize((150,150)))
```
**Program içindeki lens ve üniversite iconuyla qr kodu taranan personelin profil resminin olduğu yere başlangıç fotoğrafları Pillow kütüphanesi kullanılarak ram'e alınıp kullanılacak ekrana uygun geometrik ölçülerle şekil verilmiştir.*

```
with open('myDataFile.text') as f:
myDataList = f.read().splitlines()
```
**Txt dosyasından personelin kimlik ve ad soyad verileri hafızaya alınmıştır*

```
kimlik_bilgisi=[]
isim_bilgisi=[]
for x in myDataList:
x=x.split("-")
kimlik_bilgisi.append(x[0])
isim_bilgisi.append(x[1])
```
**Kimlik ve isim bilgileri daha sonra kullanılmak üzere iki ayrı list veri tipinden değişkene kaydedilmiştir. Dosya içindeki her satırı "-" karakterine göre ayırarak isim ve kimlik bilgisi ayrıştırılmıştır.*

```
print(kimlik_bilgisi)
print(isim_bilgisi)
#ana_pencere.attributes('-fullscreen',True)
```
**Bu satırdaki kare kaldırılırsa program ilk açıldığı anda tam ekran olarak görüntülenecektir.*

```
def show_frames():
```
**Tkinter kütüphanesinin sağladığı Label içine görüntü verecek fonksiyon tanımlamaya başlanmıştır.*

```
global genişlik
global uzunluk
global tikla
global cap
global dim
global profile
```
**Fonksiyon içinde gerekli olan global değişkenler fonksiyonun kapsama alanına sokulmuştur.*

```
if tikla:
success, img = cap.read()
img = cv2.resize(img,dim)
else:
kamera.configure(image=trigger)
cap.release()
return 0
```
*"SORGULA" butonuna tıklandığında veya qr kode çözümlendiğinde kameranın aktif olup görüntü alınmaya başlanması ya da görüntü alımının sonlanması sağlanmıştır.

```
for barcode in decode(img):
```
*Kameradan gelen görüntülerde qr kod çözümlendiği zaman bu program bloğuna girilir.

```
myData = barcode.data.decode('utf-8')
```
*Barcoddan gelen ham veri utf 8 formatında çözümlenerek anlamlı yazı karakterlerine dönüştürülür.

```
print(decode(img))
if myData in kimlik_bilgisi:
```
*Eğer okunan kimlik bilgisi txt dosyamız Yetkili olarak tanımlandı ise bu program bloğuna girilir.

```
i=kimlik_bilgisi.index(myData)
```
*Kimlik bilgisinin listede kaçıncı indis olduğu belirlenerek ad soyad verisni eleştirmek için daha sonra kullanılmak üzere i değişkenine eklenir.

```
myOutput = 'Yetkili'
myColor = (0,255,0)
onay_label.configure(text="GİRİŞ ONAYLANDI")
```
*Personel yetkiliye görsel arayüzdeki sol tarafta bulunan Label widgetında onay yazısı görüntülenir.
```
onay_label["background"]="#A6CB12"
```
*Label, eğer personel Yetkili ise yeşil renge döner.

```
isim_label.configure(text=isim_bilgisi[i])
```
*Yukarıda i değişkenine yazılan isim bilgisinin bulunduğu indis kullanılarak ekrana kimlik bilgisiyle eleştirilen ad soyad yazdırılır.

```
isim_label["background"]="#A6CB12"
```
*Label,eğer personel Yetkili ise yeşil renge döner.

```
        profile=ImageTk.PhotoImage(Image.open(myData+".jpg").resize((150,150)))
profile_label.configure(image=profile)
```
*Yetkili personelin fotoğrafı klasör içinden bulunarak açılıp yeniden boyutlandırılır ve görsel arayüzde görüntülenmesi sağlanır.

```
print(myData)
else:
```
**Eğer personel Yetkisiz ise bu kod bloğuna girilir.*

```
myOutput = 'Yetkisiz'
myColor = (0, 0, 255)
onay_label.configure(text="GİRİŞ ONAYLANMADI")
onay_label["background"]="#E00543"
isim_label["background"]="#E00543"
```
**Kırmızı fon üzerine onaylanmadı yazısı yazdırlır.*

```
isim_label.configure(text="")
```
**Listede olmayan personelin ad soyad bilgisi yeri boş bırakılır.*

```
        profile=ImageTk.PhotoImage(Image.open("profile.jpg").resize((150,150)))
profile_label.configure(image=profile)
```
**Tanımlanamayan personelin profil fotoğrafı olmadığı için varsayımlar insan ikonu görüntülenir.*

```
pts = np.array([barcode.polygon],np.int32)
```
**Kameradan gelen fotoğraf karesinde qr kodun köşelerinin konumu bir numpy matrisi içerisinde 32 bit bir integer olarak saklanır.*

```
pts = pts.reshape((-1,1,2))
```
**Pts değişkenine kaydedilen köşe konumları, opencv kütüphanesinin çözümleyebileceği boyutlarda y × 1 × 2 boyutlarına çevrilir. -1 parametresi, matrisin ilk boyutunun otomatik olarak köşe noktasına sayısına göre şekillenmesi için verilmiştir.*

```
      cv2.polylines(img,[pts],True,myColor,5)
```
**Cv2 kütüphanesi ile köşe noktalarından geçen, istenen renkte ve kalınlıkta bir dikdörtgen çizilmesi sağlanmıştır.*

```
pts2=barcode.rectcv2.putText(img,myOutput,(pts2[0],pts2[1]),cv2.FONT_HERSHEY_SIMPLEX,0.9,myColor,2)
```
**Kameradan gelen görüntünün üstüne de personelin yetkili ya da yetkisiz olduğu yazılmıştır*

```
tikla=not tikla
```
**Global olarak kullanılan tikla değişkeni güncellenerek qr code tarandıktan sonra Kameradan veri akışı kesilmiştir.*

```
cv2image= cv2.cvtColor(img,cv2.COLOR_BGR2RGB)
```
**Varsayılan olarak kamera tarafından BGR formatı olarak alınan fotoğraf kareleri RGB formatına çevrilerek doğal renk paletine geçilmiştir.*

```
img1 = Image.fromarray(cv2image)
```

*Kameradan gelen ham matris şeklinde hafızada bulunan görüntü normal image nesnesine çevrilmiştir.

```
imgtk = ImageTk.PhotoImage(image = img1)
```
*image nesnesi tkinter kütüphanesinin çözümleyeceği imagetk nesnesine dönüştürülmüştür.

```
kamera.imgtk = imgtk
kamera.configure(image=imgtk,width=genişlik,height=uzunluk)
```
*Arayüzdeki lens ikonunun olduğu bölgeye işlenmiş fotoğraf kareleri yerleştirilmiştir.

```
kamera.after(20, show_frames)
```
*Her 20 mikrosaniyede bir tün fonksiyonun recursive olarak dönmesi sağlanmıştır.

```
def tikla_func():
global cap, tikla
tikla= not tikla
if tikla:
print("tiklandi")
      cap=cv2.VideoCapture(0)
show_frames()
```
*Kullanıcı kendi isteği ile tarama işlemini başlatıp sonlandırması için "Sorgula" butonuna tıklandığında kamerayı açıp kapatan ve eğer sorgulama istenmiş ise show_frames recursive fonksiyonunu başlatan fonksiyon aşağıda kullanılmak üzere tanımlanmıştır.

```
ana_pencere.columnconfigure(0,weight=5)
ana_pencere.columnconfigure(1,weight=1)
#ana_pencere.rowconfigure(0, weight=1)
ana_pencere.rowconfigure(0, weight=1)
ana_pencere.rowconfigure(1, weight=4)
ana_pencere.rowconfigure(2, weight=4)
ana_pencere.rowconfigure(3, weight=4)
ana_pencere.rowconfigure(4, weight=1)
```
*Programın arayüzünün ekran boyutuna göre yeniden şekillenebilmesi için responsive görüntüleme katmanı oluşturulmuştur. Her satır ve sütuna ekranda kaplayacağı pay tanımlanmıştır. Bu tasarım paternine grid (ızgara) paterni denmektedir.

```
icon1=Label(ana_pencere,image=icon)
icon1["background"]="#A2B29F"
icon1.grid(row=0,column=1,sticky=NSEW,padx=(0,100),pady=(50,0))
```
*Üniversite ikonu görsel arayüze eklenmiş, arkaplan rengi programın ana temasına göre ayarlanmıştır. Sticky parametresi ile ikonun içinde bulunduğu koordinatlara göre ikonun büyüyüp küçülmesi sağlanmıştır. Padx ve pady ile ikonun göze daha uygun gözükmesi için dikey ve yatay eksende boşluklar bırakılarak hassas boyutlandırma yapılmıştır.

```
kamera =Label(ana_pencere,image=trigger)
kamera["background"]='#A2B29F'
kamera.grid(row=0,column=0,rowspan=4)
```
**Kamera görüntüsünün görüntüleneceği bölgeyi büyütmek için rowspan parametresi ile kamera görüntüsünün kendi yerleştirildiği ızgaradadan aşağı doğru 4 satır daha büyümesi sağlanmıştır.*

```
button=Button(ana_pencere,text="SORGULA",command=tikla_func,fg="#205375",
font=(font_type,font_size,"bold"))
```
**Sorgula butonu burada oluşturulmuştur. Buttona tıklandığında hangi fonksiyonun aktif olacağı command parametresi ile gösterilmiştir. tikla_func fonksiyonu yukarıda tanımlanmıştır.*

```
button["background"]="#B3E8E5"
button.grid(row=4,column=0,sticky=EW,padx=350,pady=(0,60))
```
**Sorgula butonuna şekillendirme ve renklendirme yapılmıştır.*

```
onay_label=Label(ana_pencere,text="GİRİŞ
ONAYLANMADI",fg="white",font=(font_type,font_size))
onay_label["background"]="#E00543"
onay_label.grid(row=1,column=1,sticky=NSEW,padx=(0,100),pady=(30,0),ipadx=3
0)
```
**Qr kod okutulduktan sonra personelin yetkili mi Yetkisiz mi olduğunun görüntüleneceği Label oluşturulmuş ve kullanılacak ekrana uygun boyut ve renkler verilmiştir.*

```
isim_label=Label(ana_pencere,text="...",fg="white",font=(font_type,15))
isim_label["background"]="#E00543"
isim_label.grid(row=2,column=1,sticky=NSEW,padx=(0,100),pady=(0,20))
```
**Personelin kimlik bilgisiyle eleştirilen ad soyad bilgisinin görüntüleneceği Label oluşturulmuştur.*

```
profile_label =Label(ana_pencere,image=profile)
profile_label["background"]='#A2B29F'
profile_label.grid(row=3,rowspan=2,column=1,sticky=NSEW,padx=(0,100),pady=(0
,50))
```
**Personelin profil fotoğrafının görüntüleneceği Label oluşturulmuş ve grid (ızgara) tasarım yapısına uygun şekilde boyutlandırılmıştır.*
```
mainloop()
```

3.5.8. Ziyaretçi Kontrol Sistemi Uygulamasının Çalıştırılması

Şekil 21'de gösterilen Ziyaretçi Kontrol Sistemi üzerinde "SORGULA" butonuna tıklandığında Şekil 22'de örnek olarak gösterilen Ziyaretçi Giriş Kartındaki QR Kod sistemin arka tarafında bulunan Şekil 23'de gösterilen Ziyaretçi Kontrol Sisteminin Arka Tarafında bulunan kameraya okutulduğunda ziyaretçinin sistem tarafından katılmaya yetkili olup olmadığı tespit edilmiştir.

Şekil 21. Ziyaretçi Kontrol Sistemi

Kaynak: Yazar tarafından derlenmiştir.

Şekil 22. Ziyaretçi Giriş Kartı Örneği

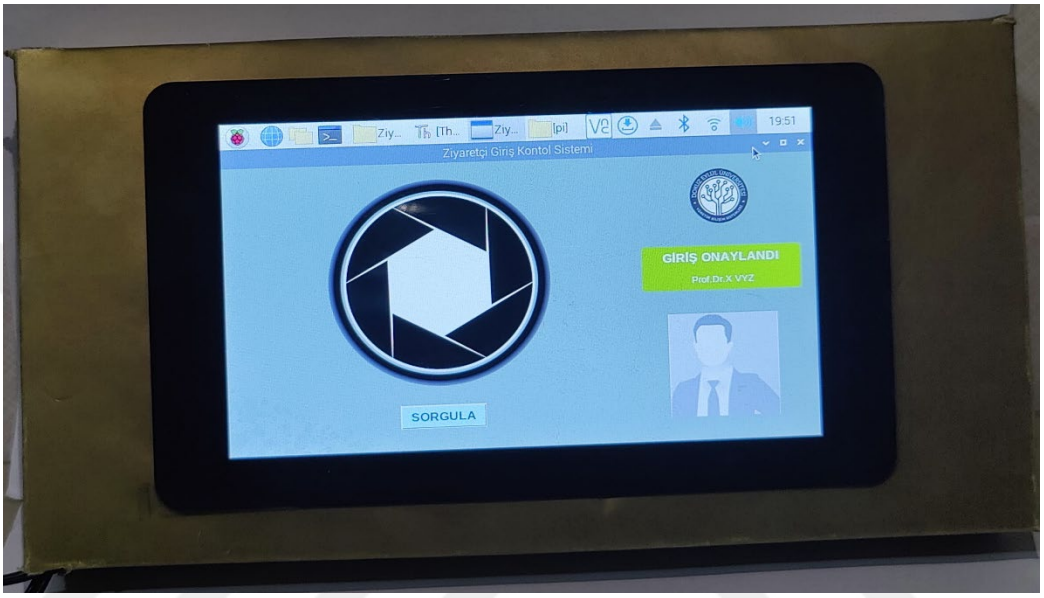
Kaynak: Yazar tarafından derlenmiştir.

Şekil 23. Ziyaretçi Girişinin Sistemin Arka Tarafı

Kaynak: Yazar tarafından derlenmiştir.

Sorgulama sonucunda sistem tarafından ziyaretçinin katılımı doğrulanır ve Şekil 24’te gösterildiği gibi "GİRİŞ ONAYLANDI" mesajı görüntülenerek ziyaretçinin katılımına onay verilir.

Şekil 24. Ziyaretçi Girişinin Sistem Tarafından Onaylanması

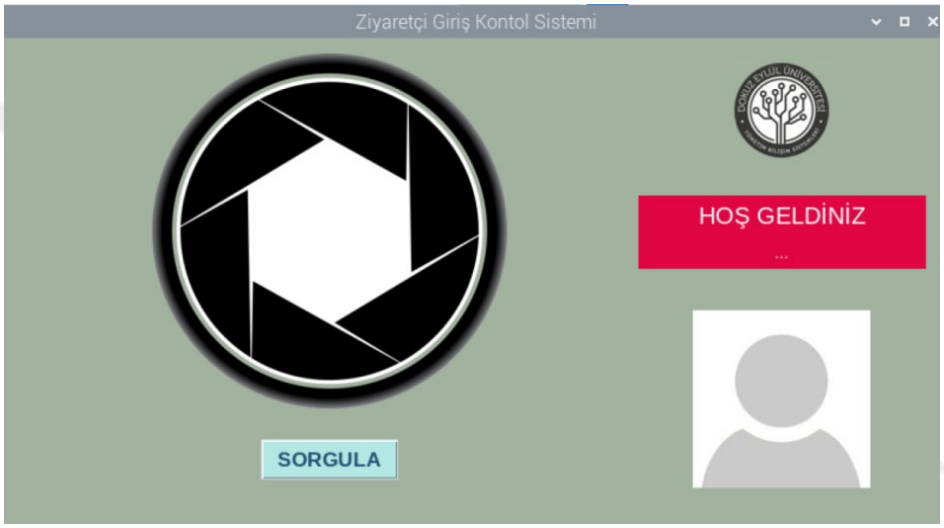


Kaynak: Yazar tarafından derlenmiştir.

3.5.9. Ziyaretçi Kontrol Sistemi Uygulamasının Ekran Alıntıları

Ziyaretçi Giriş Kontrol Sistemi Uygulaması çalıştırıldığında ekrana Şekil 25'teki gibi bir arayüz gelmektedir. Bu arayüzde bulunan "SORGULA" butonu ile giriş yapmak isteyen ziyaretçinin yetkili olup olmadığı uygulama tarafından sorgulanır.

Şekil 25. Ziyaretçi Girişinin Sistemi Uygulaması Ekran Alıntısı

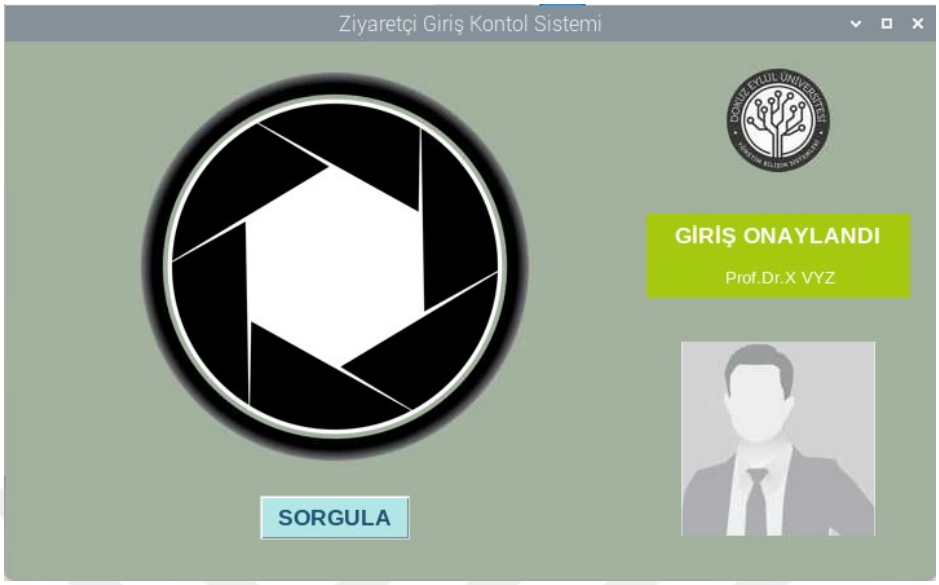


Kaynak: Yazar tarafından derlenmiştir.

Ziyaretçi kendisine daha önceden verilen QR koda sahip ziyaretçi giriş kartını kameraya gösterdiğinde yetkili olup olmadığını ziyaretçinin fotoğrafı ile birlikte Şekil 26'da gösterilmiştir.

Uygulamada Raspberry Pi kamerası ile QR kodu okuduğunda eğer kayıtlı katılımcı ise Şekil 26'daki gibi Yeşil Zemin Üzerinde "GİRİŞ ONAYLANDI" mesajı katılımcının adı ve soyadı ile birlikte ekranda görüntülenmektedir. Ayrıca katılımcının daha önceden sisteme yüklenen fotoğrafı da gösterilerek güvenlik görevlisi tarafından giriş yapmak isteyen ziyaretçinin fotoğraf üzerinden de kontrol etmesine yardımcı olmaktadır.

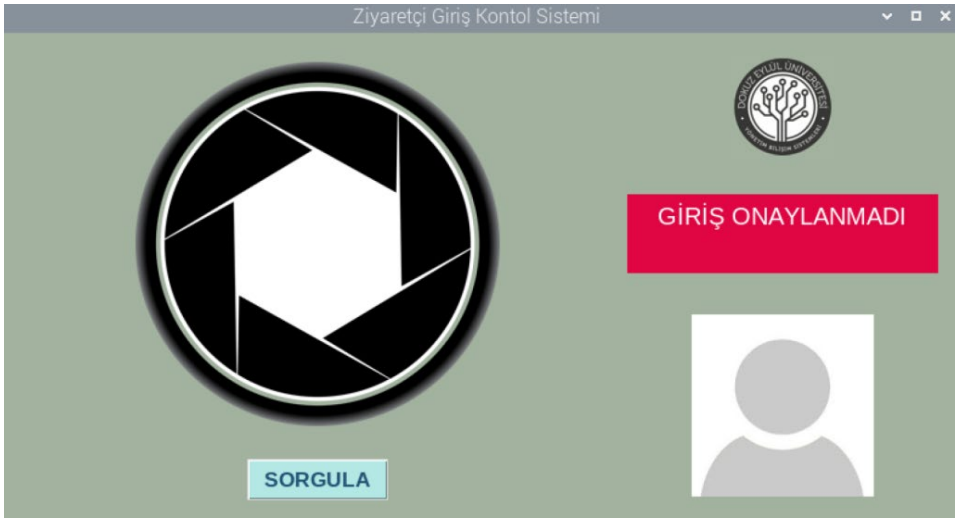
Şekil 26. Ziyaretçinin Girişi Onayının Ekran Alıntısı



Kaynak: Yazar tarafından derlenmiştir.

Buna karşın Raspberry Pi kamerası ile QR kodu okuduğunda eğer kayıtlı katılımcı değil ise Kırmızı Zemin Üzerinde "GİRİŞ ONAYLANMADI" mesajı Şekil 27'deki gibi görüntülenmektedir.

Şekil 27. Ziyaretçinin Girişi Reddinin Ekran Alıntısı



Kaynak: Yazar tarafından derlenmiştir.

SONUÇ

Raspberry Pi Donanımı ve Python Programlama dili ile gerçekleştirdiğim Kurumlarda Siber Güvenlik Tabanlı Ziyaretçi Kontrol Sistemi Tasarımı ve Uygulaması konulu Yüksek Lisans Tezimde özellikle toplantı, seminer, söyleşi, sempozyum, çalıştay, brifing, fuar vb. faaliyetlerin düzenlendiği yerlerde giriş güvenliğinin sağlanmasına yönelik "ZİYARETÇİ KONTROL SİSTEMİ" uygulaması geliştirilmiştir. Katılımcılara önceden gönderilen QR kodlu giriş kartları sayesinde giriş yapmak isteyen kişin yetkili olup olmadığı kontrol edilmekte ve ayrıca sistemde kayıtlı olan katılımcının fotoğrafı gösterilere güvenlik görevlilerinin tanımasına yardımcı olmaktadır.

Geliştirilen uygulamanın diğer güvenlik ve geçiş sistemlerine göre farkı çevrimdışı çalışması olup herhangi bir siber saldırıya maruz kalma ihtimalinin bulunmamasıdır.

Bununla birlikte Raspberry Pi de kullanılan işletim sistemi *Raspberry Pi OS* (eski adıyla *Raspbian*) linux tabanlı bir işletim sistemi olduğundan Windows'a göre daha stabil çalışması ve siber saldırılara karşı daha güvenli olduğundan dolayı Ziyaretçi Kontrol Sistemi tasarımı ve uygulaması geliştirilirken Raspberry Pi tercih edilmiştir.

Güvenlik görevlileri ziyaretçilerin giriş kontrollerinde katılımcıları daha önceden hiç tanımadıkları ve görmedikleri için gelen gerçek katılımcıların dışında, sahte kimliklerle art niyetli kişiler tarafından yetkisiz girişler yapılabilmekte, amaçlarına göre bilgi casusluğu, terörizm amaçlı saldırı vb. eylemlerde bulunabilmektedirler. Bu sistemde ise daha önceden sisteme fotoğrafları ile birlikte kayıtları yapılarak ziyaretçilerin bilgileri yüklenmektedir. Ziyaretçilere ise sadece QR koda sahip bir giriş kartı verilmektedir. Bu sayede sahte fotoğraflarla kimlik düzenlenmiş bile olsa QR kod sisteme okutulduğunda kişinin gerçek fotoğrafı ve bilgileri görüntüleneceğinden yetkisiz bir kullanıcının giriş yapması neredeyse imkansızdır.

Piyasada çok çeşitli farklı firmaların üretmiş oldukları giriş kontrol sistemleri mevcuttur. Ancak bu sistemler firmalar tarafından çok yüksek maliyetli yıllık bakım sözleşmeleri gerektiren idamesi kolay olmayan sistemlerdir. Ayrıca bu sistemlerde

ileriki yıllarda herhangi bir arıza meydana geldiğinde firmaya ya da üreticiye ulaşılamadığı durumlarda sistem atıl olarak kalmakta ve kullanıcılar yeni bir sistem tedarik etmek zorunda kalmaktadırlar. Bu durum işletmelerin ve kurumların karşılaşmak istemediği bir süreç haline gelmiştir.

Şekil 28. Yönetim Bilişim Sistemleri Piramidi

Kaynak:(vahaptecim.com.tr, 2023).

Yönetim Bilişim Sistemlerinin ilgi alanına giren bu tez çalışması kapsamında Şekil 28'de gösterilen Yönetim Bilişim Sistemleri Piramidi incelendiğinde Kurumlarda Siber Güvenlik Tabanlı Ziyaretçi Kontrol Sistemi söz konusu piramidin en alt basamağından en üst basamağına kadar olan karışılabilecek sorunların çözümlenmesinde etkin rol oynayacaktır. Çünkü kurumlarda katılımcı/ziyaretçi giriş güvenliği söz konusu olduğunda en alt çalışandan en üst seviye yöneticilere kadar herkesi ilgilendiren bir ihtiyaç konumundadır. Ancak bu tez çalışmasını tam olarak piramit üzerinde konumlandırmak gerekirse Kurumlarda Siber Güvenlik Tabanlı Ziyaretçi Kontrol Sistemi Yönetim Bilişim Sistemleri Piramidi'nin en alt basamağında bulunan "Ofis otomasyonu / Veri İşleme Sistemleri" kapsamında yer almaktadır. Problem Tipi kapsamında "Yapısal", Karar Tipleri kapsamında

“Operasyonel Kararlar” ve Yöneticiler seviyesinde ise Operasyonel Yöneticiler kapsamında yer almaktadır. Ancak Yönetim Bilişim Sistemleri Piramidi bir bütün olarak ve birbiriyle ilişkilendirilmiş bir yapı olarak düşünüldüğünde tüm basamaklara ihtiyaç olduğunu kolaylıkla görebiliriz.

Bu tez kapsamında gösterildiği üzere çok yüksek maliyetli olan ve hacim olarak büyük olan geçiş sistemleri yerine daha düşük maliyetle ve tamamen kullanıcı isteklerine göre yapılandırılabilen üzerinde çok farklı donanım ve fonksiyonları ekleyebileceğimiz düşük maliyetli, kredi kartı büyüklüğündeki Raspberry Pi ile geliştirilebilecek ek güvenlik özelliklerine sahip geçiş sistemlerinde Raspberry Pi kullanmak daha doğru sonuçlar elde edilmesine yardımcı olacaktır.

KAYNAKÇA

Asya Otomatik Kapı Sistemleri. (2023).
Şifreli ve Kartlı Geçiş Sistemleri. https://www.asyakapisistemleri.com.tr/urun/sifreli-ve-kartli-gecis-sistemleri/, (15.05.2023).

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24-28.

BARFAŞ Otomasyon Teknolojileri Sanayi ve Ticaret Limited Şirketi
Kartlı Geçiş Sistemleri Tarihe Karışıyor, QR Geçiş Sistemleri Kolaylık ve Hız Sağlıyor. (2023). https://www.barfas.com/blog-detay/kartli-gecis-sistemleri-tarihe-karisiyor-qr-gecis-sistemleri-kolaylik-ve-hiz-sagliyor. (26.05.2023).

Baykara, M. & Sherzad, A. (2020). Designing a securable smart home access control system using RFID cards. *Journal of Network Communications and Emerging Technologies (JNCET)*, 10(12), 1-12.

Boydak, A. B. (2017). İşyerlerinde Uygulanan Parmak İzli Giriş Kontrol Sistemine Hukuki Bakış. *Türkiye Adalet Akademisi Dergisi*, (30), 321-336.

Chen, N.-S., Teng, D., C.-E. & Lee, C.-H. (2010). 'AugmentingPaper-Based Reading Activitieswith Mobile Technology to Enhance Reading Comprehension. *The 6th IEEE Intenational Conference on Wireless*.

Computer Vision Zone
CV ZONE QR Reader. (2023). https://www.computervision.zone/courses/qr-reader/. (29.05.2022).

Cytron Technologies
Raspberry Pi Camera Face Detection Using OpenCV Python3. (2023). https://www.youtube.com/watch?v=hCGGKNqFO3w. (22.05.2023).

Cytron Technologies
Face Detection On Pi Camera Image Using OpenCV Python3 on Raspberry Pi. (2023).https://tutorial.cytron.io/2020/06/12/face-detection-on-pi-camera-image-using-opencv-python3-on-raspberry-pi/. (29.05.2022)

Ders Kodlayalım - YouTube Kanalı
Python / OpenCV Kamera açma / kamera üzerinden yüz tanıma. (2023). https://www.youtube.com/watch?v=LCphgx25UeQ. (22.04.2023).

Dou, Xue ve Li, Hairong. (2008). Creative Use of QR Codes in Consumer Communication.*International Journal of Mobile Marketing*, Vol. 3, Issue 2, p. 61-67.

Dönerçark, M. ve Tecim, V. (2020). Kurumsal Karar Destek Sistemlerinde Yapay Zekâ Kullanımı: Tasarım ve Uygulama. *Yönetim Bilişim Sistemleri Dergisi*, 6(2), 77-103.

Elektronikport Elektrik Elektronik Sistemleri San. ve Tic.
Raspbery Pi Dokunmatik Ekran Touch Screen 7 inch. (2023). https://www.elektronikport.com/urun/raspbery-pi-dokunmatik-ekran-touch-screen-7-inch. (18.06.2023).

Farnell Avnet Company
Raspberry Pi3 B. (2023). https://tr.farnell.com/raspberry-pi/raspberrypi3-modb-1gb/sbc-raspberry-pi-3-mod-b-1gb-ram/dp/2525225. (27.05.2023).

Geçiş Kontrol Merkezi. (2023).
https://www.geciskontrolmerkezi.com. (15.05.2023).

Genli, M. M. (2005). *Bina Otomasyon Sistemleri*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul: Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü.

Hampton, D., Peach, A. ve Rawlins, B. (2011). Reaching Mobile Userswith QR Code. *Kentucky Libraries*, 75 (2), 6-10.

IIENSTITU
SD Kart Ne İşe Yarar? (2023). https://www.iienstitu.com/blog/sd-kart-ne-ise-yarar. (12.06.2023).

İNT-EL Internatıonal Elektronik Sanayi ve Ticaret Limited Şirketi.
Raspberry Pi 3 ve 4 Uyumlu Kamera Modülü. (2023). https://www.direnc.net/raspberry-pi-kamera-modulu . (27.05.2023).

Karaca, S. (2010). *RFID teknolojisi ile anlık personel takip sistemi*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul: Maltepe ÜniversitesiFen Bilimleri Enstitüsü.

KAREL Elektronik Anonim Şirketi
Modern Güvenlik Sistemlerine Bakış: Kartlı Geçiş Sistemleri. (2023). https://www.karel.com.tr/blog/modern-guvenlik-sistemlerine-bakis-kartli-gecis-sistemleri. (16.06.2023).

Kolekar, S. D., Walekar, V. B., Patil, P. S., Mulani, A. O., & Harale, A. D. (2022). Password Based Door Lock System. *Int. J. of Aquatic Science*, 13(1), 494-501.

Komsek Elektronik Güvenlik Sistemleri Mühendislik İnşaat ve Reklam Tanıtım Hizmetleri Sanayi ve Ticaret Limited Şirketi.
Komsek Güvenlik Sistemleri, Kartlı Geçiş Sistemi Nedir ? (2023). https://www.komsek.com.tr/kartli-gecis-sistemi-nedir/. (14.05.2023)

Mamak, U., Konyar, M. Z., Solak, S. &Uçar, M. H. (2020). Gerçek zamanlı yüz tanıma tabanlı personel kontrol ve takip sistemi tasarımı. *Avrupa Bilim ve Teknoloji Dergisi*, (19), 497-504.

Merkepçi, M.&Özyazıcı, M.S. (2009). Parmak izine dayalı kapı kilit ve personel devam control sistemi. *Elektrik, Elektronik,Bilgisayar ve Biyomedikal Mühendislikleri Eğitim 4. Ulusal Sempozyumu*, 22-24 Ekim 2009, Eskişehir.

Murtaza's Workshop - Robotics and AI
How to Detect QR Code and Bar Code using OpenCV in Python + Project. (2023). https://www.youtube.com/watch?v=SrZuwM705yE. (28.06.2023)

Musayeva, G., &Yahyayev, M. (2014). Biyometrik Güvenlik Sistemleri. https://www.researchgate.net/publication/271210599_Biyometrik_Guvenlik. (15.05.2023).

Noma-Osaghae, E., Robert, O., Okereke, C., Okesola, O. J., &Okokpujie, K. (2017, December). Design and implementation of an iris biometric door Access control system. *In 2017 International conference on computational science and computational intelligence (CSCI)*. (pp. 590-593). IEEE.

Özkaya, N. & Sağıroğlu, Ş., (2006). Açık Anahtar altyapısı ve Biyometrik sistemler. *I. Ulusal Elektronik İmza Sempozyumu* (pp.283-290). Ankara, Türkiye

San Hlaing, N. N. & San Lwin, S. (2019). Electronic door lock using RFID and password based on arduino. *International Journal of Trend in Scientific Research and Development*, 3(2), 799-802.

Şamlı, R. & Yüksel, M. E. (2009). Biyometrik güvenlik sistemleri. *XI.Akademik Bilişim Konferansı Bildirileri*.11-13 Şubat 2009 Harran Üniversitesi, Şanlıurfa.

Perkotek Teknoloji Dış Tic. A.Ş.
Şifreli Kapı ve Şifreli Kapı Kilidi. (2023).https://www.perkotek.com/sifreli-kapi#:~:text=%C5%9Eifreli%20kap%C4%B1%20sistemleri%2C%20kap%C4%B1lar%C4%B1n%20kartlar,odalar%C4%B1nda%20da%20s%C4%B1k%C3%A7a%20tercih%20edilmektedir. (15.05.2023).

Pehlivanoğlu, M. K. & Nevcihan, D. U. R. U. (2016). Üniversite Öğrencilerinin Devamlılığının Parmak İzi Okuyucu Cihaz Kullanılarak İzlenmesi. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 8(2), 9-16.

Raspberry Pi Foundation
What is a Raspberry Pi?. (2023). https://www.raspberrypi.org/help/what-%20is-a-raspberry-pi/. (09.06.2023).

Robocombo Teknoloji Ürünleri San. Tic. Ltd. Şti.
Raspberry Pi Kamera Modülü V1.3 (5MP, 1080p). (2023). https://www.robocombo.com/Raspberry-Pi-Kamera-Modulu,PR-79.html. (27.05.2023).

Robolink Teknoloji Elektronik Medikal Mühendislik İnşaat Danışmanlık Yazılım Sanayi ve Tic.Ltd.Şti
Raspberry Pi 7 inch Resmi Dokunmatik Ekran. (2023). https://www.robolinkmarket.com/raspberry-pi-7-inch-resmi-dokunmatik-ekran. (12.06.2023).

Robotistan Elektronik Ticaret A.Ş.
Raspberry Pi 3 -Temel Ayarlar. (2023). https://www.youtube.com/watch?v=TlEDZ0KLzM4. (16.01.2023).

Robotistan Elektronik Ticaret A.Ş.
Raspberry Pi'ye Uzaktan Bağlantı Nasıl Yapılır? (SSH, VNC, TTL). (2023).https://www.youtube.com/watch?v=FxHzeBQFUhA. (14.04.2023)

Robotistan Elektronik Ticaret A.Ş.
SanDisk 16 GB microSDHC Hafıza Kartı Class10. (2023). https://www.robotistan.com/sandisk-16gb-microsdhc-hafiza-karti-class10-48mbsn-okuma-hizi-kart-adaptorlu. (14.06.2023).

QAR Akıllı Menü Sistemleri
QR Kod Oluşturucu. (2023). https://www.karekod.org/qr-kod-olusturucu/. (22.05.2023).
Tecim,V. (2023).*YönetimBilişimSistemleri(YBS).*https://vahaptecim.com.tr/yonetim-bilisim-sistemleri/, (12.06.2023).

Tom's Hardware
How to Train your Raspberry Pi for Facial Recognition.(2023). https://www.tomshardware.com/how-to/raspberry-pi-facial-recognition. (12.04.2023)

Türk, F., & Lüy, M. (2021). Gömülü Sistemler ve Mühendislikte Uygulama Alanları. *International Journal of Engineering Research & Development (IJERAD)*, 13(3).

Wahyudi, W. A. &Syazilawati, M. (2007). Intelligent voice-based door Access control system using adaptive-network-based fuzzy inference systems (ANFIS) for building security. *Journal of ComputerScience*, 3(5), 274-280.

Yasin Akün- Youtube Channel
Yüz Tanıma ile Kapı Kontrolü/ Raspberry Pi 3. (2023). https://www.youtube.com/watch?v=-ftvZBKpKes. (04.05.2023).

Yazılım Bilişim
Python Tkinter Örnekleri. (2023). https://www.yazilimbilisim.net/python/python-tkinter-ornekleri/. (18.04.2023).