



**T.C.
BATMAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ ANABİLİM DALI**

YÜKSEK LİSANS TEZİ

**YASAL DELİL NİTELİĞİ TAŞIYAN KAMERA ENTEGRE
EDİLMİŞ ERİŞİM KONTROL CİHAZININ TASARIMI VE
YAZILIMININ GELİŞTİRİLMESİ**

Raif SİME

**Ağustos-2024
BATMAN**

**T.C.
BATMAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ ANA BİLİM DALI**

YÜKSEK LİSANS TEZİ

**YASAL DELİL NİTELİĞİ TAŞIYAN KAMERA ENTEGRE
EDİLMİŞ ERİŞİM KONTROL CİHAZININ TASARIMI VE
YAZILIMININ GELİŞTİRİLMESİ**

Raif SİME

**Danışman
Prof. Dr. Necmettin SEZGİN**

**Ağustos-2024
BATMAN**

TEZ KABUL VE ONAYI

Raif SİME tarafından hazırlanan “Yasal Delil Niteliği Taşıyan Kamera Entegre Edilmiş Erişim Kontrol Cihazının Tasarımı ve Yazılımının Geliştirilmesi” adlı tez çalışması 29/08/2024 tarihinde aşağıdaki jüri tarafından oy birliği ile Batman Üniversitesi Fen Bilimleri Enstitüsü Bilgi Teknolojileri Anabilim Dalı’nda YÜKSEK LİSANS olarak kabul edilmiştir.

Jüri Üyeleri

İmza

Başkan

Prof. Dr. Necmettin SEZGİN

.....

Danışman

Prof. Dr. Necmettin SEZGİN

.....

Üye

Doç. Dr. Melih KUNCAN

.....

Üye

Doç. Dr. Yılmaz KAYA

.....

Yukarıdaki sonucu onaylarım.

Dr. Öğr. Üyesi Ömer Murat ÖTER
Lisansüstü Eğitim Enstitüsü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

İmza

Raif SİME

Tarih: 29.08.2024

ÖZET

YÜKSEK LİSANS TEZİ

YASAL DELİL NİTELİĞİ TAŞIYAN KAMERA ENTEGRE EDİLMİŞ ERİŞİM KONTROL CİHAZININ TASARIMI VE YAZILIMININ GELİŞTİRİLMESİ

Raif SİME

**Batman Üniversitesi Lisansüstü Eğitim Enstitüsü
Bilgi Teknolojileri Ana Bilim Dalı**

Danışman: Prof. Dr. Necmettin SEZGİN

2024, 42 Sayfa

Jüri

Prof. Dr. Necmettin SEZGİN

Doç. Dr. Yılmaz KAYA

Doç. Dr. Melih KUNCAN

Bu tez çalışması, kameralı bir kartlı geçiş sistemi tasarımı, uygulanması ve değerlendirilmesini kapsamaktadır. Güvenlik ve izleme alanında önemli bir yer tutan bu sistemler, giriş ve çıkışların kontrolünü sağlayarak güvenliği artırmakta ve izleme imkânı sunmaktadır. Bu çalışmada, NFC kart okuyucu (RC522 modülü), kamera modülü ve Raspberry Pi kullanılarak entegre bir geçiş kontrol sistemi geliştirilmiştir. Sistem tasarımında, donanım entegrasyonu ve yazılım geliştirilmesi başarıyla gerçekleştirilmiştir. Python programlama dili ve OpenCV kütüphanesi kullanılarak yüz tanıma işlemleri yapılmış, PostgreSQL veri tabanı ile verilerin güvenli bir şekilde saklanması sağlanmıştır. Laravel yardımı ile merkezi yönetim yazılımı geliştirilmiştir. Tasarımda kullanılan JSON formatında veri aktarımı, veri entegrasyonunu kolaylaştırmış ve sistemin farklı bileşenleri arasında uyumlu veri iletişimi sağlanmıştır.

Yapılan performans ve güvenilirlik testleri, sistemin yüksek doğruluk oranlarına sahip olduğunu, verilerin güvenli bir şekilde saklandığını ve zaman damgası ile veri bütünlüğünün sağlandığını göstermiştir. Elektronik delillerin geçerliliği ve güvenilirliği, 5651 sayılı yasa ve ilgili düzenlemeler çerçevesinde değerlendirilmiş ve sistemin hukuki gereksinimleri karşıladığı doğrulanmıştır. Kullanıcı deneyimini artırmak amacıyla SSH ve web arayüzü üzerinden yönetim özellikleri geliştirilmiş, kullanıcılar sistem ayarlarını kolaylıkla değiştirebilmiş, geçiş kayıtlarını görüntüleyebilmiş ve sistem durumunu izleyebilmiştir. Kullanıcı arayüzlerinin kullanılabilirliği test edilmiş ve kullanıcı dostu olduğu görülmüştür. Test kullanıcılarından alınan geri bildirimler doğrultusunda yapılan iyileştirmeler, sistemin kullanılabilirliğini ve verimliliğini artırmıştır.

Sonuç olarak, bu tezde geliştirilen kameralı kartlı geçiş sistemi, güvenilir, etkili ve kullanıcı dostu bir çözüm sunmakta ve güvenlik alanında önemli bir katkı sağlamaktadır. Sistem, gerçek dünya uygulamaları için uygun olup, güvenlik ve izleme süreçlerinde etkin bir şekilde kullanılabilir niteliktedir. Gelecekte, yapay zeka ve makine öğrenimi teknolojilerinin entegrasyonu ile sistemin daha da geliştirilebileceği ve yüz tanıma algoritmalarının doğruluk oranlarının artırılacağı öngörülmektedir. Ayrıca, Nesnelerin İnterneti (IoT) teknolojileri ile sistemlerin entegrasyonu sayesinde daha kapsamlı ve bütüncül bir güvenlik çözümü sunabileceği öngörülmektedir. Söz konusu çalışma, hem teknik hem de hukuki gereksinimleri karşılayarak, güvenlik açısından yüksek standartlarda bir çözüm sunmaktadır.

Anahtar Kelimeler: Kameralı Kartlı Geçiş Sistemi, Yüz Tanıma, NFC Kart Okuyucu, Raspberry Pi, Güvenlik ve İzleme, Zaman Damgası

ABSTRACT

MS THESIS

DESIGN AND SOFTWARE DEVELOPMENT OF A CAMERA-INTEGRATED ACCESS CONTROL DEVICE WHICH HAS LEGAL EVIDENCE QUALIFICATIONS

Raif SİME

Batman University Graduate Education Institute

Department of Information Technologies

Advisor: Prof. Dr. Necmettin SEZGİN

2024, 42 Pages

Jury

Prof. Dr. Necmettin SEZGİN

Assoc. Prof. Dr. Yılmaz KAYA

Assoc. Prof. Melih KUNCAN

This thesis focuses on the design, implementation, and evaluation of a camera-based access control system. These systems play a significant role in security and surveillance by controlling and monitoring entries and exits, thereby enhancing security and providing monitoring capabilities. In this study, an integrated access control system using an NFC card reader (RC522 module), a camera module, and a Raspberry Pi has been developed. The system design successfully integrates hardware components and develops software components. Facial recognition processes have been performed using the Python programming language and the OpenCV library, while data has been securely stored using a PostgreSQL database. A central management software has been developed using the Laravel framework. Data transfer in JSON format has facilitated data integration and ensured compatible data communication between different system components.

Performance and reliability tests have shown that the system achieves high accuracy rates, securely stores data, and ensures data integrity with timestamping. The validity and reliability of electronic evidence have been evaluated within the framework of Law No. 5651 and relevant regulations, confirming that the system meets legal requirements. To enhance user experience, management features have been developed through SSH and web interfaces, allowing users to easily change system settings, view access logs, and monitor system status. Usability tests have shown that user interfaces are user-friendly. Improvements made based on feedback from test users have increased the system's usability and efficiency.

In conclusion, the camera-based access control system developed in this thesis offers a reliable, effective, and user-friendly solution, making a significant contribution to the field of security. The system is suitable for real-world applications and can be effectively used in security and surveillance processes. It is anticipated that the system can be further developed in the future with the integration of artificial intelligence and machine learning technologies, improving the accuracy of facial recognition algorithms. Additionally, integrating the system with Internet of Things (IoT) technologies can provide a more comprehensive and holistic security solution. This study offers a high-standard solution in terms of security by meeting both technical and legal requirements.

Keywords: Camera-Based Access Control System, Facial Recognition, NFC Card Reader, Raspberry Pi, Security and Surveillance, Time Stamp

ÖNSÖZ

Bu tez çalışması, kameralı kartlı geçiş sistemlerinin tasarımı, uygulanması ve değerlendirilmesi üzerine odaklanmıştır. Bu süreçte, güvenlik ve izleme alanında önemli katkılar sağlayan bir sistem geliştirilmiş ve başarıyla uygulanmıştır.

Tez çalışmam boyunca bana akademik desteğini esirgemeyen kıymetli danışmanım Prof. Dr. Necmettin SEZGİN' hocama ve tüm çalışma süresince desteklerini esirgemeyen, bilgi ve deneyimlerini paylaşan değerli hocam Fikri AĞGÜN'e en içten teşekkürlerimi sunmak istiyorum. Kıymetli hocalarımla rehberliği ve teşvikleri, bu çalışmanın her aşamasında bana yol göstermiş ve başarıyı mümkün kılmıştır.

Ayrıca, bu çalışmanın gerçekleşmesinde emeği geçen tüm arkadaşlarıma ve aileme destekleri için teşekkür ederim. Onların sabrı, anlayışı ve teşviki, tez çalışmam boyunca motivasyonumu yüksek tutmamı sağlamıştır.

Bu tezin, güvenlik ve izleme sistemleri alanında çalışan araştırmacılar ve uygulayıcılar için faydalı olmasını diliyorum. Çalışmamın, gelecekteki araştırmalara ve uygulamalara katkıda bulunmasını umuyorum.

Saygılarımla,

Raif SİME
BATMAN-2024

İÇİNDEKİLER

ÖZET	iv
ABSTRACT.....	v
ÖNSÖZ	vi
İÇİNDEKİLER	vii
ŞEKİLLER DİZİNİ	ix
1. GİRİŞ.....	1
1.1. Kameralı Kartlı Geçiş Sistemlerinin Önemi	2
1.2. Amaç	3
1.3. Kapsam.....	4
1.3.1. Teknik Bileşenler ve Entegrasyon	4
1.3.2. Yazılım Geliştirme ve Uygulama	4
1.3.3. Hukuki ve Yasal Düzenlemeler	5
1.3.4. Çevrimiçi ve Çevrimdışı Çalışma Modları:.....	5
1.3.5. Kullanıcı Deneyimi ve Yönetim	5
1.3.6. Gelecekteki Gelişmeler ve Teknolojik Yenilikler	5
2. KAYNAK ARAŞTIRMASI.....	7
3. MATERYAL VE YÖNTEM	11
3.1. Materyal	11
3.1.1. Donanım Bileşenleri	11
3.1.2. Yazılım Bileşenleri	12
3.1.3. Geliştirme ve Test Ortamı	13
3.2. Yöntem.....	14
3.2.1. Geliştirme ve Test Ortamı	14
3. ÇALIŞMANIN SONUÇLARI VE TARTIŞMA.....	19
5. SONUÇLAR VE ÖNERİLER	21
5.1 Sonuçlar	21
5.2 Öneriler	22
KAYNAKLAR	25
ÖZGEÇMİŞ.....	31

SİMGELER VE KISALTMALAR

Simgeler

Simgeleri yazmaya buradan başlayınız ve yazım kılavuzunda belirtildiği şekilde düzenleyiniz. Simgelerin bitiminden sonra, kısaltmalar başlığından önce bir satır boşluk bırakınız.

Kısaltmalar

Kısaltma	Açıklama
NFC	Yakın alan iletişimi (Near Field Communication) olarak bilinen kablosuz bir teknolojidir.
CDP	Yöneticilerin, uzak veya yerel olarak bağlı cihazlar hakkında bilgi toplamasına yardımcı olması için Cisco tarafından tasarlanan, tescilli bir protokoldür.
SSH	Kullanıcılara sunucularını internet üzerinden kontrol etmesini ve düzenlemesini sağlayan uzak yönetim protokolüdür.
SPI	Cihazlar arasında iletişim kurmak için kullanılan bir senkron seri iletişim protokolüdür.
CAD	Bilgisayar destekli tasarım anlamına gelir ve tasarımlar ve planlar oluşturmaya yardımcı olmak için bilgisayarları kullanma eylemini ifade eder.
JSON	JavaScript Object Notation, basit veri yapılarını temsil etmek için tasarlanmış bağımsız bir veri değişim formatıdır.
IP	Bir cihazın internete bağlı olduğu yerin sayısal bir temsildir
MVC	Model-View-Controller, verinin farklı görselleştirme yöntemleriyle kullanıcıya sunulduğu, uygulamaların geliştirilmesinde kullanılan bir yazılım kalıbıdır.
ORM	İlişkisel veri tabanı ile uygulamamız arasında bir köprü görevi gören, ilişkileri ve nesneleri yönetmek için kullanılan bir tekniktir.
CSRF	Web siteleri arası istek sahtekârlığını engellemeye yarayan mekanizmadır.
HTTP	Ağ üzerinden web sayfalarının görüntülenmesini sağlayan protokoldür.
KVKK	Kişisel verileri koruma kanunu
SCI	Seri iletişim kamera portu
IOT	Internet of Things (Nesnelerin İnterneti)
RFID	İngilizce Radio Frequency Identification kelimelerinin baş harflerinden oluşan bir kimliklendirme sistemidir.

ŞEKİLLER DİZİNİ

Şekil 3.1. RC522 RFID modülü.....	12
Şekil 3.2. Donanım bileşenleri bağlantı şeması	15
Şekil 3.3. 3D Yazıcı ile tasarlanmış cihaz muhafazası prototipi	16
Şekil 3.4. Veri akış şeması	17

1. GİRİŞ

Yasal delil niteliği taşıyan kamera entegre edilmiş erişim kontrol cihazlarının tasarımı ve yazılımının geliştirilmesi, çeşitli nedenlerden dolayı gereklidir. İlk olarak, kontrol mekanizmaları güvenlik açısından büyük önem taşır. Hassas bölgelerde, giriş ve çıkışların kontrol edilmesi ve izlenmesi, bu alanların korunması için kritik bir rol oynar. Ayrıca, olayların kayıt altına alınması, güvenlik ihlallerinin, hırsızlıkların veya vandalizm gibi durumların ardından yapılacak soruşturmalar için değerli kanıtlar sağlayacaktır.

Kamera ve kartlı geçiş sistemleri, güvenlik ve izleme alanında önemli bir rol oynamaktadır. Bu sistemler, giriş ve çıkışların kontrolünü sağlayarak güvenliği artırır ve izleme imkanı sunar. Özellikle, dijital dünyada güvenlik ve delil toplama konusundaki gereksinimler, bu tür sistemlerin önemini daha da artırmaktadır (Özkaya, 2021; Henkoğlu, 2020; Nieto, Roman ve Lopez, 2016; Ryu, Moon ve Park, 2018). Türkiye'de, 5651 sayılı yasa gereği, bu sistemlerin yasal delil niteliği taşıması ve güvenilirliği kritik öneme sahiptir (İnternet Ortamında Yapılan Yayınların Düzenlenmesi, 2007; Altıparmak ve Akdeniz, 2017). Elektronik delillerin geçerliliği ve güvenilirliği, hukuki süreçlerde büyük önem taşır (Casey, 2011; Kasper ve Laurits, 2016; SEgate, 2021). Bu nedenle, zaman damgası uygulamaları gibi teknolojiler, dijital delillerin güvenilirliğini artırmak için kullanılmaktadır (Haber ve Stornetta, 1991; Birleşmiş Milletler, Uluslararası Ticaret Hukuku Komisyonu, 2001; Elektronik İmza Kanunu, 2004; Sağlık, 2022, Sağlık, 2024).

Yasal gereksinimler ve uyumluluk açısından da bu tür sistemlere ihtiyaç duyulmaktadır. Kamera kayıtları, hukuki süreçlerde delil olarak kullanılabilir ve mahkemelerde olayların ispatlanmasında önemli bir rol oynar (Horsman, 2021; Hellwig, 2021; Atılgan ve Samet, 2018). Birçok sektörde, belirli güvenlik standartlarına uyum sağlamak zorunludur ve bu standartlar, kamera kayıtlarının belirli sürelerle saklanması ve yetkisiz erişimlerin önlenmesini gerektirir. Verimlilik ve işlevsellik açısından bakıldığında, bu sistemler giriş ve çıkışların otomatik olarak kontrol edilmesini sağlar ve manuel denetim ihtiyacını azaltır. Böylece işletmelerin verimliliği artar. Ayrıca, erişim kontrol cihazları, kimlerin, ne zaman, nereye giriş yaptığını izleyebilir ve bu bilgiler, personel hareketlerinin yönetilmesinde ve güvenlik politikalarının uygulanmasında yardımcı olur (Canoğlu, 2018). Teknolojik gelişmeler de bu ihtiyacı artırmaktadır. Kamera entegre edilmiş erişim kontrol cihazları, diğer

güvenlik ve bina yönetim sistemleri ile entegre çalışabilir, bu da genel güvenlik yapısının daha etkili ve koordine bir şekilde yönetilmesine olanak tanır (Dudeja, vd. 2016; Gu, vd. 2013; Gupta, vd. 2021). Kameraların varlığı, potansiyel suçlular üzerinde caydırıcı bir etki yaratır ve insanlar kayıt altına alındıklarını bildiklerinde yasa dışı veya uygunsuz davranışlardan kaçınma eğiliminde olurlar (Arslan, 2015; Alshammari ve Rawat, 2019). Çalışanlar ve ziyaretçiler, güvenli bir ortamda olduklarını bilerek kendilerini daha güvende hissederler, bu da genel işyeri memnuniyetini ve verimliliğini artırabilir (Van Rompay, Vonk ve Fransen, 2009). Bu nedenlerden dolayı, yasal delil niteliği taşıyan kamera entegre edilmiş erişim kontrol cihazlarının tasarımı ve yazılımının geliştirilmesi büyük bir ihtiyaçtır.

Kameralı kartlı geçiş sistemlerinin entegrasyonu, çeşitli teknolojik bileşenlerin bir araya getirilmesini gerektirir. NFC kartlarını okumak için RC522 modülünün SPI protokolü üzerinden kullanılması, kamera üzerinden resim çekmek için SCI portunun kullanılması ve yüz tanıma işlemleri için OpenCV kütüphanesinin kullanılması gibi teknik çözümler bu sistemlerin temel yapı taşlarını oluşturur (Wallace, Richardson ve Donat, 2021; Van Rossum ve Drake, 1995; Bradski, 2000). Ayrıca, her yeni eklenen kameralı kart okuyucunun discovery protokolü (CDP) kullanarak sistem bilgilerini merkezi yönetim sunucusuna göndermesi, sistemin yönetimini ve izlenmesini kolaylaştırır (Rao ve Sudheer, 2020).

Geliştirilen bir sistemde, verilerin güvenli ve düzenli bir şekilde yönetilmesi ve saklanması önemlidir. JSON formatında veri aktarımı, Raspberry Pi üzerinde Python ile uygulama geliştirilmesi, yönetim yazılımının Laravel ile oluşturulması ve veri tabanı olarak PostgreSQL kullanılması bu sürecin önemli bileşenlerindendir (Droettboom, 2015; Richardson ve Wallace, 2014; Subecz, 2021; Obe ve Hsu, 2017). Ayrıca, cihazın durumu hakkında sürekli bilgi gönderimi, SSH ve web arayüzü üzerinden yönetim imkanları, sistemin esnekliğini ve yönetilebilirliğini artırır (Vani ve NithyaPriya, 2014).

1.1. Kameralı Kartlı Geçiş Sistemlerinin Önemi

Kameralı kartlı geçiş sistemleri, güvenlik açısından önemli bir rol oynar. Bu sistemler, belirli alanlara giriş çıkışların kontrol altında tutulmasını ve izlenmesini sağlar. Güvenlik personelinin müdahale gereksinimini azaltarak, olayların kayıt altına alınmasını mümkün kılar (Campion ve Campion, 2018). İzleme sistemleri, olayların

geriye dönük incelenmesine olanak tanıyarak güvenlik olaylarının analiz edilmesini sağlar (Arante, vd., 2018).

Türkiye'de, 5651 sayılı kanun, internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi amacıyla yürürlüğe girmiştir. Bu kanun, elektronik delillerin geçerliliğini ve güvenilirliğini sağlamak için çeşitli düzenlemeler içerir (İnternet Ortamında Yapılan Yayınların Düzenlenmesi, 2007). TÜBİTAK tarafından sağlanan zaman damgası, bu delillerin yasal geçerliliğini artırmak için kullanılır (Yalçın, 2015, Kamu Sertifikasyon Merkezi, t.y.). Elektronik delillerin hukuki geçerliliği, yargı süreçlerinde doğruluk ve güvenilirlik açısından büyük önem taşır (Ryan ve Shpantzer, 2022).

1.2. Amaç

Bu tezin amacı, kameralı kartlı geçiş sistemlerinin tasarımını, uygulanmasını ve işlevselliğini detaylı bir şekilde incelemektir. Tez kapsamında, güvenlik ve izleme alanında önemli bir yer tutan bu sistemlerin, hem teknik hem de hukuki yönleriyle ele alınması hedeflenmiştir. Ayrıca, sistemin entegre edildiği teknolojilerin ve yöntemlerin açıklanarak, kullanıcı dostu ve güvenilir bir çözüm sunulması amaçlanmıştır. Bu çalışmada, kartlı geçiş sisteminin tüm bileşenlerinin nasıl tasarlandığını ve uygulandığını detaylandırmayı amaçlanmıştır. NFC kart okuyucu (RC522 modülü), kamera modülü ve kontrol ünitesinin entegrasyonu ile ilgili teknik detaylar, yazılım ve donanım düzeyinde ele alınmaktadır. Sistem tasarımında kullanılacak olan yazılım dili, donanım bileşenleri ve protokoller hakkında bilgi verilecek, bu bileşenlerin birbirleriyle nasıl iletişim kurduğu açıklanacaktır.

Ayrıca hukuki açıdan 5651 sayılı yasa ve ilgili düzenlemeler çerçevesinde, sistemin hukuki geçerliliği ve güvenilirliği değerlendirilecektir. Bu bağlamda, TÜBİTAK zaman damgasının kullanımı, dijital delillerin geçerliliği ve güvenilirliği konuları ele alınarak, sistemin yasal standartlara uygunluğu incelenecektir. Tez, sistemin teknoloji açısından nasıl geliştirilebileceğini ve mevcut teknolojilerle nasıl entegre edilebileceğini araştıracaktır. NFC kart okuyucu ve kamera modülünün entegrasyonu, veri iletim protokolleri, veri tabanı yönetimi ve yüz tanıma teknolojilerinin kullanımı detaylı olarak ele alınacaktır. Bu kapsamda, Python ve Laravel gibi yazılım dillerinin kullanımı, PostgreSQL veri tabanının yönetimi ve JSON veri formatı ile veri aktarım yöntemleri incelenecektir.

Sistemin çevrimiçi ve çevrimdışı çalışma modlarının avantajları ve dezavantajları değerlendirilecektir. Online modda veri aktarımının anlık yapılabilmesi, offline modda ise verilerin cihazda saklanarak daha sonra merkezi sunucuya gönderilmesi süreçleri incelenecektir. Bu modların sistem performansı ve güvenilirliği üzerindeki etkileri analiz edilecektir. Sistem kullanıcılarının deneyimini artırmak amacıyla SSH ve web arayüzü üzerinden yönetim özellikleri geliştirilecektir.

Bu çalışma, yukarıda belirtilen konuları detaylı bir şekilde ele alarak, kartlı geçiş sistemlerinin hem teknik hem de hukuki boyutlarıyla daha güvenilir, etkili ve kullanıcı dostu hale getirilmesini amaçlamaktadır. Ayrıca, gelecekteki teknolojik gelişmeler doğrultusunda bu sistemlerin nasıl geliştirilebileceği konusunda öneriler sunmayı hedeflemektedir.

1.3. Kapsam

Bu tez çalışması, kameralı kartlı geçiş sistemlerinin teknik, hukuki ve uygulama boyutlarını kapsayan geniş bir inceleme yapmayı amaçlamaktadır. Bu kapsamda ele alınacak konular ve detaylar aşağıda sıralanmıştır:

1.3.1. Teknik bileşenler ve entegrasyon

Kartlı geçiş sisteminin temel teknik bileşenleri ve bu bileşenlerin entegrasyonu ele alınacaktır. Özellikle NFC kart okuyucu (RC522 modülü), kamera modülü, Raspberry Pi kontrol ünitesi ve bu bileşenlerin birbirleriyle nasıl entegre edildiği detaylandırılacaktır. Bu bölümde ayrıca kullanılan donanım ve yazılım bileşenlerinin özellikleri, bağlantı ve iletişim protokolleri gibi teknik detaylar da incelenecektir.

1.3.2. Yazılım geliştirme ve uygulama

Tezde, sistemin yazılım kısmı da detaylı bir şekilde ele alınacaktır. Python programlama dili ile Raspberry Pi üzerinde geliştirilen uygulamalar, NFC kart okuyucunun ve kamera modülünün nasıl kontrol edildiği ve veri işleme süreçleri açıklanacaktır. Ayrıca, merkezi kontrol ve yönetim yazılımı olarak kullanılan Laravel

Framework(çerçeve) üzerinde yapılan geliřtirmeler, PostgreSQL veri tabanı yönetimi ve JSON veri formatı ile veri aktarımı konuları detaylandırılacaktır.

1.3.3. Hukuki ve yasal düzenlemeler

Ülkemizde biliřim alanında kullanılmakta olan 5651 sayılı yasa ve ilgili diğerk yasal düzenlemeler kapsamında, kameralı kartlı geçiř sistemlerinin hukuki geçerliliğı ve güvenilirliğı incelenecektir. TÜBİTAK zaman damgasının kullanımı ve dijital delillerin adli süreçlerde nasıl kullanıldığı tartışılacaktır. Ayrıca, Kiřisel Verilerin Korunması Kanunu (KVKK) çerçevesinde, sistemin veri güvenliğı ve mahremiyet konularına uygunluğı değerkendirilecektir.

1.3.4. Çevrimiçi ve çevrimdışı çalışma modları:

Sistemin online ve offline çalışma modlarının avantajları ve dezavantajları üzerinde durulacaktır. Online modda veri aktarımının gerçek zamanlı yapılabilmesi, offline modda ise verilerin cihazda saklanarak daha sonra merkezi sunucuya gönderilmesi süreçleri detaylandırılacaktır. Her iki çalışma modunun sistem performansı, veri güvenliğı ve kullanıcı deneyimi üzerindeki etkileri incelenecektir.

1.3.5. Kullanıcı deneyimi ve yönetim

Sistem kullanıcılarının deneyimini artırmak amacıyla geliştirilen özellikler bu bölümde ele alınacaktır. SSH ve web arayüzü üzerinden sistem yönetimi, kullanıcıların sistem ayarlarını değıştirmesi, geçiř kayıtlarını görüntülemesi ve sistem durumunu izlemesi için sunulan arayüzler detaylandırılacaktır. Ayrıca, sesli uyarı mekanizması gibi kullanıcı deneyimini iyileřtiren özellikler de incelenecektir.

1.3.6. Gelecekteki gelişmeler ve teknolojik yenilikler

Tasarlanmış olan sistemin gelecekte nasıl geliştirilebileceğı ve hangi yeni teknolojik yeniliklerin uygulanabileceğı tartışılacaktır. Yapay zeka ve makine öğrenimi teknolojilerinin yüz tanıma sistemlerine entegrasyonu, Nesnelerin İnterneti (IoT) teknolojileri ile sistemlerin entegrasyonu gibi konular ele alınacaktır. Ayrıca,

sistemlerin güvenlik, performans ve kullanıcı deneyimi açısından nasıl iyileştirilebileceği konusunda öneriler sunulacaktır. Bu kapsam dahilinde, tezimiz kameralı kartlı geçiş sistemlerinin tasarımı, uygulaması, hukuki boyutları ve gelecekteki gelişmeleri hakkında geniş bir perspektif sunmayı hedeflemektedir. Sistemlerin güvenilir, etkili ve kullanıcı dostu hale getirilmesi için gerekli olan tüm teknik ve hukuki detaylar incelenecek ve öneriler sunulacaktır.

2. KAYNAK ARAŞTIRMASI

Bu tez çalışmasında, kameralı kartlı geçiş sistemlerinin tasarımı, uygulanması ve değerlendirilmesi için geniş bir literatür araştırması yapılmıştır. Aşağıda, bu konuyla ilgili temel literatürler ve önceki çalışmalar detaylı bir şekilde incelenmiş, çalışmanın teorik altyapısını oluşturan kaynaklar özetlenmiştir.

Kameralı kartlı geçiş sistemleri, güvenlik ve izleme alanında kritik bir rol oynar. Bu sistemler, belirli alanlara giriş ve çıkışların kontrolünü sağlayarak güvenliği artırır ve izleme imkanı sunar. Marshall (2009), güvenlik sistemlerinin dijital forensik uygulamalarını ele alarak, bu tür sistemlerin güvenlik olaylarını tespit etme ve izleme açısından nasıl kullanıldığını detaylandırmıştır. Marshall, çalışmasında, "Dijital forensik uygulamalar, güvenlik sistemlerinin etkinliğini artırmak ve olayların doğru bir şekilde tespit edilmesi ve analiz edilmesi için kritik öneme sahiptir" ifadesine yer vermiştir. Landwehr (2001), kampüs güvenliği ve olayların yönetimi konularında bu sistemlerin önemini vurgulamaktadır. Landwehr, "Kampüs güvenlik sistemleri, öğrenci ve personelin güvenliğini sağlamak için kapsamlı bir izleme ve kontrol mekanizması sunar" diye belirtmiştir. Ayrıca, Casey (2011), güvenlik sistemlerinin hukuki boyutlarını ve elektronik delillerin adli süreçlerdeki rolünü incelemektedir. Casey, "Elektronik delillerin hukuki geçerliliği, adli süreçlerde delil bütünlüğünün korunması ve güvenilirliğin sağlanması açısından kritik öneme sahiptir" demektedir. Bu çalışmalar, kameralı kartlı geçiş sistemlerinin güvenlik ve izleme alanındaki önemini ve kullanımını desteklemektedir.

Yüz tanıma teknolojileri, modern güvenlik sistemlerinde kimlik doğrulama süreçlerinin ayrılmaz bir parçasıdır. Balaban (2015), derin öğrenme tekniklerinin yüz tanıma uygulamalarında nasıl kullanıldığını ve bu tekniklerin doğruluk oranlarını nasıl artırdığını açıklamaktadır. Teoh ve arkadaşları (2021), "Derin öğrenme algoritmaları, büyük veri kümelerinden öğrenerek yüz tanıma işlemlerinde yüksek doğruluk oranlarına ulaşmamızı sağlar" ifadesine yer vermektedir. Wang ve Li (2018), derin konvolüsyonel sinir ağlarının (CNN) görüntü tanıma performansını artırmadaki rolünü incelemiştir. Taigman ve arkadaşları (2014), "Konvolüsyonel sinir ağları, görüntü tanıma görevlerinde üstün performans göstererek birçok uygulamada devrim yaratmıştır" demektedir. Ayrıca, Ford ve Siraj (2014), yapay zeka tekniklerinin güvenlik uygulamalarında nasıl kullanılabileceğini ve bu teknolojilerin yüz tanıma sistemlerindeki etkisini tartışmaktadır. Murphy, "Yapay zeka, güvenlik uygulamalarında

otomatikleştirilmiş ve yüksek doğruluklu yüz tanıma sistemleri geliştirmek için büyük bir potansiyele sahiptir" diye belirtmektedir. Bu çalışmalar, yüz tanıma teknolojisinin güvenlik sistemlerinde kullanımını ve potansiyelini göstermektedir.

NFC (Yakın Alan İletişimi) teknolojisi, kartlı geçiş sistemlerinin temel bileşenlerinden biridir (Al-Ofeishat ve Al Rababah, 2012). Kumar ve Sharma (2019), NFC tabanlı sistemlerin tasarımı ve uygulanması üzerine kapsamlı bir inceleme sunmaktadır. Kumar ve arkadaşları (2021), "NFC teknolojisi, kısa mesafeli iletişim sağlama yeteneği ile güvenli ve hızlı kimlik doğrulama süreçleri sunar" ifadesini kullanmaktadır. RC522 NFC kart okuyucu modülü, düşük maliyeti ve yaygın erişilebilirliği nedeniyle bu tez çalışmasında tercih edilmiştir. Roland (2012), NFC teknolojisinin güvenlik sistemlerindeki kullanımını ve avantajlarını detaylandırmaktadır. Roland (2012), "NFC teknolojisi, kullanıcı dostu ve güvenilir bir kimlik doğrulama aracı olarak güvenlik sistemlerinde yaygın olarak kullanılmaktadır" demektedir. Bu çalışmalar, NFC teknolojisinin kartlı geçiş sistemlerindeki rolünü ve kullanımını desteklemektedir (Singh, Adzman ve Hassan, 2018; Thammarat, 2020).

Raspberry Pi, düşük maliyetli ve güçlü bir mini bilgisayar olarak, birçok güvenlik ve izleme uygulamasında kullanılmaktadır (Nguyen, vd., 2015; Monk 2022). Poyen (2019), Raspberry Pi'nin farklı uygulamalarda nasıl kullanılabileceğini ve donanım entegrasyonunun nasıl gerçekleştirileceğini detaylandırmaktadır. Maksimović ve diğerleri (2014), "Raspberry Pi, geniş bağlantı seçenekleri ve esnekliği ile çok çeşitli projelerde kullanılabilir ve kolayca entegre edilebilir" ifadesini kullanmaktadır. Donat ve Krause (2014), Raspberry Pi'nin Python programlama dili ile entegrasyonunu ve uygulama geliştirmedeki avantajlarını açıklamaktadır. Donat ve Krause (2014), "Python, Raspberry Pi ile birlikte kullanıldığında hızlı ve etkili uygulama geliştirme imkanı sunar" demektedir. Bu çalışmalar, Raspberry Pi'nin esnekliği ve geniş bağlantı seçenekleri nedeniyle donanım entegrasyonu için ideal bir platform olduğunu göstermektedir.

PostgreSQL, açık kaynaklı ve güçlü bir ilişkisel veri tabanı yönetim sistemidir. Schönig (2023), PostgreSQL'in veri yönetimi ve güvenlik özelliklerini kapsamlı bir şekilde ele almıştır. Kilavo, Mrutu ve Dudu (2023), "PostgreSQL, esnek veri modelleme ve güçlü sorgulama yetenekleri ile veri yönetimi ve güvenliği için ideal bir seçenektir" ifadesini kullanmaktadır. PostgreSQL'in esnekliği ve güçlü sorgulama yetenekleri, bu tez çalışmasında veri saklama ve yönetim için tercih edilmesinin nedenlerindendir. Jung ve diğerleri (2015), veri tabanı sistemlerinin performansını ve yönetimini

incelemektedir. Jung ve diğeri, "Veri tabanı sistemlerinin performansı, veri yönetimi süreçlerinin verimliliği ve güvenliği açısından kritik öneme sahiptir" demektedir. Bu çalışmalar, PostgreSQL'in veri tabanı yönetimi için neden uygun bir seçenek olduğunu desteklemektedir.

Laravel, modern web uygulamaları geliştirmek için kullanılan PHP tabanlı bir framework'tür (McCool, 2012). Laaziri ve diğeri (2019), Laravel'in temel özelliklerini ve avantajlarını açıklamaktadır. Laaziri ve diğeri, "Laravel, güçlü ORM yapısı, modüler tasarımı ve güvenlik özellikleri ile modern web uygulamaları geliştirmek için ideal bir çerçevedir" demektedir. Dockins (2017), Laravel'in tasarım desenleri ve en iyi uygulamalarını detaylandırmaktadır. Dockins, "Laravel, MVC yapısı ve güçlü özellikleri ile geliştiricilere esnek ve ölçeklenebilir uygulamalar geliştirme imkanı sunar" diye belirtmektedir. Laravel, MVC yapısı ve güçlü ORM özellikleri ile merkezi yönetim yazılımı geliştirmek için ideal bir seçimdir. Bu çalışmalar, Laravel'in web uygulama geliştirme süreçlerinde sağladığı avantajları göstermektedir.

5651 sayılı yasa ve ilgili düzenlemeler, elektronik delillerin hukuki geçerliliğini belirlemektedir (İnternet Ortamında Yapılan Yayınların Düzenlenmesi, 2007; Altıparmak ve Akdeniz, 2017). Rijavec ve Keresteš (2015), elektronik delillerin hukuki boyutlarını ve bu delillerin yargı süreçlerinde nasıl kullanıldığını detaylandırmaktadır. Rijavec ve Keresteš (2015), "Elektronik delillerin hukuki geçerliliği, adli süreçlerde delil bütünlüğünün korunması ve güvenilirliğin sağlanması açısından kritik öneme sahiptir" demektedir. TÜBİTAK tarafından sağlanan zaman damgası hizmetleri, elektronik delillerin güvenilirliğini artırmaktadır (Kamu Sertifikasyon Merkezi, t.y.). TÜBİTAK, "Zaman damgası, elektronik verilerin değişmezliğini ve bütünlüğünü sağlamak için kullanılan bir güvenlik önlemidir" ifadesine yer vermektedir (Tübitak Bilgem, 2022). Bu çalışmalar, elektronik delillerin yasal gereksinimlerini ve güvenilirliğini desteklemektedir.

Yapay zeka ve makine öğrenimi teknolojileri, güvenlik sistemlerinde yüz tanıma ve veri analizi süreçlerinde kullanılmaktadır. Saeed, Pejas ve Mosdorf (2007), yapay zeka tekniklerinin güvenlik uygulamalarında nasıl kullanılabileceğini ve bu teknolojilerin sistem performansını nasıl artırabileceğini açıklamaktadır. Mohammed (2013), "Yapay zeka, güvenlik uygulamalarında otomatikleştirilmiş ve yüksek doğruluklu yüz tanıma sistemleri geliştirmek için büyük bir potansiyele sahiptir" diye belirtmektedir. Glorot ve Bengio (2010), makine öğrenimi algoritmalarının yüz tanıma uygulamalarındaki başarılarını ve potansiyellerini tartışmaktadır. Glorot ve Bengio

(2010), "Makine öğrenimi, büyük veri kümelerinden öğrenerek yüz tanıma işlemlerinde yüksek doğruluk oranlarına ulaşmamızı sağlar" ifadesini kullanmaktadır. Bu çalışmalar, yapay zeka ve makine öğrenimi teknolojilerinin güvenlik sistemlerindeki kullanımını ve etkilerini göstermektedir.

IoT teknolojileri, güvenlik sistemlerinin diğer izleme ve kontrol sistemleri ile entegrasyonunu sağlamaktadır. Hassija ve diğerleri (2019), IoT'nin güvenlik uygulamalarındaki rolünü ve potansiyelini incelemektedir. Hassija ve diğerleri, "IoT, güvenlik sistemlerinde veri toplama, analiz ve paylaşma süreçlerini optimize ederek daha kapsamlı ve bütüncül çözümler sunar" demektedir. Balaji, Nathani ve Santhakumar (2019), IoT teknolojilerinin güvenlik sistemlerindeki kullanımını ve avantajlarını tartışmaktadır. Balaji, Nathani ve Santhakumar (2019), "IoT, çeşitli cihazların birbirleriyle iletişim kurarak entegre bir güvenlik ağı oluşturmasını sağlar" ifadesini kullanmaktadır. Hudson-Smith ve diğerleri (2021), IoT'nin veri toplama ve paylaşma süreçlerindeki etkisini açıklamaktadır. Hudson-Smith ve diğerleri (2021), "IoT, büyük veri analitiği ve gerçek zamanlı izleme imkanları sunarak güvenlik uygulamalarının etkinliğini artırır" diye belirtmektedir. Bu çalışmalar, IoT teknolojilerinin güvenlik sistemlerinde nasıl kullanılabileceğini ve entegrasyonun sağladığı avantajları göstermektedir.

Bu kaynak araştırması, kameralı kartlı geçiş sistemlerinin teknik, hukuki ve uygulama boyutlarıyla ilgili kapsamlı bir literatür incelemesi sunmaktadır. Bu çalışmalar, tezin teorik altyapısını oluşturmakta ve sistemin tasarımı ve uygulanmasında yol gösterici olmaktadır. Bu literatür araştırması, tezde ele alınan konuların bilimsel temellerini sağlamlaştırmakta ve çalışmanın geçerliliğini artırmaktadır.

3. MATERYAL VE YÖNTEM

3.1. Materyal

Bu tezin amacı doğrultusunda, kameralı kartlı geçiş sistemlerinin tasarımı, uygulanması ve değerlendirilmesi için çeşitli donanım ve yazılım bileşenleri kullanılmıştır. Bu bölümde, kullanılan tüm materyaller detaylı bir şekilde açıklanacaktır.

3.1.1. Donanım bileşenleri

3.1.1.1. Raspberry Pi

Raspberry Pi, bu tez çalışmasının merkezinde yer alan düşük maliyetli, küçük boyutlu bir bilgisayardır. Çalışmada, Raspberry Pi 4 Model B kullanılmıştır. Bu model, güçlü bir işlemci, yeterli RAM ve çeşitli giriş/çıkış portlarına sahip olması nedeniyle tercih edilmiştir.

3.1.1.2. RC522 NFC kart okuyucu

RC522 modülü, NFC (Yakın Alan İletişimi) kartlarını okumak için kullanılan bir RFID okuyucusudur. Bu modül, SPI (Serial Peripheral Interface) protokolü üzerinden Raspberry Pi'ye bağlanarak çalışmaktadır. RC522, düşük maliyeti ve yaygın kullanılabilirliği nedeniyle seçilmiştir.



Şekil 3.1. RC522 RFID Modülü

3.1.1.3. Kamera modülü

Raspberry Pi kamera modülü, geçiş sırasında fotoğraf çekmek için kullanılmıştır. Bu modül, yüksek çözünürlüklü görüntüler sağlayabilen ve Raspberry Pi'nin CSI (Camera Serial Interface) portuna bağlanabilen bir kameradır. Bu özellikler, yüz tanıma işlemleri için gerekli olan yüksek kaliteli görüntüleri sağlamakta önemli rol oynamaktadır.

3.1.1.4. SD Kart

Raspberry Pi işletim sistemi ve uygulamaların depolanması için kullanılan SD kart, tez çalışmasında kritik bir bileşendir. En az 16 GB kapasiteli bir SD kart kullanılmıştır.

3.1.1.5. Güç kaynağı

Raspberry Pi ve bağlı bileşenlerin düzgün çalışması için 5V 3A kapasiteli bir güç kaynağı kullanılmıştır.

3.1.1.6. Diğer aksesuarlar

Tez çalışmasında ayrıca çeşitli kablolar, breadboard, jumper kabloları ve bağlantı elemanları gibi yardımcı malzemeler kullanılmıştır.

3.1.2. Yazılım bileşenleri

3.1.2.1. Raspberry Pi OS

Raspberry Pi üzerinde çalışan Raspberry Pi OS, bu tez çalışmasının temel işletim sistemidir. Bu işletim sistemi, Linux tabanlı olup, Raspberry Pi donanımıyla tam uyumlu çalışmaktadır.

3.1.2.2. Python

Tez çalışması boyunca kullanılan ana programlama dili Python'dur. Python, geniş kütüphane desteği ve kolay anlaşılır syntax'ı ile donanım kontrolü ve veri işleme işlemlerini kolaylaştırmaktadır. Tez çalışmasında, RC522 modülünü kontrol etmek, kamera ile fotoğraf çekmek ve verileri işlemek için çeşitli Python kütüphaneleri kullanılmıştır.

3.1.2.3. OpenCV

Yüz tanıma ve görüntü işleme işlemleri için OpenCV (Open Source Computer Vision Library) kütüphanesi kullanılmıştır. OpenCV, güçlü ve geniş kapsamlı görüntü işleme fonksiyonları sunar.

3.1.2.4. PostgreSQL

Tez çalışmasının veri tabanı yönetim sistemi olarak PostgreSQL kullanılmıştır. PostgreSQL, açık kaynaklı, güçlü ve esnek bir ilişkisel veri tabanı yönetim sistemidir. Geçiş bilgileri ve zaman damgası verileri bu veri tabanında saklanmıştır.

3.1.2.5. Laravel

Merkezi kontrol ve yönetim yazılımı olarak Laravel PHP çerçevesi kullanılmıştır. Laravel, MVC (Model-View-Controller) yapısı, güçlü ORM (Eloquent), güvenlik özellikleri ve geniş kütüphane desteği ile bu tez çalışmasında tercih edilmiştir.

3.1.2.6. JSON

Veri aktarımı ve entegrasyonu için JSON (JavaScript Object Notation) formatı kullanılmıştır. JSON, veri değişimi için hafif, dil bağımsız ve kolay anlaşılır bir formattır.

3.1.2.7. Diğer araçlar ve kütüphaneler

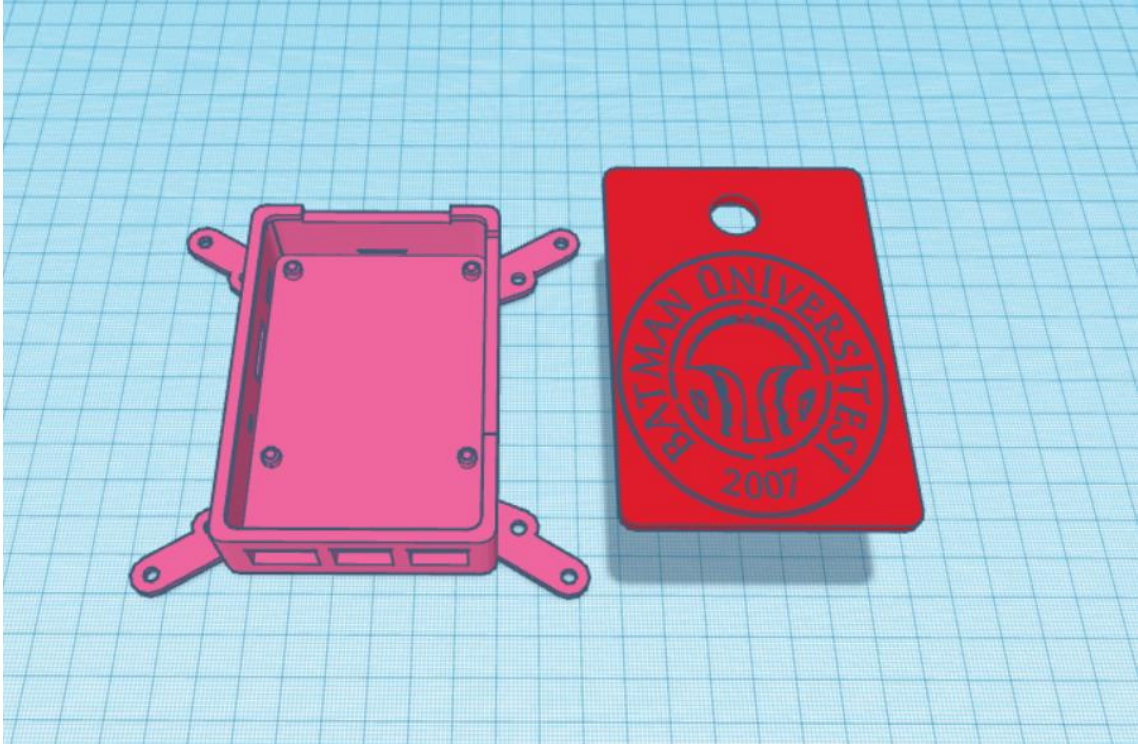
Tez çalışması kapsamında çeşitli yardımcı araçlar ve kütüphaneler de kullanılmıştır. Bu araçlar arasında, HTTP isteklerini yönetmek için kullanılan requests kütüphanesi, zaman damgası uygulamaları için kullanılan datetime kütüphanesi ve PostgreSQL veri tabanına bağlanmak için kullanılan psycopg2 kütüphanesi bulunmaktadır.

3.1.3. Geliştirme ve test ortamı

Tez çalışması boyunca kullanılan geliştirme ve test ortamları şunlardır:

- **Visual Studio Code:** Python ve PHP kodlarının yazılması ve düzenlenmesi için kullanılan bir kod editörüdür.
- **Postman:** API isteklerini test etmek ve doğrulamak için kullanılmıştır.

- **Raspberry Pi Terminal:** Raspberry Pi üzerinde doğrudan komut çalıştırmak ve sistem yönetimi yapmak için kullanılmıştır.
- **3D Yazıcı:** Cihaz muhafazasının prototipini üretmek için kullanılmıştır.



Şekil 3.2. 3D Yazıcı ile tasarlanmış cihaz muhafazası prototipi

Bu materyaller, tez çalışmasından tüm aşamalarında kullanılarak, kameralı kartlı geçiş sisteminin tasarımı, geliştirilmesi ve test edilmesi sağlanmıştır. Bu bileşenlerin seçimi, sistemin güvenilir, etkili ve kullanıcı dostu olmasını sağlamak amacıyla yapılmıştır.

3.2. Yöntem

Bu bölümde, kameralı kartlı geçiş sisteminin tasarımı, geliştirilmesi, uygulanması ve test edilmesi sürecinde izlenen yöntemler detaylı bir şekilde açıklanacaktır. Tez kapsamında kullanılan donanım ve yazılım bileşenlerinin entegrasyonu, veri işleme ve analiz yöntemleri ile sistemin performans ve güvenilirlik testleri ele alınacaktır.

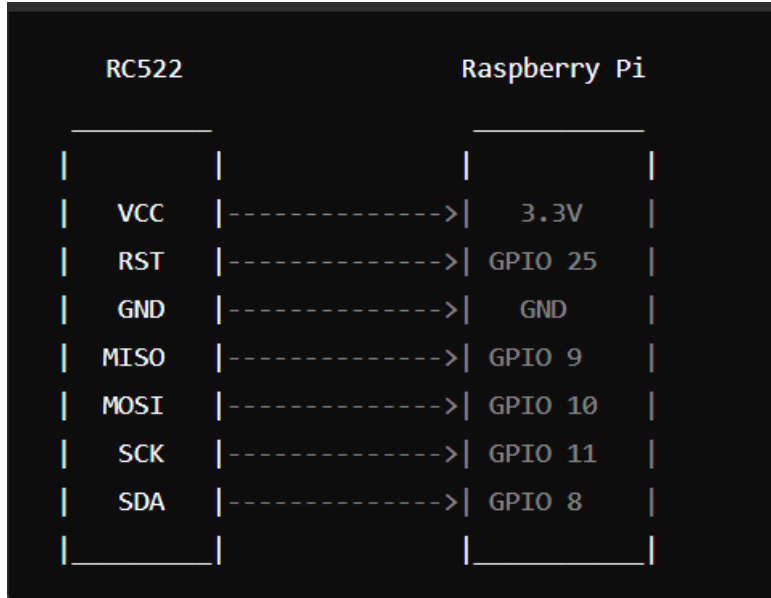
3.2.1. Geliştirme ve test ortamı

3.2.1.1. Sistem tasarımı

Donanım Tasarımı

Sistem tasarımının ilk aşaması, gerekli donanım bileşenlerinin belirlenmesi ve entegrasyonudur. Bu kapsamda, Raspberry Pi, RC522 NFC kart okuyucu, Raspberry Pi kamera modülü ve diğer gerekli aksesuarlar (kablosuz bağlantı modülü, güç kaynağı, kablolar vb.) seçilmiştir.

Bağlantı Şeması: Donanım bileşenlerinin birbirleriyle nasıl bağlanacağı belirlenmiş ve bağlantı şeması oluşturulmuştur.



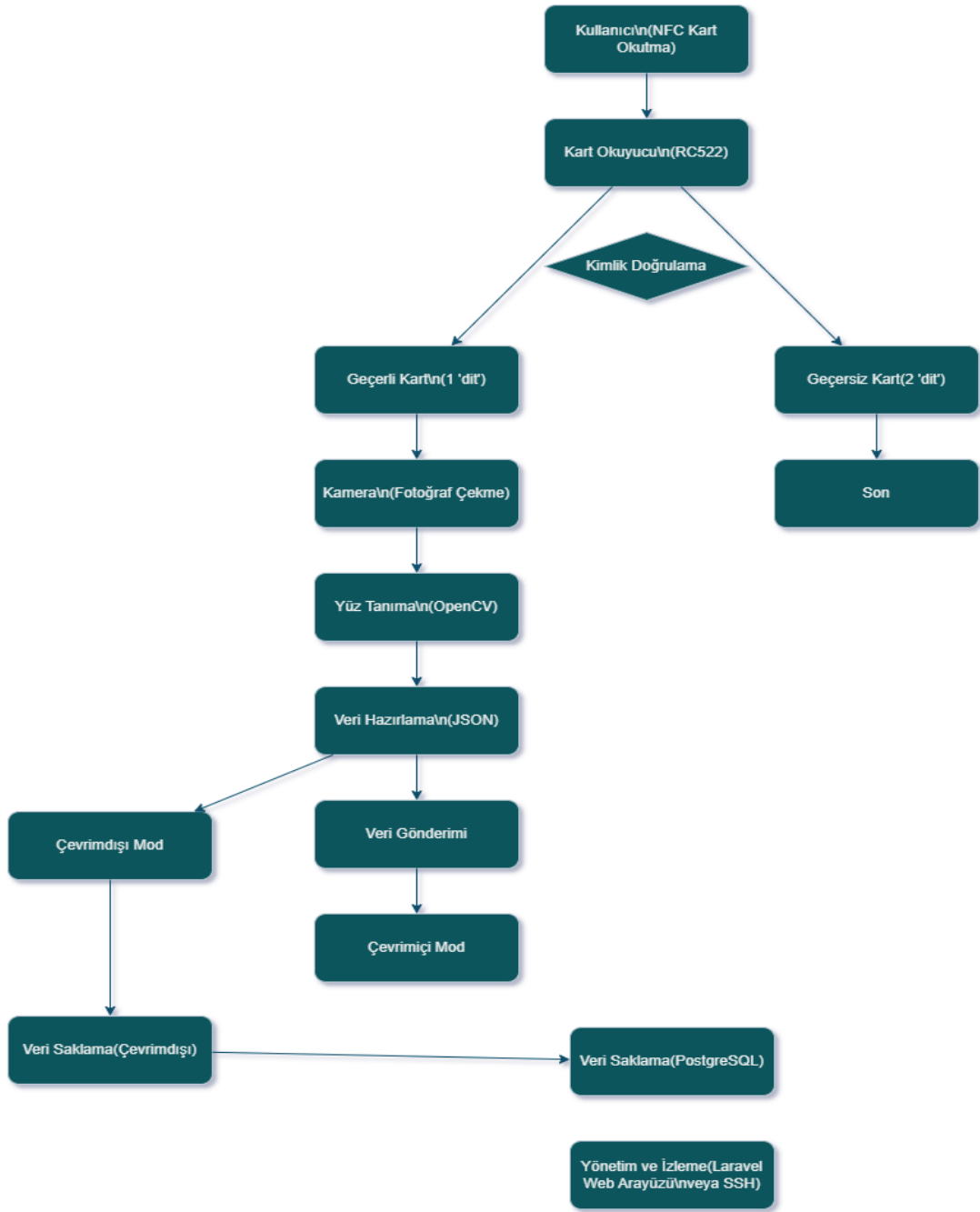
Şekil 3.3. Donanım bileşenleri bağlantı şeması

Tüm bileşenler, belirlenen bağlantı şemasına göre monte edilmiştir. NFC kart okuyucu SPI protokolü ile Raspberry Pi'ye bağlanmış, kamera modülü ise CSI portu üzerinden entegre edilmiştir.

Yazılım Tasarımı

Yazılım tasarımında, sistemin fonksiyonlarını yerine getirecek yazılım bileşenlerinin geliştirilmesi amaçlanmıştır. Bu kapsamda, sistem gereksinimlerine uygun yazılım bileşenleri belirlenmiştir. tez çalışmasının geliştirilmesi sürecinde Python, OpenCV, PostgreSQL ve Laravel gibi teknolojiler kullanılacaktır.

Yazılım bileşenleri her bir modül, belirli bir fonksiyonu yerine getirecek şekilde modüler bir yapıda tasarlanmıştır tasarlanmıştır (NFC kart okuma, yüz tanıma, veri kaydı vb.). Sistem veri akışı şeması aşağıdaki şekilde görüldüğü gibi oluşturulmuş ve veri işleme süreçleri tanımlanmıştır.



Şekil 3.4. Veri akış şeması

3.2.1.1. Geliştirme süreci

Donanım Entegrasyonu

Donanım entegrasyonu sürecinde, NFC kart okuyucu ve kamera modülü Raspberry Pi'ye bağlanmış ve bu bileşenlerin düzgün çalıştığından emin olunmuştur. Bu süreçte, bağlantı kontrolü testi yapılarak tüm bağlantıların doğru yapıldığından emin

olunmuş ve bileşenlerin düzgün çalışıp çalışmadığı test edilmiş, NFC kart okuyucunun kartları okuyup okuyamadığı, kamera modülünün görüntü alıp alamadığı kontrol edilmiştir.

Yazılım Geliştirme

Yazılım geliştirme sürecinde, sistemin tüm fonksiyonlarını yerine getirecek yazılım bileşenleri geliştirilmiştir. Bu süreçte, aşağıdaki adımlar izlenmiştir:

- **Python ile NFC Kart Okuma:** RC522 modülü kullanılarak NFC kartların okunması için Python kodu yazılmıştır.
- **OpenCV ile Yüz Tanıma:** Kamera modülü kullanılarak çekilen görüntüler üzerinde yüz tanıma işlemleri yapılmıştır.
- **Veri Kaydı ve Yönetimi:** PostgreSQL veri tabanı kullanılarak geçiş bilgileri ve zaman damgası verileri kaydedilmiş ve yönetilmiştir.
- **Laravel ile Yönetim Yazılımı:** Merkezi kontrol ve yönetim yazılımı olarak Laravel çerçevesi kullanılarak bir web uygulaması geliştirilmiştir.

Veri İşleme ve Analiz

Sistem, NFC kart okuyucu ve kamera modülü aracılığıyla veri toplar. Toplanan veriler şunlardır:

- **Kart Bilgileri:** NFC kart okuyucu tarafından okunan kart ID'si ve diğer bilgiler.
- **Görüntü Verileri:** Kamera modülü tarafından çekilen geçiş anındaki görüntüler.
- **Zaman Damgası:** TÜBİTAK zaman damgası ile damgalanan geçiş zamanı bilgileri.

Veri İşleme

Toplanan veriler, sistemde işlenir ve anlamlı hale getirilir. Bu süreçte, aşağıdaki adımlar izlenmiştir:

- **Yüz Tanıma:** OpenCV kullanılarak çekilen görüntülerde yüz tanıma işlemleri yapılır.
- **Veri Formatlama:** Toplanan veriler JSON formatında yapılandırılır.

- **Veri Kaydı:** Veri tabanına kaydedilir ve yönetim yazılımı aracılığıyla erişilebilir hale getirilir.

Performans ve Güvenilirlik Testleri

Geliştirilen sistem, çeşitli test senaryoları ile test edilmiştir. Bu süreçte, aşağıdaki testler gerçekleştirilmiştir:

- **Fonksiyonel Testler:** Sistem bileşenlerinin belirlenen fonksiyonları yerine getirip getirmediği test edilmiştir.
- **Performans Testleri:** Sistem performansı, özellikle veri işleme ve yanıt süreleri açısından test edilmiştir.
- **Güvenilirlik Testleri:** Sistem güvenilirliği, verilerin doğru kaydedilmesi ve zaman damgası uygulamalarının doğruluğu açısından test edilmiştir.

Kullanıcı Deneyimi Testleri

Kullanıcı deneyimini artırmak amacıyla geliştirilen SSH ve web arayüzü üzerinden yönetim özellikleri test edilmiştir. Bu süreçte, aşağıdaki adımlar izlenmiştir:

- **Arayüz Testleri:** Kullanıcı arayüzlerinin kullanılabilirliği ve kullanıcı dostu olup olmadığı test edilmiştir.
- **Geri Bildirim:** Test kullanıcılarından geri bildirim alınarak sistemde iyileştirmeler yapılmıştır.

Testler sonucunda elde edilen veriler, sistemin performansı, güvenilirliği ve kullanıcı deneyimi açısından değerlendirilmiştir. Bu değerlendirme sonucunda, sistemin mevcut durumu ve gelecekte yapılabilecek iyileştirmeler belirlenmiştir.

Bu yöntemler, kameralı kartlı geçiş sisteminin tasarımı, geliştirilmesi, uygulanması ve değerlendirilmesi sürecinde izlenmiştir. Bu süreçte elde edilen bulgular, sistemin güvenilir, etkili ve kullanıcı dostu hale getirilmesini sağlamıştır.

3. ÇALIŞMANIN SONUÇLARI VE TARTIŞMA

Bu bölümde, kameralı kartlı geçiş sisteminin geliştirilmesi ve uygulanması sürecinde elde edilen sonuçlar ve bu sonuçların değerlendirilmesi ele alınacaktır. Ayrıca, sistemin performansı, güvenilirliği ve kullanıcı deneyimi açısından değerlendirilecektir.

Sistem Tasarımı ve Uygulaması

Bu tezde, NFC kart okuyucu, kamera modülü ve Raspberry Pi kullanılarak entegre bir geçiş kontrol sistemi tasarlanmış ve uygulanmıştır. Tasarım sürecinde, donanım bileşenlerinin birbirleriyle uyumlu bir şekilde çalışması sağlanmıştır. NFC kart okuyucu, SPI protokolü üzerinden Raspberry Pi ile başarılı bir şekilde iletişim kurmuş ve kullanıcı kartlarını okuyabilmiştir. Kamera modülü, CSI portu üzerinden bağlanarak yüksek çözünürlüklü görüntüler sağlamış ve yüz tanıma işlemleri için gerekli verileri sunmuştur.

Yazılım Geliştirme

Yazılım geliştirme sürecinde, Python programlama dili ve OpenCV kütüphanesi kullanılarak yüz tanıma ve veri işleme işlemleri gerçekleştirilmiştir. NFC kart okuyucu ve kamera modülü ile entegre çalışan yazılım bileşenleri, geçiş bilgilerini toplamak ve işlemek için gerekli fonksiyonları yerine getirmiştir. PostgreSQL veri tabanı kullanılarak verilerin güvenli bir şekilde saklanması sağlanmış ve Laravel Framework kullanılarak merkezi yönetim yazılımı geliştirilmiştir. JSON formatında veri aktarımı, veri entegrasyonunu kolaylaştırmış ve sistemin farklı bileşenleri arasında uyumlu veri iletişimi sağlamıştır.

Performans ve Güvenilirlik

Sistemin performansı ve güvenilirliği, çeşitli test senaryoları ile değerlendirilmiştir. Fonksiyonel testlerde, NFC kart okuyucunun kartları doğru bir şekilde okuduğu ve kamera modülünün yüksek kaliteli görüntüler sağladığı görülmüştür. Yüz tanıma algoritmaları, OpenCV kullanılarak başarılı bir şekilde uygulanmış ve yüksek doğruluk oranları elde edilmiştir. Veri işleme ve kaydetme süreçlerinde herhangi bir veri kaybı yaşanmamış, tüm veriler PostgreSQL veri tabanında güvenli bir şekilde saklanmıştır.

Güvenilirlik testlerinde, sistemin yasal gereksinimlere uygun olarak çalıştığı ve TÜBİTAK zaman damgası ile veri bütünlüğünün sağlandığı doğrulanmıştır. Elektronik delillerin geçerliliği ve güvenilirliği, 5651 sayılı yasa çerçevesinde değerlendirilmiş ve sistemin hukuki gereksinimleri karşıladığı görülmüştür.

Kullanıcı Deneyimi

Sistem kullanıcılarının deneyimini artırmak amacıyla SSH ve web arayüzü üzerinden yönetim özellikleri geliştirilmiştir. Kullanıcılar, sistem ayarlarını kolaylıkla değiştirebilmiş, geçiş kayıtlarını görüntüleyebilmiş ve sistem durumunu izleyebilmiştir. Kullanıcı arayüzlerinin kullanılabilirliği test edilmiş ve kullanıcı dostu olduğu görülmüştür. Test kullanıcılarından alınan geri bildirimler doğrultusunda, sistemde çeşitli iyileştirmeler yapılmıştır.

Bu çalışma, kameralı kartlı geçiş sistemlerinin tasarımı ve uygulanması konusunda önemli bulgular sunmaktadır. NFC kart okuyucu, kamera modülü ve Raspberry Pi'nin entegrasyonu, güvenli ve etkili bir geçiş kontrol sistemi oluşturmak için başarılı bir çözüm sunmaktadır. Python ve OpenCV kullanılarak gerçekleştirilen yüz tanıma işlemleri, yüksek doğruluk oranları ile sistemin güvenilirliğini artırmıştır. Merkezi yönetim yazılımı, verilerin güvenli bir şekilde saklanmasını ve yönetilmesini sağlamıştır.

Sistemin performans ve güvenilirlik testleri, sistemin yasal gereksinimleri karşıladığını ve kullanıcı deneyimi açısından tatmin edici olduğunu göstermiştir. SSH ve web arayüzü üzerinden yönetim özellikleri, kullanıcıların sistemi kolaylıkla yönetmesini sağlamış ve kullanıcı dostu bir deneyim sunmuştur. Bu sonuçlar, sistemin gerçek dünya uygulamaları için uygun olduğunu ve güvenlik açısından önemli bir katkı sağladığını göstermektedir.

Gelecekte, yapay zeka ve makine öğrenimi teknolojilerinin entegrasyonu ile sistemin daha da geliştirilebileceği ve yüz tanıma algoritmalarının doğruluk oranlarının artırılabilirliği öngörülmektedir. Ayrıca, Nesnelerin İnterneti (IoT) teknolojileri ile sistemlerin entegrasyonu, daha kapsamlı ve bütüncül bir güvenlik çözümü sunabilecektir.

4. SONUÇLAR VE ÖNERİLER

5.1 Sonuçlar

Bu tezde, kameralı kartlı geçiş sistemlerinin tasarımı, uygulanması ve değerlendirilmesi kapsamlı bir şekilde ele alınmıştır. NFC kart okuyucu, kamera modülü ve Raspberry Pi kullanılarak entegre bir geçiş kontrol sistemi geliştirilmiştir. Sistem, güvenlik ve izleme alanında önemli bir rol oynayarak, giriş ve çıkışların kontrolünü sağlamış ve izleme imkanı sunmuştur.

Sistem tasarımında, donanım bileşenlerinin entegrasyonu ve yazılım bileşenlerinin geliştirilmesi başarıyla gerçekleştirilmiştir. Python ve OpenCV kullanılarak yüz tanıma işlemleri yüksek doğruluk oranları ile gerçekleştirilmiş, PostgreSQL veri tabanı ile verilerin güvenli bir şekilde saklanması sağlanmıştır. Laravel Framework kullanılarak geliştirilen merkezi yönetim yazılımı, kullanıcıların sistem ayarlarını yönetmesini, geçiş kayıtlarını görüntülemesini ve sistem durumunu izlemesini kolaylaştırmıştır.

Yapılan performans ve güvenilirlik testleri, sistemin yüksek doğruluk oranlarına sahip olduğunu, verilerin güvenli bir şekilde saklandığını ve zaman damgası ile veri bütünlüğünün sağlandığını göstermiştir. Elektronik delillerin geçerliliği ve güvenilirliği, 5651 sayılı yasa ve ilgili düzenlemeler çerçevesinde değerlendirilmiş ve sistemin hukuki gereksinimleri karşıladığı doğrulanmıştır.

Kullanıcı deneyimini artırmak amacıyla geliştirilen SSH ve web arayüzü yönetim özellikleri, kullanıcıların sistemi kolaylıkla yönetebilmesini sağlamış ve kullanıcı dostu bir deneyim sunmuştur. Test kullanıcılarından alınan geri bildirimler doğrultusunda yapılan iyileştirmeler, sistemin kullanılabilirliğini ve verimliliğini artırmıştır.

Bu çalışmanın sonucunda, kameralı kartlı geçiş sistemlerinin güvenilir, etkili ve kullanıcı dostu bir çözüm sunduğu ve güvenlik alanında önemli bir katkı sağladığı ortaya konulmuştur. Sistem, gerçek dünya uygulamaları için uygun olup, güvenlik ve izleme süreçlerinde etkin bir şekilde kullanılabileceği gösterilmiştir.

Sonuç olarak, bu tezde geliştirilen kameralı kartlı geçiş sistemi, güvenlik ve izleme alanında önemli bir adım olup, gelecekte yapılacak iyileştirmelerle daha da geliştirilebilir ve yaygın olarak kullanılabilecektir. Bu sistem, hem teknik hem de

hukuki gereksinimleri karşılayarak, güvenlik açısından yüksek standartlarda bir çözüm sunmaktadır.

5.2 Öneriler

Bu çalışmanın sonuçları, kameralı kartlı geçiş sistemlerinin güvenilirlik ve etkinlik açısından önemli bir çözüm sunduğunu ortaya koymaktadır. Ancak, sistemin daha da geliştirilmesi ve genişletilmesi için bazı önerilerde bulunmak mümkündür. Aşağıda, bu tür sistemlerin gelecekte nasıl iyileştirilebileceği ve hangi yeniliklerin uygulanabileceği konusundaki öneriler yer almaktadır:

- **Yapay Zeka ve Makine Öğrenimi Entegrasyonu**

Gelişmiş yüz tanıma algoritmalarının doğruluğunu ve güvenilirliğini artırmak için yapay zeka ve makine öğrenimi tekniklerinin entegrasyonu yapılabilir. Derin öğrenme modelleri, yüz tanıma işlemlerinde daha yüksek doğruluk oranları sağlayabilir ve güvenlik seviyesini artırabilir. Bu amaçla, TensorFlow veya PyTorch gibi kütüphaneler kullanılabilir.

- **Nesnelerin İnterneti (IoT) ile Entegrasyon**

Sistemin daha kapsamlı ve bütüncül bir güvenlik çözümü sunması için Nesnelerin İnterneti (IoT) teknolojileri ile entegrasyonu gerçekleştirilebilir. IoT cihazları, farklı sensörler ve kameralar arasında veri paylaşımını mümkün kılarak, daha geniş bir güvenlik ağı oluşturabilir. Bu, güvenlik olaylarının daha hızlı ve etkin bir şekilde tespit edilmesini sağlayabilir.

- **Bulut Tabanlı Veri Depolama ve İşleme**

Sistem verilerinin daha güvenli ve erişilebilir bir şekilde saklanması için bulut tabanlı veri depolama ve işleme çözümlerinin kullanılması söz konusu olabilir. Bulut hizmetleri, büyük veri setlerinin saklanması ve işlenmesi için ölçeklenebilir ve güvenli bir altyapı sunar. Bu, veri kaybı riskini azaltır ve verilerin her yerden erişilebilir olmasını sağlar.

- **Mobil Uygulama Geliştirilmesi**

Kullanıcıların sisteme mobil cihazlar üzerinden erişim sağlaması için bir mobil uygulama geliştirilmesi öngörülebilir. Bu sayede, kullanıcıların geçiş kayıtlarını görüntülemesini, sistem ayarlarını yönetmesini ve anlık bildirimler almasını kolaylaştırabilir. Ayrıca, mobil uygulama üzerinden yüz tanıma ve kimlik doğrulama işlemleri de yapılabilir.

- **Çok Faktörlü Kimlik Doğrulama**

Sistemin güvenliğini artırmak için çok faktörlü kimlik doğrulama yöntemlerinin eklenmesi ilerisi için üzerinde çalışılması gereken bir konu olabilir. NFC kart okuyucu ve yüz tanıma işlemlerine ek olarak, parmak izi tarayıcılar veya mobil doğrulama kodları gibi ek güvenlik katmanları kullanılabilir. Bu, yetkisiz erişim riskini azaltır ve sistemin güvenliğini artırır.

- **Kullanıcı Eğitimleri ve Bilgilendirme**

Sistemin etkin ve doğru bir şekilde kullanılabilmesi için kullanıcı eğitimleri ve bilgilendirme oturumlarının düzenlenmesi gerekecektir. Kullanıcılar, sistemin özellikleri, kullanımı ve güvenlik önlemleri hakkında bilgilendirilmelidir. Bu, sistemin verimli kullanılmasını ve olası güvenlik ihlallerinin önlenmesini sağlayacaktır.

- **Sürekli İyileştirme ve Güncellemeler**

Sistemin performansını ve güvenilirliğini korumak için düzenli olarak güncellemeler yapılması ve iyileştirmeler uygulanması gerekecektir. Yazılım ve donanım bileşenlerinin güncel tutulması, yeni güvenlik tehditlerine karşı korunmayı sağlar ve sistemin uzun ömürlü olmasını garanti eder.

- **Veri Analitiği ve Raporlama**

Sistemin topladığı verilerin analiz edilmesi ve anlamlı raporlar oluşturulması için veri analitiği çözümlerinin kullanılması gerekmektedir. Bu, geçiş verilerinin trendlerini belirlemeyi, anomali tespit etmeyi ve güvenlik açıklarını erken aşamada fark etmeyi sağlar. Veri analitiği araçları, karar destek sistemleri için de değerli bilgiler sunabilir.

Bu öneriler, kameralı kartlı geiş sistemlerinin daha güvenli, verimli ve kullanıcı dostu hale getirilmesine katkıda bulunacaktır. Gelecekte yapılacak alışmalar ve iyileştirmeler ile bu sistemlerin yaygınlaşması ve güvenlik alanında daha geniş bir kullanım alanı bulması mümkün olacaktır.

KAYNAKLAR

- Al-Ofeishat, H. A., & Al Rababah, M. A. (2012). Near field communication (NFC). *International Journal of Computer Science and Network Security*, 12(2), 93.
- Alshammari, A., & Rawat, D. B. (2019, January). Intelligent multi-camera video surveillance system for smart city applications. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 317-323). IEEE.
- Altıparmak, K., & Akdeniz, Y. (2017). 5651 sayılı Kanunun Değişiklik Tasarısının Getirdiği Değişiklikler Üzerine Bir Değerlendirme. *TBB Dergisi*.
- Arante, R. B., Eguna, S. M., Mondala, C., & Jacon, D. (2018). Surveillance camera provision for tricycles in Cabadbaran City: Its perceived effects on passengers' safety and security. *International Journal of Recent Advances in Organization and Decision Sciences*, 4(1), 1123-1141.
- Arslan, Ç. (2015). Digital evidence and supervision of communication. *Journal of Penal Law and Criminology*, 3(2), 253-266.
- Atılğan, M., & Samet, R. (2018). Güvenlik kamera görüntülerindeki tarih ve zaman sayacı üzerinde yapılan manipülasyonların tespit edilebilirliği. *Bilişim Teknolojileri Dergisi*, 11(4), 333-347.
- Balaban, S. (2015). Deep learning and face recognition: The state of the art. In *Biometric and Surveillance Technology for Human and Activity Identification XII* (Vol. 9457, pp. 68-75). SPIE.
- Balaji, S., Nathani, K., & Santhakumar, R. (2019). IoT technology, applications and challenges: A contemporary survey. *Wireless Personal Communications*, 108, 363-388.
- Birleşmiş Milletler, Uluslararası Ticaret Hukuku Komisyonu (2001). Model Law on Electronic Signatures. Erişim adresi: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures
- Bradski, G. (2000). The OpenCV library. *Dr. Dobb's Journal: Software Tools for the Professional Programmer*, 25(11), 120-123.
- Campion, E. D., Campion, M. C., & Campion, M. A. (2018). Compensating tipped work: Security cameras as a tool for time use measurement. *Compensation & Benefits Review*, 50(1), 36-54.
- Canoğlu, V. C. (2018). Disiplin soruşturmasında delil ve ispat. *TBB Dergisi*, 138.
- Casey, E. (2011). Digital evidence in the courtroom. In *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (pp. 49-84). Elsevier.

- Dockins, K. (2017). Design Patterns in PHP and Laravel (pp. 100-140). *Apress*.
- Donat, W., & Krause, C. (2014). Learn Raspberry Pi Programming with Python. *Apress*.
- Droettboom, M. (2015). Understanding JSON Schema. Erişim adresi: <http://spacetelescope.github.io/understanding-jsonschema/UnderstandingJSONSchema.pdf> (accessed on 14 April 2014).
- Dudeja, K., Sinha, A., Saini, N., Mandal, S., & Bansal, P. (2016). Raspberry Pi based solar camera for city surveillance. *International Journal of Scientific Research in Science, Engineering and Technology*, 5(5).
- Elektronik İmza Kanunu (2004). Resmî Gazete, (Sayı: 25355).
- Ford, V., & Siraj, A. (2014, October). Applications of machine learning in cyber security. In *Proceedings of the 27th International Conference on Computer Applications in Industry and Engineering* (Vol. 118). Kota Kinabalu, Malaysia: IEEE Xplore.
- Glorot, X., & Bengio, Y. (2010, March). Understanding the difficulty of training deep feedforward neural networks. In *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics* (pp. 249-256). JMLR Workshop and Conference Proceedings.
- Gu, Y., Kim, M., Cui, Y., Lee, H., Choi, O., Pyeon, M., & Kim, J. (2013, June). Design and implementation of UPnP-based surveillance camera system for home security. In *2013 International Conference on Information Science and Applications (ICISA)* (pp. 1-4). IEEE.
- Gupta, A., Maurya, S., Mehra, N., & Kapil, D. (2021, January). Covid-19: Employee fever detection with thermal camera integrated with attendance management system. In *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 355-361). IEEE.
- Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. In *Advances in Cryptology* (pp. 437-455). Springer.
- Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*, 7, 82721-82743.
- Hellwig, K. (2021). The potential and the challenges of digital evidence in international criminal proceedings. *International Criminal Law Review*, 22(5-6), 965-988.
- Henkoğlu, T. (2020). Adli bilişim: Dijital delillerin elde edilmesi ve analizi. *Pusula*.
- Horsman, G. (2021). Digital evidence and the crime scene. *Science & Justice*, 61(6), 761-770.

- Hudson-Smith, A., Wilson, D., Gray, S., & Dawkins, O. (2021). Urban IoT: Advances, challenges, and opportunities for mass data collection, analysis, and visualization. *Urban Informatics*, 701-719.
- İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (2007). Resmi Gazete (Sayı: 26530). Erişim adresi: <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf>
- Jung, M. G., Youn, S. A., Bae, J., & Choi, Y. L. (2015, November). A study on data input and output performance comparison of MongoDB and PostgreSQL in the big data environment. In *2015 8th International Conference on Database Theory and Application (DTA)* (pp. 14-17). IEEE.
- Kamu Sertifikasyon Merkezi (t.y.). Zaman Damgası. Erişim adresi: https://kamusm.bilgem.tubitak.gov.tr/urunler/zaman_damgasi/. Erişim Tarihi: 20.08.2024.
- Kasper, A., & Laurits, E. (2016). Challenges in collecting digital evidence: A legal perspective. In *The Future of Law and eTechnologies* (pp. 195-233).
- Kilavo, H., Mrutu, S. I., & Dudu, R. G. (2023). Securing relational databases against security vulnerabilities: A case of Microsoft SQL Server and PostgreSQL. *Journal of Applied Security Research*, 18(3), 421-435.
- Kumar, A., Sharma, S., Singh, A., Alwadain, A., Choi, B. J., Manual-Brenosa, J., ... & Goyal, N. (2021). Revolutionary strategies analysis and proposed system for future infrastructure in internet of things. *Sustainability*, 14(1), 71.
- Laaziri, M., Benmoussa, K., Khouilji, S., Larbi, K. M., & El Yamami, A. (2019). A comparative study of Laravel and Symfony PHP frameworks. *International Journal of Electrical and Computer Engineering*, 9(1), 704-712.
- Landwehr, C. E. (2001). Computer security. *International Journal of Information Security*, 1(1), 3-13.
- Maksimović, M., Vujović, V., Davidović, N., Milošević, V., & Perišić, B. (2014). Raspberry Pi as Internet of things hardware: Performances and constraints. *Design Issues*, 3(8), 1-6.
- Marshall, A. M. (2009). Digital forensics: Digital evidence in criminal investigations. *John Wiley & Sons*.
- McCool, S. (2012). *Laravel Starter*. Packt Publishing.
- Mohammed, I. A. (2013). An exploratory study into the face detection and recognition system to strengthen security precautions using an artificial intelligence system.
- Monk, S. (2022). *Raspberry Pi Cookbook*. O'Reilly Media, Inc.

- Nguyen, H. Q., Loan, T. T. K., Mao, B. D., & Huh, E. N. (2015, July). Low cost real-time system monitoring using Raspberry Pi. In *2015 Seventh International Conference on Ubiquitous and Future Networks* (pp. 857-859). IEEE.
- Nieto, A., Roman, R., & Lopez, J. (2016). Digital witness: Safeguarding digital evidence by using secure architectures in personal devices. *IEEE Network*, 30(6), 34-41.
- Obe, R. O., & Hsu, L. S. (2017). *PostgreSQL: Up and Running: A Practical Guide to the Advanced Open Source Database*. O'Reilly Media, Inc.
- Özkaya, P. (2021). Adli bilişimde standardizasyon sertifikasyon akreditasyon ve en iyi uygulamalar (Master's thesis, Ankara Üniversitesi, Turkey).
- Poyen, F. B. (2019). Raspberry Pi and its use in IoT applications. *Annual Technical Volume of Computer Engineering Division Board: Theme: Role of IoT in Make in India*, 44-47.
- Rao, B. N., & Sudheer, R. (2020, July). Surveillance camera using IoT and Raspberry Pi. In *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 1172-1176). IEEE.
- Richardson, M., & Wallace, S. (2014). *Getting Started with Raspberry Pi: Electronic Projects with Python, Scratch, and Linux*. Maker Media, Inc.
- Rijavec, V., & Keresteš, T. (Eds.). (2015). Dimensions of evidence in European civil procedure. *Kluwer Law International BV*.
- Roland, M. (2012, June). Software card emulation in NFC-enabled mobile phones: Great advantage or security nightmare. In *Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use* (pp. 1-6).
- Ryan, D. J., & Shpantzer, G. (2002, September). Legal aspects of digital forensics. In *Proceedings: Forensics Workshop*.
- Ryu, J. H., Moon, S. Y., & Park, J. H. (2018). The study on data of smart home system as digital evidence. In *Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 17* (pp. 967-972). Springer Singapore.
- Saeed, K., Pejas, J., & Mosdorf, R. (Eds.). (2007). Biometrics, computer security systems and artificial intelligence applications. *Springer Science & Business Media*.
- Sağlık, Ö. (2022). *Elektronik belgelerin güvenilirliği*. İstanbul: Hiperlink Yayınları.
- Sağlık, Ö. (2024). Elektronik imzalı belgelerin sahteciliği: Yargıtay kararları bağlamında bir inceleme.

- Schönig, H. J. (2023). *Mastering PostgreSQL 15: Advanced Techniques to Build and Manage Scalable, Reliable, and Fault-Tolerant Database Applications*. Packt Publishing Ltd.
- Segate, R. V. (2021). Cognitive bias, privacy rights, and digital evidence in international criminal proceedings: Demystifying the double-edged AI revolution. *International Criminal Law Review*, 21(2), 242-279.
- Singh, M. M., Adzman, K. A. A. K., & Hassan, R. (2018). Near Field Communication (NFC) technology security vulnerabilities and countermeasures. *International Journal of Engineering & Technology*, 7(4.31), 298-305.
- Subecz, Z.
(2021). Web-development with Laravel framework. *Gradus*, 8(1), 211-218.
- Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 1701-1708).
- Teoh, K. H., Ismail, R. C., Naziri, S. Z. M., Hussin, R., Isa, M. N. M., & Basir, M. S. S. M. (2021, February). Face recognition and identification using deep learning approach. In *Journal of Physics: Conference Series* (Vol. 1755, No. 1, p. 012006). IOP Publishing.
- Thammarat, C. (2020). Efficient and secure NFC authentication for mobile payment ensuring fair exchange protocol. *Symmetry*, 12(10), 1649.
- Tübitak Bilgem (2022). Zaman Damgası İlkeleri. Erişim adresi: https://kamusm.bilgem.tubitak.gov.tr/BilgiDeposu/KSM_ZDI/POL.01.02_03_KAMU_SM_ZAMAN_DAMGASI_ILKELERI.pdf. Erişim Tarihi: 23.08.2024.
- Van Rompay, T. J., Vonk, D. J., & Fransen, M. L. (2009). The eye of the camera: Effects of security cameras on prosocial behavior. *Environment and Behavior*, 41(1), 60-74.
- Van Rossum, G., & Drake, F. L. (1995). *Python Reference Manual* (Vol. 111, pp. 1-52). Amsterdam: Centrum voor Wiskunde en Informatica.
- Vani, P. S., & NithyaPriya, G. (2014). Database administration in Raspberry using a server machine. *International Journal of Innovative Engineering and Technology*, 3, 41-47.
- Wallace, S., Richardson, M., & Donat, W. (2021). *Getting Started with Raspberry Pi*. O'Reilly Media.
- Wang, J., & Li, Z. (2018, July). Research on face recognition based on CNN. In *IOP Conference Series: Earth and Environmental Science* (Vol. 170, No. 3, p. 032110). IOP Publishing.

Yalçın, H. (2015). Elektronik belge yönetim sistemlerinin elektronik arşiv sistemleriyle entegrasyonu: İKCU UBS örneği. *e-BEYAS*, 21-22.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Raif SİME
Uyruğu : TC

EĞİTİM

Derece Adı, İlçe, İl Eskişehir /Merkez Bitirme Yılı 2013
Üniversite : ANADOLU ÜNİVERSİTESİ
Yüksek Lisans :
Doktora :

İŞ DENEYİMLERİ

Yıl	Kurum	Görevi
2008	Sanayi Bakanlığı	Tekniker
2010	Ağrı İbrahim Çeçen Üniversitesi	Tekniker
2014	Kamu Denetçiliği Kurumu	Tekniker
2016	Anayasa Mahkemesi	Tekniker
2020	Bitlis Eren Üniversitesi	Şube Müdürü

UZMANLIK ALANI

YABANCI DİLLER

YAYINLAR