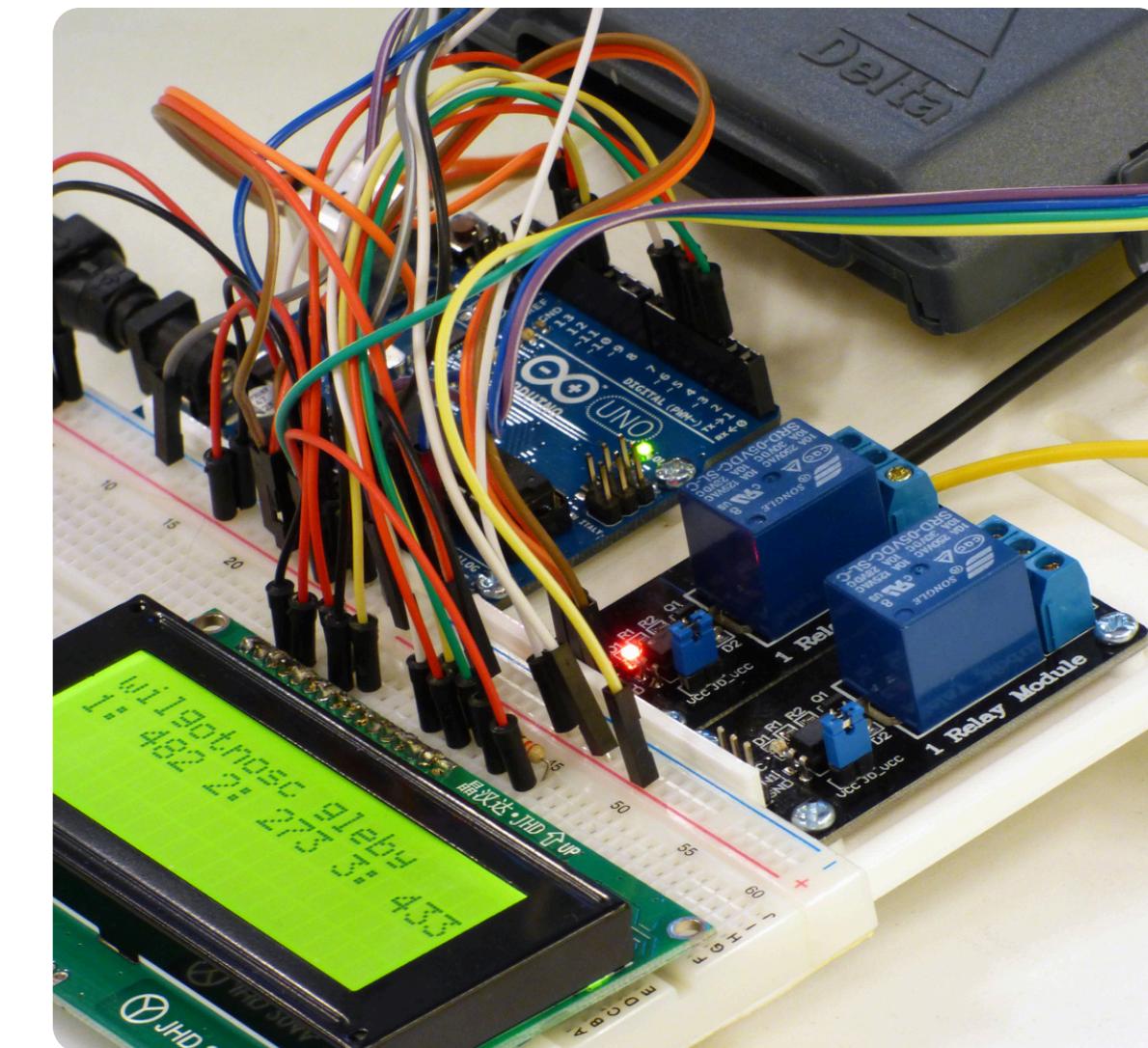


2 FAKTÖR DOĞRULAMALI NFC TABANLI AKILLI KILIT SİSTEMİ



içindeKİLER

Giriş

Motivasyon ve Katkılar

Literatür Özeti

Donanım Bileşenleri

Projenin Uygulanması

Analog vs Dijital

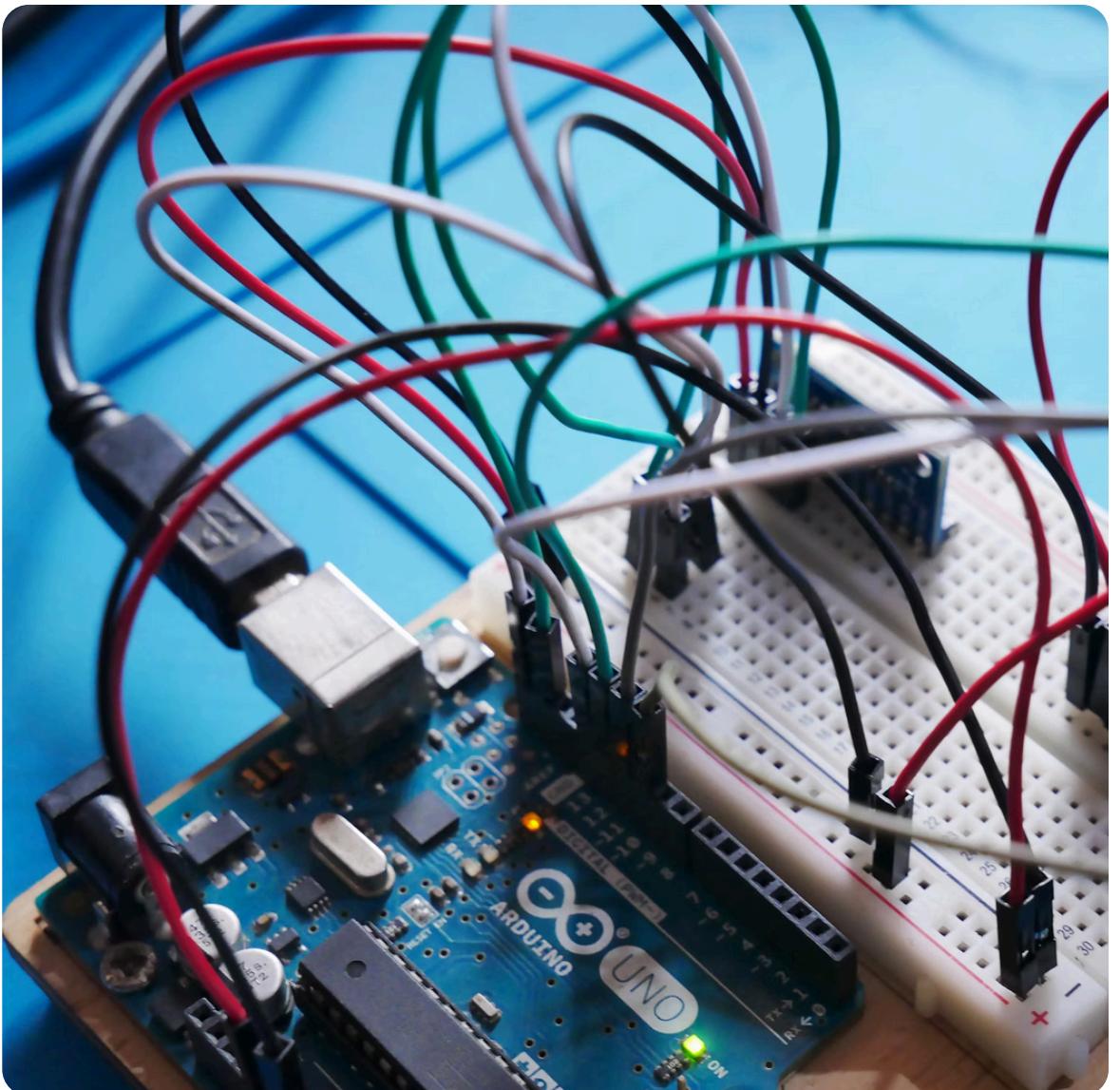
Geliştirilecek Yönler ve Yol Haritası

Sonuçlar

Kaynakça

gİRİŞ

- 1 Teknolojinin hızlı gelişimi, geleneksel anahtar sistemlerinin yerini akıllı kilitlere bırakarak daha güvenli ve pratik erişim kontrolü sağlamıştır.
- 2 NFC teknolojisi, temassız ve hızlı veri aktarımı özellikleriyle ev, ofis ve endüstriyel alanlarda kolay erişim imkânı sunmaktadır.
- 3 Biyometrik doğrulama sistemleri, özellikle parmak izi teknolojisi, kullanıcıya özgü benzersiz verilerle ek bir güvenlik katmanı oluşturur.
- 4 Parmak izi okuma, yüksek doğruluk ve hızlı tarama özellikleri sayesinde güvenlik seviyesini artırmaktadır.
- 5 NFC ve biyometrik doğrulamanın birlikte kullanımı, yetkisiz erişimi neredeyse imkânsız hale getirerek güvenlik risklerini en aza indirir.



MOTİVASYON VE KATKILAR

MOTİVASYON

- Fiziksel anahtarlar güvenlik açıkları yaratır (kayıp, kopyalama, çalınma)
- Tek faktörlü akıllı kilitler güvenlik tehditleri oluşturur
- NFC ve biyometrik doğrulamayı birleştiren çok katmanlı kimlik doğrulama ihtiyacı

KATKILAR

- Bu çalışma, fiziksel anahtarların güvenlik risklerini ortadan kaldırarak kullanıcılar daha güvenli ve pratik erişim imkanı sunmuştur.
- Sistem mimarisi ve donanım-yazılım entegrasyonunda özgün çözümler geliştirerek, uygun maliyetli ve yüksek güvenlikli akıllı kilit sistemlerinin oluşturulmasına katkı sağlamıştır.
- Proje, geliştirilen protokol ve bileşen uyumluluğu ile benzer çalışmalar için model teşkil etmiş ve teknoloji entegrasyonunda yenilikçi perspektifler kazandırmıştır.

LITERATÜR ÖZETİ

Akıllı ev teknolojilerinin yaygınlaşmasıyla, erişim kontrolünde NFC ve RFID tabanlı akıllı kilit sistemleri öne çıkmaktadır.

NFC teknolojisi, düşük enerji tüketimi ve hızlı doğrulama sağlasa da man-in-the-middle ve replay saldırılara karşı savunmasızdır.

Biyometrik sistemler (parmak izi gibi) yüksek doğruluk sunar ancak kayıt süreçleri karmaşık ve maliyetlidir.

Tuş takımı PIN sistemleri basit ve kullanışlı olsa da şifre sızıntısı durumunda güvenlik zayıflığı oluşur.

NFC tabanlı kilitler uygun maliyetlidir, ancak tek başına kullanıldığında kart kopyalama riski taşır.

Biyometrik sistemler güvenliği artırır, ancak yüksek donanım ve yazılım altyapısı gerektirir.

PIN tabanlı sistemler pratik olsa da kullanıcı hataları veya tahmin saldırılarına açıktır.

Teknoloji entegrasyonu eğilimi, bu sistemlerin zayıf yönlerini dengelemek için artmaktadır.

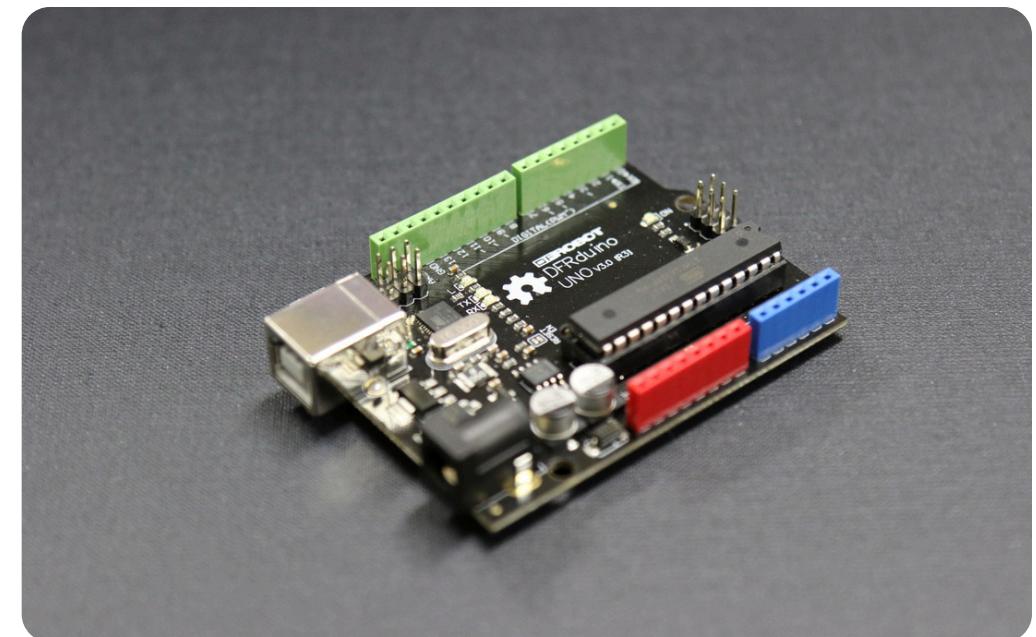
Çok faktörlü doğrulama (NFC + biyometri + PIN) güvenlik açılarını en aza indirmekte etkilidir.

Akademik ve endüstriyel çalışmalar, hibrit sistemlerin erişim güvenliğini önemli ölçüde artırdığını göstermektedir.

Gelecekteki akıllı kilit sistemleri, kullanıcı dostu ve yüksek güvenlikli çoklu doğrulama yöntemlerine odaklanacaktır.

Teknolojik gelişmelerle birlikte, entegre akıllı kilit çözümlerinin yaygınlaşması beklenmektedir.

DONANIM BİLEŞENLERİ



4x4 Tuş Takımı

4x4 Tuş Takımı, kullanıcıların PIN girişi yaparak ek kimlik doğrulama sağlamasına olanak tanır ve NFC/biyometri ile kombine edilerek güvenlik artırılır.

RC522 NFC Okuyucu

RC522 NFC Okuyucu, akıllı kartlarla kısa mesafeli iletişim kurar ve misafir erişim kontrolü için kullanılır.

Misafir kartı tanımlanmamışsa, sistem erişimi otomatik olarak reddeder ve "Erişim reddedildi" uyarısı gösterir.

R503 Parmak İzi Modülü

R503 Parmak İzi Modülü, hızlı tarama (0.3 saniye) ve yüksek doğruluk orANIyla kullanıcı kimlik denetimi sağlar.

Sistem, NFC, PIN ve parmak izini birleştirerek çok katmanlı bir güvenlik sunar. Tüm entegrasyonlar, yetkisiz erişimi engelleyerek kayıtlı ve kontrollü girişü garanti eder.

PROJENİN UYGULANMASI

```
// — Sabitler ve Pin Tanımları —
#define LCD_ADDRESS      0x27
#define RELAY_PIN         7
#define SDA_PIN           10 // UNO'da RC522 CS olarak D10 kullanıyoruz
#define RST_PIN           9 // UNO'da RC522 RST olarak D9 kullanıyoruz

#define EEPROM_UID_SIZE_ADDR 0 // EEPROM[0] = storedUIDSize
#define EEPROM_UID_BASE_ADDR 1 // EEPROM[1..] = storedUID[]

const uint16_t FINGER_ID = 1;
const String MASTER_PASS = "123";

// Parmak izi modülü için SoftwareSerial (UNO'da)
SoftwareSerial fingerSS(2, 3); // RX = D2, TX = D3 (UNO'da istediğiniz digital pin olur)
Adafruit_Fingerprint finger(&fingerSS);

MFRC522 mfrc522(SDA_PIN, RST_PIN);
LiquidCrystal_I2C lcd(LCD_ADDRESS, 16, 2);

// Keypad
const byte ROWS = 4, COLS = 4;
char keys[ROWS][COLS] = {
    {'1', '2', '3', 'A'},
    {'4', '5', '6', 'B'},
    {'7', '8', '9', 'C'},
    {'*', '0', '#', 'D'}
};
```

Entegrasyon, Performans ve Güvenlik Analizi

Donanım ve Yazılım Entegrasyonu: Arduino tabanlı bir sistemle NFC, parmak izi ve tuş takımı modülleri optimize edilerek entegre edilmiştir.

Test ve Performans: Her modülün tek başına ve birlikte çalışma performansı test edilmiş, hızlı ve hatasız çalışması sağlanmıştır.

Güvenlik Analizi: Sistemin zayıflıkları ve olası saldırı yöntemleri (NFC klonlama, parmak izi taklidi) detaylıca incelenmiştir.

Çok Faktörlü Kimlik Doğrulama Sisteminde Savunma Mekanizmaları

Koruma Önlemleri: Kopyalama ve taklit saldırılarına karşı yazılımsal önlemler alınmış, güvenlik artırılmıştır.

Yazılım Güvenliği: Kodun güncel tutulması ve güvenlik açıklarının hızlıca kapatılması vurgulanmıştır.

Çok Katmanlı Doğrulama: NFC, PIN ve biyometri kombinasyonuyla yetkisiz erişim riski minimize edilmiştir.

ANALOG VS DİJİTAL

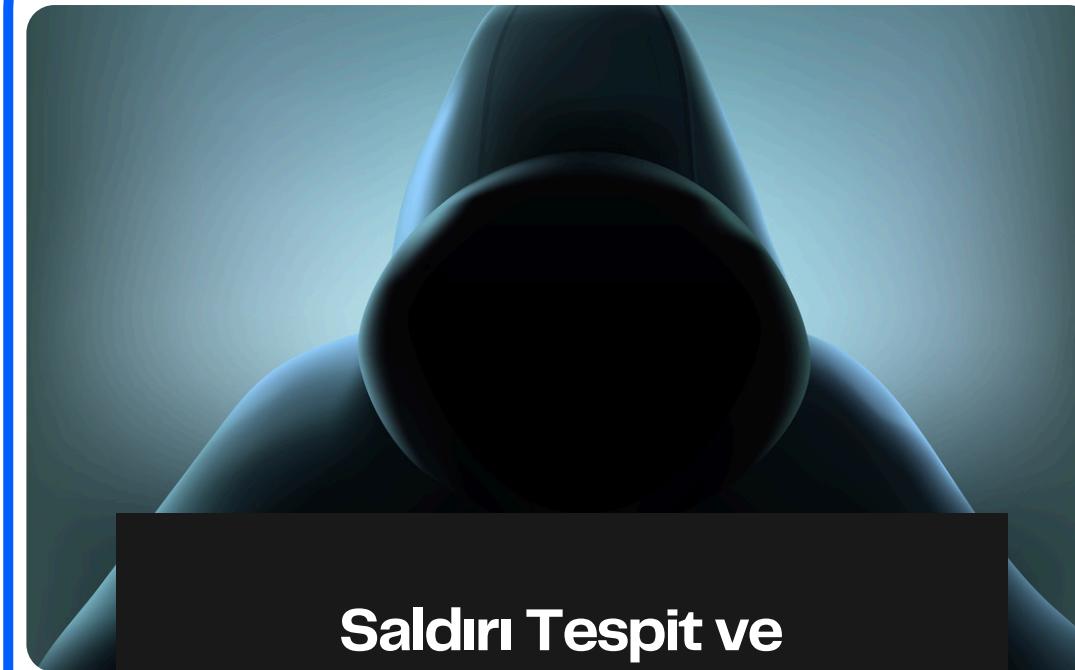
ANALOG VE DİJİTAL KİLİT SİSTEMLERİNİN KARŞILAŞTIRILMASI



Yetkisiz Erişim Başarı Oranı

- Analog kilitler, fiziksel kopyalama (anahtar kopyalama, lock picking) nedeniyle %60-70 oranında bypass edilebiliyor.
- Dijital kilitler (NFC/Parmak izi/PIN kombinasyonlu) çok faktörlü doğrulama sayesinde bu risk %5-2 oranında

(Kaynak: ASIS International, 2023)



Saldırı Tespit ve Önleme Süresi

- Analog kilitlerde izinsiz girişler genellikle sonradan fark ediliyor (ortalama 8-12 saat).
- Dijital sistemler, anormal erişim girişimlerini gerçek zamanlı tespit edip <1 saniye içinde alarm verebiliyor.

(Kaynak: IEEE Security & Privacy, 2022)



Güvenlik İhlali Maliyetleri

- Analog kilitli sistemlerde bir ihlalin ortalama maliyeti \$3,000-\$5,000 (anahtar değişimi, güvenlik açığı onarımı).
- Dijital sistemlerde uzaktan erişim iptali ve otomatik güncellemelerle bu maliyet %80 daha düşük

(Kaynak: Gartner, 2023)

GELİŞTİRİLEBİLECEK VÖNLERİ VE YOL HARİTASI

Farklı Biyometrik Doğrulama Yöntemleri

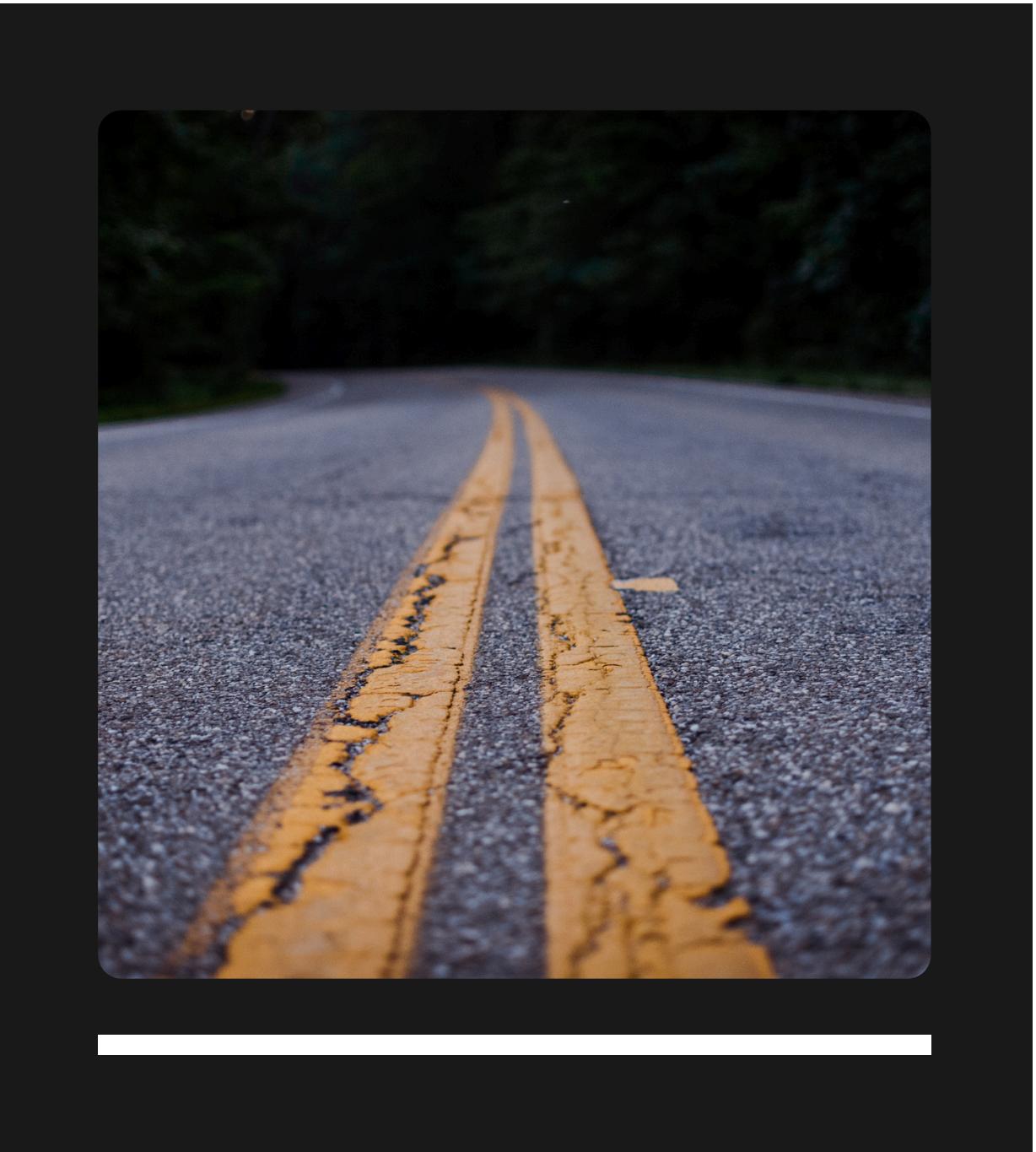
Parmak izine ek olarak yüz tanıma, iris tarama veya ses tanıma gibi alternatif biyometrik sistemlerin entegrasyonu.

Sosyal Mühendislik Senaryolarına Karşı Önlemler

Kullanıcıları şifre paylaşımı veya zorla erişim durumlarına karşı uyanan bir eğitim modülü veya acil durum butonu.

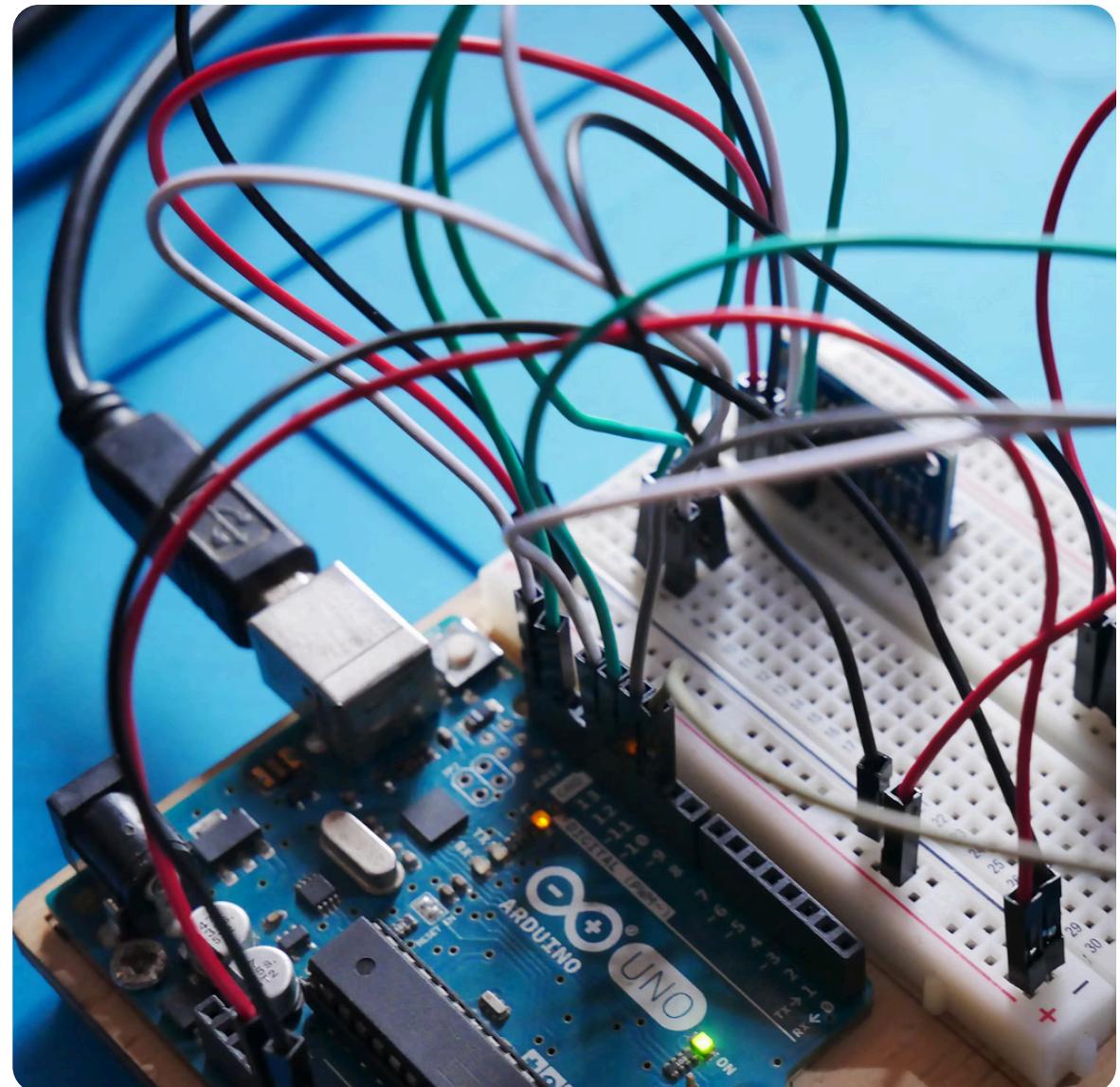
Genişletilebilir Modüler Yapı

Farklı güvenlik seviyelerine uyum sağlamak için ek doğrulama modüllerinin (örneğin, OTP veya davranışsal biyometri) kolayca eklenebileceği esnek bir altyapı.



SONUÇLAR

- 1 Bu tez çalışmasında geliştirilen iki faktörlü NFC tabanlı akıllı kilit sistemi, güvenlik ve kullanıcı dostu bir deneyim sunarak başarılı sonuçlar vermiştir.
- 2 Sistemin entegrasyonu sırasında yüksek uyumluluk ve performans gözlemlenmiş, ancak teknik zorluklar ve iyileştirilecek yönler tespit edilmiştir.
- 3 Gelecek çalışmalar için kriptografik doğrulama, IoT entegrasyonu ve uzaktan yönetim gibi güvenlik özelliklerinin geliştirilmesi planlanmaktadır.
- 4 İki faktörlü doğrulamanın NFC ve biyometri tabanlı akıllı kilitlerde etkili olduğu kanıtlanmış, prototip güvenli ve pratik bir erişim çözümü sunmuştur.
- 5 Önerilen iyileştirmeler arasında kullanıcı deneyiminin artırılması, maliyet optimizasyonu ve daha gelişmiş şifreleme tekniklerinin uygulanması yer almaktadır.



KAYNAKÇA

- Arduino Documentation. (2025, January 1). *UNO R3 – Arduino Documentation*. <https://docs.arduino.cc/hardware/uno-rev3>
- University of Kentucky. (2024, October 24). *Why you should be using multifactor authentication for all your online accounts*. <https://itsuky.edu/news/why-you-should-be-using-multifactor-authentication-all-your-online-accounts>
- Chief Information Officer Council. (2022, October 26). *The importance of multifactor authentication*. <https://www.cio.gov/2022-10-26-importance-multifactor-authentication>
- ResearchGate. (n.d.). *Arduino Uno: The Arduino UNO is a widely used open-source microcontroller board based on the ATmega328P microcontroller and developed by Arduino.cc*. https://www.researchgate.net/figure/Arduino-Uno-The-Arduino-UNO-is-a-widely-used-open-source-microcontroller-board-based-on_fig3_325220732
- How2Electronics. (2022, April 19). *Interfacing R502/R503 Capacitive Fingerprint Sensor with Arduino*. <https://how2electronics.com/interfacing-r502-r503-capacitive-fingerprint-sensor-with-arduino>
- nfc-rfid-reader-sdk. (2023, August 1). *MFRC522_PN512: PN512 NFC Reader Library* [GitHub repository]. https://github.com/nfc-rfid-reader-sdk/MFRC522_PN512
- The Stempedia. (2023, August 23). *Interfacing 4x4 Keypad Module with Arduino (Part 1) – Example Project*. <https://ai.thestempedia.com/example/interfacing-4x4-keypad-module-with-arduino-part-1>
- ResearchGate. (2025, January 9). *Multi-security system based on RFID fingerprint and keypad to access the door*. https://www.researchgate.net/publication/364400152_Multi-Security_System_Based_on_RFID_Fingerprint_and_Keypad_to_Access_the_Door

TEŞEKKÜRLER

Hazırlayan ve Sunan

BAHA ALAGÖZ-ARDA İRDEP

DANIŞMAN

ELİF DENİZ YİĞİTBAŞI