IŞIK ÜNİVERSİTESİ

İktisadi, İdari ve Sosyal Bilimler Fakültesi

Enformasyon Teknolojileri Bölümü

Yönetim Bilişim Sistemleri Programı

Lisans Tezi

2 Faktör Doğrulamalı NFC Tabanlı Akıllı Kilit Sistemlerinin Geliştirilmesi ve Güvenlik Açısından Değerlendirilmesi

Sunan:

BAHA ALAGÖZ 20YOBI1020

ARDA İRDEP 21YOBI1049

Tez Danışmanı: Elif Deniz Yelmenoğlu

06-2025

Özet

Bu tez çalışmasında, iki faktörlü doğrulama sistemi kullanılarak NFC (Near Field Communication) tabanlı akıllı kilit sistemlerinin tasarımı ve geliştirilmesi gerçekleştirilmiştir. Sisteme RC522 NFC kart okuyucu modülü, 4x4 tuş takımı ve R503 parmak izi sensörü entegre edilerek çift aşamalı kimlik doğrulama protokolü oluşturmuştur. Bu sayede, fiziksel anahtarların yol açtığı güvenlik zafiyetleri önemli ölçüde azaltılmıştır. Donanım ve yazılım bileşenleri arasında etkin bir entegrasyon sağlanmış, sistem kapsamlı testlere tabi tutulmuştur. Testler sonucunda sistem performansı analiz edilmiş, kullanım kolaylığı ve güvenlik dengesi incelenmiştir. Potansiyel güvenlik açıkları tespit edilip, sistemin dayanıklılığını artıracak iyileştirme önerileri sunulmuştur. Ayrıca, kullanıcıların güvenliğini sağlamak için çok katmanlı doğrulama yöntemlerinin etkinliği vurgulanmıştır. Bu tez çalışması, erişim kontrolünde yüksek güvenlik sunan ve pratik kullanım sağlayan bir akıllı kilit sistemi modeli ortaya koymuştur.

Sonuç olarak, proje hem teorik hem de uygulamalı açıdan akıllı kilit teknolojilerine önemli katkılar sağlamıştır.

İçindekiler

Şekil Listesi

Bölüm 1: Giriş

1.1 Giriş

Son yıllarda teknolojinin hızlı gelişimi ve akıllı cihazların hayatımıza giderek daha fazla entegre olması güvenlik sistemlerinde önemli değişimlere yol açmıştır. Bu değişimlerin en dikkat çekeni, geleneksel anahtar sistemlerinin yerini alan akıllı kilit sistemlerinin yaygınlaşmasıdır. Akıllı kilitler, sadece kapıyı açıp kapatmanın ötesinde kullanıcıların kimlik bilgilerini doğrulayarak daha güvenli ve pratik bir erişim kontrolü sunmaktadır. NFC teknolojisi, temassız iletişim ve hızlı veri aktarımı özellikleriyle, ev, ofis ve endüstriyel alanlarda erişim kontrolünde büyük kolaylık sağlamaktadır. Temassız olması sebebiyle kullanıcılar sadece kart veya cihazlarını kilide yaklaştırarak hızlı ve güvenli şekilde erişim elde edebilmektedir. Ayrıca, biyometrik doğrulama sistemleri, özellikle parmak izi teknolojisi, kullanıcıya özgü benzersiz verilerle ikinci bir güvenlik katmanı oluşturarak yetkisiz erişimleri engellemektedir. Parmak izi okuma, yüksek doğruluk oranı ve hızlı tarama özellikleri sayesinde kullanıcıların güvenlik seviyesini artırmaktadır. Bu iki teknolojinin bir arada kullanılması, sistemde yetkisiz kişilerin erişimini neredeyse imkânsız hale getirmekte ve güvenlik risklerini minimize etmektedir. Sonuç olarak, NFC ve biyometrik tabanlı akıllı kilit sistemleri, modern yaşamın gereksinimlerine uygun olarak hem güvenlik hem de kullanım kolaylığı açısından etkili çözümler sunmaktadır.

1.2 Motivasyon

Fiziksel anahtarların kaybolması, kopyalanması veya çalınması gibi riskler göz önüne alındığında, tek faktörlü akıllı kilit sistemlerinin güvenlik açığı yaratabileceği anlaşılmaktadır. Bu sebeple, hem

NFC kart doğrulaması hem de biyometrik verinin beraber kullanıldığı iki faktörlü sistemler geliştirilmiştir. Bu birleşik doğrulama yöntemi, sistemin sadece yetkili kullanıcılar tarafından açılmasını garanti eder. Ayrıca kullanıcı alışkanlıklarını kolaylaştırmak, misafir erişimini güvenli bir şekilde yönetmek ve sistemin güvenlik açıklarını minimuma indirmek bu çalışmanın önemli motivasyonlarını oluşturmaktadır.

1.3 Katkılar

Çalışma, fiziksel anahtar kullanımına bağlı güvenlik risklerini azaltarak kullanıcıların daha güvenli ve pratik erişim sağlamasına olanak tanımıştır. Ayrıca, sistem mimarisi tasarımı ve donanım-yazılım entegrasyonu alanında özgün çözümler sunarak, uygun maliyetli ve yüksek güvenlikli akıllı kilit sistemlerinin geliştirilmesine katkıda bulunmuştur.

Proje, geliştirilen protokol ve kullanılan bileşenlerin uyumlu çalışması, benzer projelerde kullanılmak üzere model oluşturmuş ve teknoloji entegrasyonunda yenilikçi bakış açıları kazandırmıştır.

Bölüm 2: Literatür Özeti

2.1 Genel Bakış

Günümüzde akıllı ev sistemlerinin yaygınlaşmasıyla birlikte, güvenlik ve erişim kontrolüne yönelik çözümler büyük önem kazanmıştır. Geleneksel anahtar sistemlerinin yerini alan akıllı kilit teknolojileri, kullanıcı dostu arayüzleri ve gelişmiş doğrulama yöntemleriyle dikkat çekmektedir. Bu bağlamda, yakın alan iletişimi (NFC) ve radyo frekanslı tanımlama (RFID) gibi teknolojiler, düşük güç tüketimi ve hızlı veri aktarımı avantajlarıyla erişim kontrol sistemlerinde yaygın olarak kullanılmaktadır (6). Ancak, bu sistemlerin tek başına kullanımı, kart kopyalama veya elektronik dinleme gibi siber saldırılara karşı savunmasız kalabilmektedir (3).

Biyometrik doğrulama yöntemleri, özellikle parmak izi tanıma sistemleri, yüksek güvenlik seviyesi ve kullanıcı kolaylığı sunmaktadır. Bununla birlikte, bu sistemlerin uygulanması sırasında karşılaşılan yüksek donanım maliyetleri ve karmaşık yazılım gereksinimleri, kullanıcılar için dezavantaj oluşturabilmektedir (5). PIN tabanlı tuş takımı sistemleri ise basit yapıları ve düşük maliyetleri nedeniyle yaygın olarak tercih edilmektedir. Ancak, bu sistemlerde kullanıcıların zayıf şifre seçimleri veya şifrelerin yetkisiz kişilerin eline geçmesi, güvenlik açıklarına yol açabilmektedir (7). Bu nedenle, günümüzde çok faktörlü kimlik doğrulama (MFA) sistemleri, farklı teknolojilerin bir arada kullanılmasıyla daha güvenli çözümler sunmayı hedeflemektedir (2).

2.2 Mevcut Sistemlerin İncelenmesi

NFC ve RFID tabanlı sistemler, temas gerektirmeden çalışabilme özellikleri sayesinde kullanıcılar için büyük kolaylık sağlamaktadır. Özellikle Arduino gibi açık kaynaklı platformlarla entegre edilebilen bu sistemler, düşük maliyetli ve esnek çözümler sunmaktadır (Arduino Documentation, 2025). Ancak, bu sistemlerin tek faktörlü yapısı, kartların kopyalanması veya sinyallerin ele geçirilmesi durumunda güvenlik açıklarına yol açabilmektedir (ResearchGate, 2025). Bu riskleri en

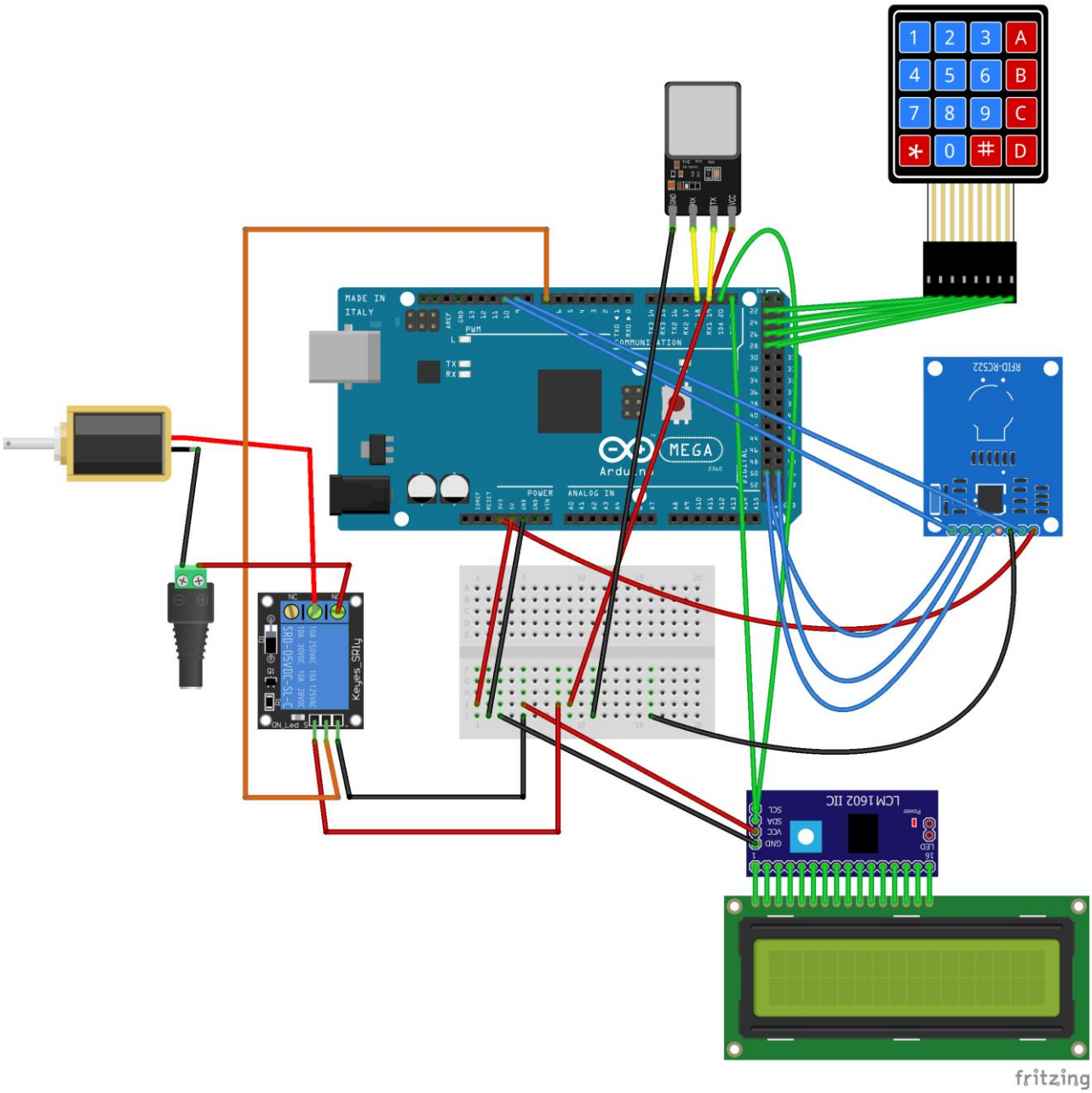
aza indirmek için, NFC tabanlı sistemlerin biyometrik doğrulama veya PIN gibi ek güvenlik katmanlarıyla desteklenmesi önerilmektedir.

Biyometrik sistemler, bireye özgü fiziksel özelliklerin kullanılması nedeniyle yüksek güvenlik seviyelerine ulaşabilmektedir. Parmak izi tanıma sistemleri, özellikle R502/R503 gibi kapasitif sensörlerle yüksek doğruluk oranları sunmaktadır (How2Electronics, 2022). Ancak, bu sistemlerin kurulumu ve bakımı sırasında karşılaşılan yüksek maliyetler, küçük ölçekli uygulamalarda kullanımını sınırlandırabilmektedir. Ayrıca, biyometrik verilerin depolanması sırasında ortaya çıkabilecek veri ihlali riskleri, bu sistemlerin dikkatli bir şekilde yönetilmesini gerektirmektedir.

Tuş takımı tabanlı sistemler, özellikle basit kullanım ve düşük maliyet avantajları nedeniyle yaygın olarak tercih edilmektedir. 4x4 tuş takımları gibi modüller, Arduino gibi mikrodenetleyicilerle kolayca entegre edilebilmekte ve kullanıcı dostu çözümler sunmaktadır (The Stempedia, 2023). Ancak, bu sistemlerde kullanıcıların tahmin edilebilir şifreler seçmesi veya şifrelerin başkaları tarafından öğrenilmesi, güvenlik açıklarına yol açabilmektedir.

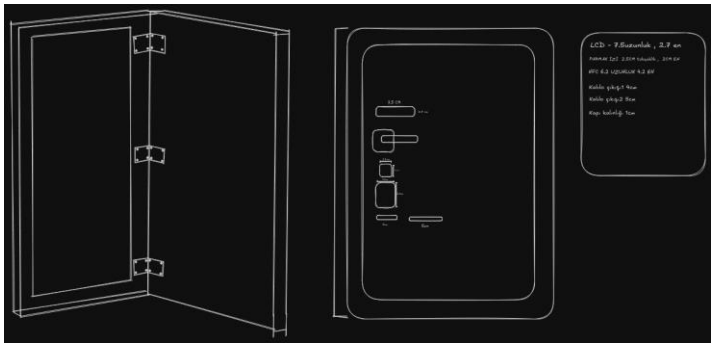
Bu nedenle, son yıllarda çok faktörlü kimlik doğrulama sistemleri giderek daha fazla önem kazanmaktadır. Özellikle NFC, biyometrik veri ve PIN tabanlı sistemlerin bir arada kullanılması, güvenlik açıklarını en aza indirmektedir (University of Kentucky, 2024). Araştırmalar, bu tür hibrit sistemlerin tek faktörlü sistemlere kıyasla çok daha güvenli olduğunu göstermektedir (Chief Information Officer Council, 2022). Örneğin, ResearchGate'de yayınlanan bir çalışmada, RFID, parmak izi ve tuş takımının bir arada kullanıldığı bir sistemin, geleneksel yöntemlere kıyasla çok daha yüksek güvenlik sağladığı belirtilmektedir (ResearchGate, 2025).

Bölüm 3 Devre Şeması

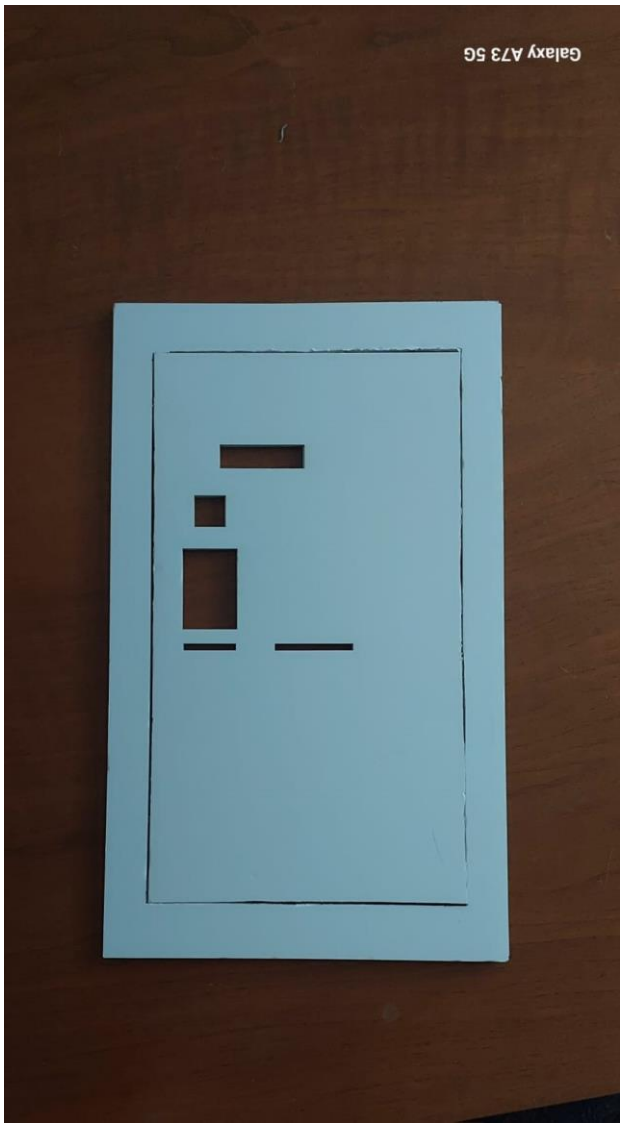


Şekil 1 – Fritzing devre şeması

Bölüm 4 Proje Fotoğrafları



Şekil 2 - Kapı mock design



Şekil 3 - Kapı çerçeve tasarımı

Şekil 4 - Tahtadan kapı modeli

Şekil 5 - Kapı son hali

Bölüm 5: 2 Faktör Doğrulamalı NFC Tabanlı Akıllı Kilit Sistemlerinin Geliştirilmesi ve Güvenlik Açısından Değerlendirilmesi

5.1 Giriş

Güvenli erişim için çok faktörlü doğrulama, kimlik doğrulamada artan güvenlik katmanı sağlar. NFC ve biyometrik tabanlı sistemlerin beraber kullanımı, özellikle konut ve iş yerlerinde yaygınlaşmaktadır. Bu bölümde, NFC tabanlı kart doğrulama ve parmak izi okuma modüllerinin birleşik çalışması için gerekli altyapı ve yazılım mimarisi detaylandırılmıştır.

5.2 Donanım ve Yazılım Entegrasyonu

RC522 NFC modülü, SPI iletişim protokolü kullanarak mikrodenetleyici ile haberleşmektedir. Kart numarası okunduktan sonra doğrulama için mikrodenetleyiciye iletilir. Parmak izi modülü ise UART haberleşme protokolüyle entegre edilerek kullanıcıdan alınan biyometrik veriyle kimlik doğrulaması yapılır. Bu iki sistem arasındaki koordinasyon, yazılım tabanlı bir kontrol algoritması ile sağlanmıştır.

5.3 İki Faktörlü Doğrulama Prosedürü

Sistem İşleyişi:

Sistem ilk açıldığında EEPROM'da kayıtlı bir şifrenin olup olmadığını kontrol eder. Eğer şifre bulunmuyorsa, kullanıcıdan yeni bir şifre belirlemesi istenir.

Ana İşlem Akışı:

- Kullanıcı tarafından girilen şifre doğrulanır. Doğru şifre girilirse, sistem menüye erişim sağlar.

Menü Seçenekleri:

- **Giriş:** RFID kart ve parmak izi doğrulaması yapılır. Her iki faktör de onaylanırsa, röle 5 saniye boyunca aktif hale gelir.
- **Kayıt:** Master kart kullanılarak yeni bir kullanıcı eklenir (RFID kart bilgisi ve parmak izi ID'si kaydedilir).
- **Şifre Değiştirme:** Master kartla yetkilendirme yapıldıktan sonra sistem şifresi güncellenebilir.

Veri Saklama ve Güvenlik:

- EEPROM, şifre, RFID UID ve parmak izi ID'si gibi kritik verileri kalıcı olarak depolar.
- Sistem, master kart olmadan yeni kayıt veya şifre değişikliği işlemlerine izin vermez, böylece yetkisiz erişim engellenir.

Bölüm 6: 4x4 Tuş Takımı Modülü Entegrasyonu

6.1 Giriş

4x4 tuş takımı, kullanıcıların ilave kimlik doğrulama için PIN girmesine olanak sağlar. Bu modül, yapısı itibarıyla 16 ayrı giriş sunar ve mikrodenetleyici tarafından kolaylıkla yönetilebilir. Güvenlik açısından PIN, NFC ve biyometri kombinasyonuna ek bir katman sağlar.

Bölüm 7: RC522 NFC Kart Okuyucu Entegrasyonu

7.1 Giriş

RC522 modülü, akıllı kartlar ve etiketler ile kısa mesafeli (yaklaşık 3–5 cm) temas gerektiren iletişim sağlar. Hafif yapısı ve kolay programlanabilir olması sebebiyle projelerde yaygın olarak tercih edilir.

7.2 Misafir Anahtarı Entegrasyonu

Sistemimizde misafir kartı entegrasyonu, ziyaretçi güvenliği ve kontrolünü sağlamak amacıyla titizlikle tasarlanmıştır. Eğer bir misafir kartında ne NFC ne de parmak izi tanımlaması mevcutsa, sistem erişimi otomatik olarak engellemektedir. Bu durumda, LCD ekran üzerinde "Yetkisiz Erişim" mesajı görüntülenir ve misafir kaydı tamamlanmadan sisteme giriş mümkün olmaz.

Bu yöntem sayesinde, yetkisiz kişilerin erişimi önlenmekte ve misafirlerin sisteme kaydı mutlaka doğrulanarak gerçekleştirilmiş olmaktadır.

Bölüm8: R503 Parmak İzi Modülü Entegrasyonu

8.1 Giriş

R503 modülü kompakt tasarımı ve hızlı tarama kabiliyeti ile parmak izi doğrulamada etkin bir bileşen olarak öne çıkar. Yüksek başarı oranı, düşük hata payı ve hafıza kapasitesi ile farklı kullanıcı kayıtlarını tutabilir.

8.2 Entegrasyon Detayları

- UART iletişimi ile mikrodenetleyiciye bağlıdır.
- Parmak izi tarama süresi ortalama 0.3 saniyedir.

Bölüm 9: Proje Kodu ve Açıklaması

Bu kod, bir güvenlik sistemi için yazılmış bir Arduino programıdır. Sistem, bir RFID kart okuyucu (MFRC522), parmak izi sensörü (Adafruit_Fingerprint), LCD ekran (LiquidCrystal_I2C), 4x4 tuş takımı (Keypad) ve EEPROM bellek kullanarak kullanıcı girişi, kayıt ve şifre yönetimi işlemlerini gerçekleştirir. Ayrıca bir röle (RELAY_PIN) aracılığıyla fiziksel bir cihazı (kilit) kontrol eder. Aşağıda, kodun işleyişi adım adım açıklanmıştır:

9.1 Kütüphaneler ve Tanımlamalar

```
#include <SPI.h>
#include <MFRC522.h>
#include <Adafruit_Fingerprint.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>
#include <EEPROM.h>
```

- **SPI.h**: RFID modülü ile iletişim için seri periferal arayüzü (SPI) kütüphanesi.
- **MFRC522.h**: RFID kart okuyucu için kütüphane.
- **Adafruit_Fingerprint.h**: Parmak izi sensörü için kütüphane.
- **Wire.h**: I2C protokolü ile LCD ekran için iletişim sağlar.
- **LiquidCrystal_I2C.h**: I2C üzerinden 20x2 LCD ekran kontrolü için.
- **Keypad.h**: 4x4 tuş takımı için kütüphane.
- **EEPROM.h**: Kalıcı veri saklama için Arduino'nun EEPROM belleğini kullanır.

Pin ve Sabit Tanımlamaları

```
#define RELAY_PIN    7
#define SS_PIN       10
#define RST_PIN      9
#define MAX_PASS_LEN 10
#define PASS_ADDR    20
#define UID_ADDR     40
#define FID_ADDR     60
```

- **RELAY_PIN (7)**: Röle kontrol pini (örneğin, kapı kilidi).
- **SS_PIN (10), RST_PIN (9)**: RFID modülünün Slave Select ve Reset pinleri.
- **MAX_PASS_LEN (10)**: Şifrenin maksimum uzunluğu.
- **PASS_ADDR (20), UID_ADDR (40), FID_ADDR (60)**: EEPROM'da şifre, RFID kart UID'si ve parmak izi ID'sinin saklanacağı adresler.

Nesneler ve Sabitler

```
MFRC522 rfid(SS_PIN, RST_PIN);
Adafruit_Fingerprint finger(&Serial1);
LiquidCrystal_I2C lcd(0x3F, 20, 2);
```

- **rfid**: RFID okuyucu nesnesi.
- **finger**: Parmak izi sensörü nesnesi (Serial1 üzerinden iletişim kurar).
- **lcd**: 20x2 I2C LCD ekran nesnesi, adresi 0x3F.

Tuş Takımı Tanımlamaları

```
const byte ROWS = 4, COLS = 4;
char keys[ROWS][COLS] = {{'1','2','3','A'},{'4','5','6','B'},{'7','8','9','C'},{'*','0','#','D'}};
byte rowPins[ROWS] = {22,23,24,25};
byte colPins[COLS] = {26,27,28,29};
Keypad keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS);
```

- 4x4 tuş takımı matrisi tanımlanır. Tuşlar, keys dizisinde belirtilir (0-9, A-D, *, #).
- **rowPins** ve **colPins**: Tuş takımı pin bağlantıları.
- **keypad**: Tuş takımı nesnesi.

Master Kart UID

```
const byte masterUID[7] = {0x04,0x43,0x7C,0xA7,0x30,0x02,0x89};
```

- Sistemde yönetici (master) kartın benzersiz kimliği (UID).

9.2. setup() Fonksiyonu

```
void setup() {
  pinMode(RELAY_PIN, OUTPUT); digitalWrite(RELAY_PIN, LOW);
  Serial.begin(9600); Serial1.begin(57600);
  SPI.begin(); rfid.PCD_Init(); finger.begin(57600);
  lcd.init(); lcd.backlight();
  byte first = EEPROM.read(PASS_ADDR);
  if (first==0xFF || first==0) setInitialPassword();
}
```

- **Röle pini**: Çıkış olarak ayarlanır ve başlangıçta kapalı (LOW).
- **Seri iletişim**: Serial (9600 baud) hata ayıklama için, Serial1 (57600 baud) parmak izi sensörü için başlatılır.
- **SPI ve RFID**: SPI başlatılır ve RFID modülü hazır hale getirilir.
- **Parmak izi sensörü**: 57600 baud ile başlatılır.
- **LCD**: Ekran başlatılır ve arka ışık açılır.
- **EEPROM kontrolü**: İlk şifre kontrol edilir. Eğer EEPROM'daki PASS_ADDR adresi boş (0xFF veya 0) ise, setInitialPassword() ile şifre belirlenir.

9.3 Loop() Fonksiyonu

```
void loop() {
  if (checkPassword()) showMenu();
  else { lcd.clear(); lcd.print("Sifre Yanlis"); delay(1500); }
}
```

Ana döngü: Kullanıcıdan şifre istenir (checkPassword()).

- Şifre doğruysa, showMenu() ile menü gösterilir.
- Şifre yanlışsa, "Şifre Yanlış" mesajı 1.5 saniye görüntülenir ve döngü başa döner.

9.4 Şifre İşlemleri

a. setInitialPassword()

```
void setInitialPassword() {
  String p1 = getPasswordInput("Sifre Belirle:");
  String p2 = getPasswordInput("Tekrar Gir:");
  if (p1!=p2) { lcd.clear(); lcd.print("Uyusmuyor"); delay(1500); return setInitialPassword(); }
  for (int i=0;i<MAX_PASS_LEN;i++) EEPROM.update(PASS_ADDR+i, i<p1.length()?p1[i]:0);
  lcd.clear(); lcd.print("Sifre Kaydedildi"); delay(1500);
}
```

- İlk şifre belirleme işlemi.
- Kullanıcıdan iki kez şifre alınır (p1 ve p2).
- Şifreler uyuşmazsa, hata mesajı gösterilir ve fonksiyon tekrar çağrılır.
- Uyuşursa, şifre EEPROM'a kaydedilir (her karakter bir bayt olarak, fazla alanlar 0 ile doldurulur).

b. checkPassword()

```
bool checkPassword() {
  String ent = getPasswordInput("Sifre:");
  String st="";
  for(int i=0;i<MAX_PASS_LEN;i++){ char c=EEPROM.read(PASS_ADDR+i);
if(c==0||c==0xFF) break; st+=c; }
  return ent==st;
}
```

- Kullanıcıdan şifre alınır (getPasswordInput).
- EEPROM'daki şifre okunur ve bir string (st) oluşturulur.
- Girilen şifre (ent) ile EEPROM'daki şifre karşılaştırılır, doğruysa true döner.

c. getPasswordInput()

```
String getPasswordInput(String msg) {
  lcd.clear(); lcd.print(msg); lcd.setCursor(0,1);
  String s=""; char k;
  while(true){
    k=keypad.getKey(); if(!k)continue;
    if(k=='#')break;
```

```
    if(k=='*'&&s.length()){ s.remove(s.length()-1); lcd.setCursor(s.length(),1); lcd.print(' ');
lcd.setCursor(s.length(),1); }
    else if(k>='0'&&k<='9'&&s.length()<MAX_PASS_LEN){ s+=k; lcd.print('*'); }
  }
  return s;
}
```

- Belirtilen mesaj (msg) LCD'de gösterilir.
- Kullanıcı tuş takımından şifre girer:
- #: Girişi tamamlar.
- *: Son karakteri siler.
- 0-9: Şifreye eklenir (maksimum MAX_PASS_LEN).
- Her karakter girildiğinde LCD'de * gösterilir (gizlilik için).
- Girilen şifre bir String olarak döner.

9.5 Menü ve Kullanıcı İşlemleri

a. showMenu()

```
void showMenu() {
  lcd.clear(); lcd.print("1:Giris 2:Kayit"); lcd.setCursor(0,1); lcd.print("3:SifreDegistir");
  while(true){ char k=keypad.getKey();
    if(k=='1'){ loginUser(); break; }
    if(k=='2'){ registerUser(); break; }
    if(k=='3'){ changePassword(); break; }
  }
}
```

- LCD'de menü gösterilir: 1-Giriş, 2-Kayıt, 3-Şifre Değiştir.
- Kullanıcı 1, 2 veya 3 tuşuna basarak ilgili işlemi başlatır.

b. loginUser()

```
void loginUser() {
  lcd.clear(); lcd.print("Kart okutun");
  byte uid[10], len = readUID(uid); if(len==0){ lcd.clear(); lcd.print("Kart yok"); delay(1500);
return; }
  bool m=(len==7&&memcmp(uid,masterUID,7)==0);
  if(!m){ byte sl=EEPROM.read(UID_ADDR), su[10]; for(int i=0;i<sl;i++)
su[i]=EEPROM.read(UID_ADDR+1+i);
    if(len!=sl||memcmp(uid,su,len)) { lcd.clear(); lcd.print("Yetkisiz"); delay(1500); return; }
  }
  lcd.clear(); lcd.print("Parmak:"); int fid=getFingerprintID();
  if((m&&fid==1)||(!m&&fid==EEPROM.read(FID_ADDR))){
    lcd.clear(); lcd.print("Giris OK"); digitalWrite(RELAY_PIN,HIGH); delay(5000);
digitalWrite(RELAY_PIN,LOW);
```

```
  } else { lcd.clear(); lcd.print("Parmak hatali"); delay(1500); }
}
```

- Kullanıcıdan RFID kart okutulur (readUID).
- Kart master UID ile eşleşirse (m=true) veya EEPROM'daki UID ile eşleşirse doğrulama geçer.
- Ardından parmak izi kontrolü yapılır (getFingerprintID):
  - Master kart için parmak izi ID'si 1 olmalı.
  - Normal kullanıcı için parmak izi ID'si EEPROM'daki FID_ADDR ile eşleşmeli.
- Başarılıysa röle 5 saniye açılır ("Giriş OK").
- Başarısızsa hata mesajı gösterilir.

c. registerUser()

```
void registerUser() {
  lcd.clear(); lcd.print("Master kart:"); if(!verifyUID(masterUID)){ lcd.clear(); lcd.print("Yetkisiz");
delay(1500); return; }
  lcd.clear(); lcd.print("Master ok"); delay(1500);
  lcd.clear(); lcd.print("Yeni kart:"); delay(500);
  byte uid[10], len=readUID(uid); if(!len){ lcd.clear(); lcd.print("Yok"); delay(1500); return; }
  EEPROM.update(UID_ADDR,len); for(int i=0;i<len;i++)
EEPROM.update(UID_ADDR+1+i,uid[i]);
  lcd.clear(); lcd.print("Parmak1/2"); if(!captureFinger(1)){ lcd.clear(); lcd.print("Hata");
delay(1500); return; }
  lcd.clear(); lcd.print("Parmak2/2"); if(!captureFinger(2)){ lcd.clear(); lcd.print("Hata");
delay(1500); return; }

if(finger.createModel()!=FINGERPRINT_OK||finger.storeModel(1)!=FINGERPRINT_OK){ lcd.cl
ear(); lcd.print("Hata"); delay(1500); return; }
```

```
  EEPROM.update(FID_ADDR,1); lcd.clear(); lcd.print("Kayit OK"); delay(1500);
}
```

Yeni kullanıcı kaydı için:

- Master kart doğrulanır (verifyUID).
- Yeni RFID kart okutulur ve UID'si EEPROM'a kaydedilir.
- Parmak izi iki kez taranır (captureFinger):
- İlk tarama buffer 1'e, ikinci tarama buffer 2'ye kaydedilir.
- Parmak izi modeli oluşturulur ve ID 1 olarak kaydedilir.
- Başarılıysa "Kayıt OK" gösterilir, hata varsa "Hata" mesajı.

d. changePassword()

```
void changePassword() {
  lcd.clear(); lcd.print("Master kart:"); if(!verifyUID(masterUID)){ lcd.clear(); lcd.print("Yetkisiz");
delay(1500); return; }
  String p1=getPasswordInput("Yeni Sifre:"), p2=getPasswordInput("Tekrar Gir:");
  if(p1!=p2){ lcd.clear(); lcd.print("Uyusmuyor"); delay(1500); return; }
  for(int i=0;i<MAX_PASS_LEN;i++) EEPROM.update(PASS_ADDR+i, i<p1.length()?p1[i]:0);
  lcd.clear(); lcd.print("Sifre degisti"); delay(1500);
}
```

Şifre değiştirme işlemi:

- Master kart doğrulanır.
- Yeni şifre iki kez alınır ve eşleşme kontrol edilir.
- Eşleşirse şifre EEPROM'a kaydedilir ve "Şifre değişti" mesajı gösterilir.

9.6 Yardımcı Fonksiyonlar

a. verifyUID()

```
bool verifyUID(const byte* ref) {
  byte u[10]; byte l=readUID(u); return l==7&&memcmp(u,ref,7)==0;
}
```

- Verilen UID ile okunan kart UID'sini karşılaştırır.
- UID uzunluğu 7 bayt olmalı ve ref ile eşleşmelidir.

b. readUID()

```
byte readUID(byte* u){
  rfid.PCD_Init();
  unsigned long t=millis();
  while(millis()-t<5000){
    if(!rfid.PICC_IsNewCardPresent()||!rfid.PICC_ReadCardSerial())continue;
    byte l=rfid.uid.size;
    memcpy(u,rfid.uid.uidByte,l);
    rfid.PICC_HaltA();
    rfid.PCD_StopCrypto1();
    return l;
  }
  return 0;
}
```

- RFID kart okur (5 saniye zaman aşımı).
- Kart varsa UID'sini u dizisine kopyalar ve uzunluğunu döner.
- Kart yoksa 0 döner.

c. captureFinger()

```
bool captureFinger(int slot){
  unsigned long t=millis();
  while(finger.getImage()!=FINGERPRINT_OK) if(millis()-t>5000)return false;
  if(finger.image2Tz(slot)!=FINGERPRINT_OK)return false;
  return true;
}
```

- Parmak izi tarar (5 saniye zaman aşımı).
- Görüntü alınır ve belirtilen slot (1 veya 2) için şablona dönüştürülür.
- Başarılıysa true, hata varsa false döner.

d. getFingerprintID()

```
int getFingerprintID() {
  unsigned long start = millis();
  while (finger.getImage() != FINGERPRINT_OK) {
    if (millis() - start > 5000) return -1;
  }
  if (finger.image2Tz() != FINGERPRINT_OK) return -1;
  if (finger.fingerFastSearch() != FINGERPRINT_OK) return -1;
  return finger.fingerID;
}
```

- Parmak izi tarar ve eşleşen ID'yi döner.
- 5 saniye içinde veri alınamazsa veya eşleşme bulunamazsa -1 döner.

Genel İş Akışı

1. **Başlangıç**: Sistem, EEPROM'da şifre olup olmadığını kontrol eder. Şifre yoksa kullanıcıdan şifre belirlemesi istenir.
2. **Ana Döngü**: Kullanıcı şifre girer. Doğruysa menüye erişir.
3. **Menü**:

a. **Giriş**: RFID kart ve parmak izi kontrol edilerek erişim sağlanır. Başarılıysa röle 5 saniye açılır.

b. **Kayıt**: Master kartla yeni kullanıcı (RFID + parmak izi) kaydedilir.

c. **Şifre Değiştirme**: Master kartla şifre güncellenir.

4. **EEPROM Kullanımı**: Şifre, UID ve parmak izi ID'si kalıcı olarak saklanır.
5. **Güvenlik**: Master kart olmadan kayıt ve şifre değiştirme işlemleri yapılamaz.

Özet

Bu kod, RFID ve parmak izi tabanlı bir erişim kontrol sistemi uygular. Kullanıcılar şifre, RFID kart ve parmak izi ile doğrulanır. Master kart, yönetimsel işlemler (kayıt ve şifre değiştirme) için gereklidir. Sistem, kullanıcı dostu bir arayüz sunmak için LCD ve tuş takımı kullanır, verileri EEPROM'da saklar ve röle ile fiziksel bir cihazı kontrol eder.

Bölüm 10: Projenin Uygulanması

10.1 Giriş

Donanım seçimi, entegrasyonu ve yazılım geliştirme süreçleri ayrıntılı olarak yürütülmüştür. Mikrodenetleyici platformu olarak Arduino veya geliştirme kartı kullanılmış; donanım modülleri uyumluluk ve fiziksel bağlantı açısından optimize edilmiştir.

10.2 Sistem Testleri ve Performans Değerlendirmesi

- Her bir doğrulama modülünün tek başına ve entegrasyon sonrası performansı test edilmiştir.
- Kullanıcı deneyimi açısından sistemin hızlı ve hatasız çalışması sağlanmıştır.

Bölüm 11: Kullanım Senaryoları

11.1 Kayıt Senaryosu

Kullanıcı kayıt işlemi sırasında sırasıyla: Şifreyi girer. NFC kartını okutur. Parmak izi taraması yapar. Bu süreçte, sistem her adımı doğrular ve son aşamada çok faktörlü kimlik doğrulamasını tamamlar. Kayıt başarılı olursa, sistem giriş senaryosu için hazır hale gelir.

11.2 Giriş Senaryosu

Kullanıcı kayıtlardan sonra giriş yaparken: Kayıt sırasında belirlenen şifreyi girer. NFC kartını okutur. Parmak izi taraması gerçekleştirir. Sistem, tüm doğrulama adımlarını başarıyla tamamladığında erişim sağlanır. Her aşamadaki doğrulama, sistemin güvenliğini ve kullanıcının kimliğini teyit eder. Başarısız girişlerde uyarı mesajları gösterilir.

Bölüm 12: Sistemin Güvenlik Açısından Değerlendirilmesi

12.1 Giriş

Akıllı kilit sistemlerinde güvenlik kritik öneme sahiptir. Bu bölümde potansiyel zafiyet noktaları belirlenmiş, saldırı türleri sınıflandırılmış ve sistemin bu saldırılara karşı dayanıklılığı analiz edilmiştir.

12.2 Güvenlik Tehditleri ve Koruma Önlemleri

Erişim Kopyalama ve Taklit NFC kartların klonlanması ve parmak izi verisinin taklit edilmesi riskleri değerlendirilmiştir ve kod kısmında önlenmiştir.

Yazılım Güvenliği Kodun güncel tutulması, açık tespiti ve güvenlik yamalarının hızlı uygulanması gerekliliği vurgulanmıştır.

Bölüm 13: Sonuçlar ve Tartışma

13.1 Sonuçlar

Bu tez çalışmasında geliştirilen iki faktörlü NFC tabanlı akıllı kilit sistemi, güvenlik ve kullanım kolaylığını optimize etmiş, kullanıcı doğrulamasında tutarlı ve hızlı sonuçlar üretmiştir. Entegrasyon aşamalarında uyumluluk ve sistem performansı açısından başarılı sonuçlar elde edilmiştir.

13.2 Tartışma

Tasarım ve uygulama süreçlerinde karşılaşılan bazı teknik zorluklar ve geliştirilebilecek yönler ele alınmıştır. Güvenlik açılarından sonraki çalışmalar için kriptografik doğrulama, uzaktan yönetim yetenekleri ve IoT entegrasyonları planlanmaktadır. Ayrıca kullanıcı deneyiminin artırılması ve maliyet etkinliği üzerinde durulması gerekmektedir.

13.3 Özet

Araştırma, iki faktörlü doğrulama sistemlerinin NFC ve biyometri tabanlı akıllı kilitlerde etkili olduğunu göstermiştir. Geliştirilen prototip ve güvenlik analizleri, kullanıcılara güvenli, pratik ve esnek bir erişim kontrol çözümü sunmaktadır. Gelecekteki çalışmalar için genişletilebilirlik ve daha kapsamlı şifreleme teknikleri üzerinde durulacaktır.

Referanslar

[1] - Arduino Documentation. (2025, January 1). *UNO R3 - Arduino Documentation*. https://docs.arduino.cc/hardware/uno-rev3

[2] - University of Kentucky. (2024, October 24). *Why you should be using multifactor authentication for all your online accounts*. https://its.uky.edu/news/why-you-should-be-using-multifactor-authentication-all-your-online-accounts

[3] - Chief Information Officer Council. (2022, October 26). *The importance of multifactor authentication*. https://www.cio.gov/2022-10-26-importance-multifactor-authentication

[4] - 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

[5] - How2Electronics. (2022, April 19). *Interfacing R502/R503 Capacitive Fingerprint Sensor with Arduino*. https://how2electronics.com/interfacing-r502-r503-capacitive-fingerprint-sensor-with-arduino

[6] - nfc-rfid-reader-sdk. (2023, August 1). *MFRC522_PN512: PN512 NFC Reader Library* [GitHub repository]. https://github.com/nfc-rfid-reader-sdk/MFRC522_PN512

[7] - 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

[8] - 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