UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Elektronické zabezpečení dveří

Bakalářská práce

2025 Filip Nosek

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Filip Nosek**
Osobní číslo:	**I22022**
Studijní program:	**B0714A150008 Automatizace**
Téma práce:	**Elektronické zabezpečení dveří**
Zadávající katedra:	**Katedra automatizace a matematiky**

Zásady pro vypracování

Cílem práce je návrh elektronického systému zabezpečení dveří. Tedy vstupní systém s elektronickým zámkem a evidencí vstupů. Teoretická část práce bude obsahovat rešerši možností elektronických identifikací, od snímání biometrických údajů, čárových/QR kódů přes RFID, NFC, případně Bluetooth a podobných. Rešerše bude kromě stručného popisu principu obsahovat rešerši a popis modulů dostupných pro jednotlivá řešení a jejich srovnání z hlediska bezpečnosti a složitosti implementace. Dále bude teoretická část obsahovat alespoň základní rešerši ostatních prvků systému, jako je detekce otevření dveří, či připojení do nadřazené sítě.
V praktické části práce bude postaven a ověřen koncept zabezpečovacího systému dveří (elektronický zámek) s identifikací a evidencí příchozích. Seznam uživatelů by měl být uložen mimo zámek, nebo by měl umožňovat vzdálenou správu.

Rozsah pracovní zprávy: **30-50**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

[1] VÁŇA, V. Mikrokontroléry ATMEL AVR: popis procesoru a instrukční soubor. Praha: BEN technická literatura, 2003.336 s. ISBN 978-80-7300-083-0.
[2] VÁŇA, V. Mikrokontroléry ATMEL AVR: programování v jazyce C. Praha: BEN technická literatura, 2003. 216 s. ISBN 978-80-7300-102-0.
[3] VLACH, J. Řízení a vizualizace technologických procesů. Praha: BEN technická literatura, 2002. 160 s. ISBN 978-80-86056-66-X.
[4] BRTNÍK, B. Základní elektronické obvody. Praha:BEN technická literatura, 2011. 156s. ISBN 978--80-7300-408-8
[5] RIPKA, P.; TIPEK, A. Master Book of Sensors. Praha : BEN, 2003. ISBN 0-12-752184

Vedoucí bakalářské práce: **Ing. Pavel Rozsíval**
Katedra elektroniky a rádiových systémů

Datum zadání bakalářské práce: **15. prosince 2024**
Termín odevzdání bakalářské práce: **16. května 2025**

L.S.

prof. Ing. Petr Doležel, Ph.D. v.r.
děkan

Ing. Libor Kupka, Ph.D. v.r.
vedoucí katedry

V Pardubicích dne 24. ledna 2025

Prohlašuji:

Práci s názvem Elektronické zabezpečení dveří jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury. Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše. Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 15.5.2025

Filip Nosek v. r.

Poděkování:

Chtěl bych poděkovat svému vedoucímu bakalářské práce Ing. Pavlovi Rozsívalovi za cenné rady a odborné vedení.

Anotace

Cílem práce je návrh elektronického systému zabezpečení dveří. Tedy vstupní systém s elektronickým zámkem a evidencí vstupů. Teoretická část práce bude obsahovat rešerši možností elektronických identifikací, od snímání biometrických údajů, čárových/QR kódů přes RFID, NFC, Bluetooth. Rešerše bude kromě stručného popisu principu obsahovat rešerši a popis modulů dostupných pro jednotlivá řešení a jejich srovnání z hlediska bezpečnosti a složitosti implementace. Teoretická část bude obsahovat alespoň základní rešerši ostatních prvků systému, jako je detekce otevření dveří, či připojení do nadřazené sítě. V praktické části práce bude postaven a ověřen koncept zabezpečovacího systému dveří s identifikací a evidencí příchozích. Seznam uživatelů by měl být uložen mimo zámek, nebo by měl umožňovat vzdálenou správu.

Klíčová slova

identifikace, nadřazené sítě, mikrokontrolér, bezpečnost

Title

Electronic access control

Annotation

The objective of this thesis is the design of an electronic door security system, specifically an access control system with an electronic lock and entry logging. The theoretical part of the thesis will include a review of available electronic identification methods, ranging from biometric data scanning, barcode/QR code reading, to RFID, NFC, Bluetooth technologies. The review will include a brief description of each principle, as well as an overview and comparison of the available modules for each solution in terms of security and implementation complexity. Theoretical part will cover a basic review of other system components, such as door open detection and connection to a higher-level network. In the practical part of the thesis, a prototype of the door security system with identification and entry logging will be built and tested. The user list should be stored externally from the lock or allow for remote management.

Keywords

Identification, supervisory networks, microcontroller, security

Obsah

Seznam Obrázků

Seznam Tabulek

Seznam zkratek a značek

API – Application Programming Interface

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

I2C – Inter-Integrated Circuit

IDE – Integrated Development Environment

JSON – JavaScript Object Notation

LCD – Liquid Crystal Display

LoRa – Long Range

LoRaWAN – Long Range Wide Area Network

MQTT – Message Queuing Telemetry Transport

NAS – Network Attached Storage

NFC – Near Field Communication

NTP – Network Time Protocol

PIR – Passive InfraRed

PLA – Polylactic Acid

PWM – Pulse Width Modulation

QR – Quick Response (kód)

RFID – Radio Frequency Identification

SPI – Serial Peripheral Interface

UID – Unique Identifier

UART – Universal Asynchronous Receiver/Transmitter

VCS – Version Control System

Wi-Fi – Wireless Fidelity

Úvod

V dnešní době je zabezpečení majetku a kontrola přístupu do prostor stále důležitější součástí nejen komerčních, ale i domácích systémů. Tradiční mechanické zámky jsou postupně nahrazovány moderními elektronickými řešeními, která umožňují nejen vyšší úroveň zabezpečení, ale i flexibilní správu uživatelů, záznam přístupů a možnost vzdáleného ovládání. Cílem této bakalářské práce je návrh a realizace elektronického systému zabezpečení dveří. Systém bude využívat radiofrekvenční identifikace osob a umožní řízení přístupu pomocí elektronického zámku s evidencí a zápisu jednotlivých vstupů, přičemž záznamy budou ukládány do vzdálené databáze. Důraz bude kladen na praktickou použitelnost, bezpečnost a možnost propojení s nadřazeným systémem či vzdálenou správou uživatelských dat. Teoretická část práce se zaměří na rešerši dostupných technologií pro elektronickou identifikaci, včetně popisu principů fungování a dostupných modulů. Součástí bude rovněž porovnání těchto technologií z hlediska bezpečnosti, náročnosti implementace a vhodnosti použití v daném typu systému. Dále budou popsány další klíčové prvky systému, jako je detekce otevření dveří a možnosti komunikace s vyššími systémy. Praktická část práce bude věnována návrhu, sestavení a otestování funkčního prototypu zabezpečovacího systému s elektronickým zámkem a záznamem přístupů.

Teoretická část

1. Možnosti el. identifikací a detekce dveří

1.1. Biometrická metoda

Biometrická identifikace využívá jedinečné fyzické vlastnosti jednotlivce, které jsou pro každého člověka specifické a obtížně napodobitelné. Mezi nejčastěji používané metody patří rozpoznávání otisků prstů, obličeje, oční duhovky nebo hlasu. Tyto metody jsou v moderních bezpečnostních systémech stále více využívány, protože nevyžadují, aby uživatel nosil fyzický klíč nebo kartu – k identifikaci postačí samotná přítomnost oprávněné osoby. [1]

Výhodou biometrických systémů je vysoká úroveň zabezpečení a obtížnost zneužití. Na druhé straně je však potřeba počítat s vyšší cenou senzorů a vyššími nároky na zpracování dat a ochranu soukromí uživatelů. V oblasti přístupových systémů je nejčastěji nasazováno právě ověření pomocí otisku prstu, a to díky relativně jednoduché implementaci, rychlosti ověření a dostupnosti vhodných modulů pro mikrokontroléry jako je například Arduino nebo ESP32. [1]

1.1.1. Konkrétní snímač s BM

Biometrickou metodu využívá například modul **R305** viz Obrázek 1, kompaktní optický snímač otisků prstů. Snímač obsahuje vlastní procesor, který zajišťuje veškeré zpracování obrazu, extrakci charakteristik a tvorbu biometrické šablony. Vnitřní paměť umožňuje uložení až 162 otisků prstů, které lze pomocí definovaných příkazů přes sériové rozhraní vyhledávat nebo ověřovat. [2, 3]

Obrázek 1 Optický snímač prstů (4)

Snímač komunikuje s řídicím mikrokontrolérem pomocí UART (TTL úrovně). Datová rychlost je běžně nastavena na 57600 bitů za sekundu, ale lze ji změnit. Napájení modulu je 3.6–6 V, přičemž typické napětí je 5 V. Proudový odběr při běžné činnosti dosahuje hodnoty přibližně 100 mA, což je třeba zohlednit při návrhu napájecí části, jelikož v případě Arduino nano je celkový max. odběr proudu 500 mA, s tím že na této úrovni se začíná přehřívat. [2, 3]

Z hlediska funkce je R305 vybaven dvěma částmi – snímačem obrazu a výpočetní jednotkou. Modul podporuje příkazy pro přidávání nových otisků (registraci), mazání, vyhledávání a porovnání. Komunikace probíhá pomocí jednoduchého protokolu založeného na hexadecimálních příkazech, což umožňuje snadnou integraci i bez hlubších znalostí obrazového zpracování. [2, 3]

Pro zajištění spolehlivosti snímání se doporučuje chránit čtecí plochu před znečištěním a intenzivním světlem. Modul je díky své samostatnosti a jednoduchému zapojení vhodný i pro začátečnické projekty v oblasti biometrického zabezpečení. [2, 3]

Výhodou biometrických systémů je vysoká úroveň zabezpečení a obtížnost zneužití. Na druhé straně je však potřeba počítat s vyšší cenou senzorů a vyššími nároky na zpracování dat a ochranu soukromí uživatelů. V oblasti přístupových systémů je nejčastěji nasazováno právě ověření pomocí otisku prstu, a to díky relativně jednoduché implementaci, rychlosti ověření a dostupnosti vhodných modulů pro mikrokontroléry jako je například Arduino nebo ESP32.

1.2. Čárové a QR kódy

Čárové a QR kódy představují optickou metodu elektronické identifikace, která umožňuje zakódování dat do grafického obrazce čitelného kamerou nebo specializovanou čtečkou. QR kódy mohou obsahovat větší množství informací než klasické čárové kódy – například unikátní identifikátor (UID), odkazy na webové stránky nebo další šifrované údaje [5].

Z hlediska bezpečnosti však tato technologie představuje určitá rizika. QR kódy jsou statické a jejich obsah není na první pohled zřejmý, což otevírá prostor pro zneužití – například přelepením legitimního kódu škodlivým, který odkazuje na falešnou stránku nebo infikuje zařízení malwarem. Úroveň zabezpečení se proto hodnotí jako nízká až střední a vyžaduje zvýšenou pozornost uživatele, zejména v otevřených nebo veřejně přístupných prostředích [5]. Implementačně je technologie snadná při použití přednastavených hardwarových čteček,

zatímco nasazení kamerového systému s vlastním dekódováním je o něco náročnější. Vzhledem k široké dostupnosti modulů a nízkým nákladům je využití QR kódů vhodné zejména pro systémy, kde nejsou kladeny vysoké nároky na zabezpečení.

1.2.1. Konkrétní typ snímače

Obrázek 2 Snímač QR a čárových kódů – DE2120 (6).

Pro praktickou implementaci v přístupových systémech se využívají různé druhy zařízení. Například modul **DE2120** viz Obrázek 2 od společnosti DYScan je specializovaná čtečka určená pro skenování QR kódů z papíru i digitálních displejů. Komunikuje pomocí rozhraní USB nebo TTL a je optimalizována pro integraci s mikrokontroléry jako Arduino nebo ESP32 [6]. Alternativním řešením je použití kamery **ESP32-CAM** v kombinaci se softwarovou knihovnou **OpenCV**, která umožňuje vlastní dekódování obrazu. Tento přístup nabízí vyšší flexibilitu, ale vyžaduje pokročilejší programování a vyšší výpočetní výkon zařízení.

1.3. NFC (Near-Field Communication)

NFC je technologie bezdrátové komunikace na krátkou vzdálenost, která umožňuje výměnu dat mezi dvěma zařízeními. Na rozdíl od klasických RFID systémů, které podporují pouze jednosměrnou komunikaci, NFC umožňuje obousměrnou interakci mezi dvěma aktivními zařízeními nebo mezi aktivním a pasivním prvkem, jako je NFC tag. Tato technologie je standardizována normami ISO/IEC 18092 a ISO/IEC 14443 a pracuje na frekvenci 13,56 MHz s dosahem do 10 cm [7].

Bezpečnost NFC technologie je považována za střední až vysokou, zejména díky možnosti implementace šifrování a autentizačních mechanismů. Například při využití NFC pro přístupové systémy lze implementovat jednorázové tokeny nebo šifrované identifikátory, což zvyšuje odolnost systému proti neoprávněnému přístupu [7].

Vzhledem k široké dostupnosti modulů, jako je PN532, a podpoře ze strany mobilních zařízení s NFC funkcionalitou, je tato technologie vhodná pro různé aplikace, včetně přístupových systémů, bezkontaktních plateb nebo sdílení dat mezi zařízeními [7].

1.3.1. Typ modulu pro NFC identifikaci

Obrázek 3 NFC modul PN532 (8)

Pro implementaci NFC u projektů s mikrokontroléry je často využíván právě zmíněný modul **PN532** viz Obrázek 3. Tento modul podporuje různá komunikační rozhraní, včetně I2C, SPI a UART, což umožňuje flexibilní integraci s platformami jako Arduino nebo ESP32. PN532 je kompatibilní s různými NFC standardy, včetně ISO/IEC 14443 A/B a FeliCa, a podporuje režimy čtení/zápisu, emulace karty a peer-to-peer komunikaci [8].

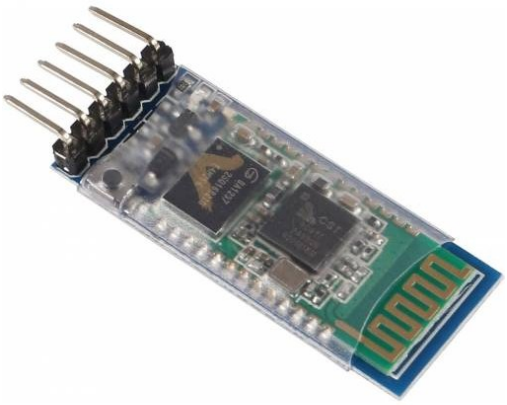
1.4. Bluetooth

Bluetooth je bezdrátová technologie určená pro krátké vzdálenosti, která umožňuje komunikaci mezi různými zařízeními, jako jsou mobilní telefony, počítače, senzory nebo mikrokontroléry. Je široce využívána v přístupových systémech, kde slouží k autentizaci uživatelů prostřednictvím mobilních zařízení nebo specializovaných modulů.

Z hlediska bezpečnosti Bluetooth technologie poskytuje několik úrovní ochrany. Mezi základní bezpečnostní služby patří autentizace zařízení, zajištění důvěrnosti přenášených dat prostřednictvím šifrování a řízení přístupu k službám. Například standard Bluetooth v2.1 zavedl metodu Secure Simple Pairing (SSP), která zvyšuje bezpečnost párování zařízení [10]. Pro moderní aplikace je doporučeno využívat vyšší bezpečnostní režimy, jako je "Secure Connections Only Mode", který vyžaduje šifrované spojení mezi zařízeními [11].

Při implementaci Bluetooth technologie do přístupových systémů je důležité dbát na správné nastavení bezpečnostních parametrů a pravidelně aktualizovat firmware zařízení, aby byla zajištěna ochrana proti známým zranitelnostem. Dále je vhodné omezit dosah signálu na nezbytně nutnou vzdálenost a monitorovat připojená zařízení, aby se minimalizovalo riziko neoprávněného přístupu.

1.4.1. Konkrétní Bluetooth modul



Obrázek 4 Bluetooth modul – HC-05 (15)

Jedním z nejběžněji používaných modulů pro mikrokontroléry je **HC-05** viz Obrázek 4, který podporuje standard Bluetooth v2.0 + EDR (Enhanced Data Rate), což umožnuje vyšší rychlosti přenosu dat až do 3 Mbps. Tento modul pracuje v pásmu 2,4 GHz a umožňuje komunikaci na vzdálenost až 10 metrů. Podporuje sériovou komunikaci přes UART a může fungovat v režimu master i slave, což umožňuje flexibilní integraci do různých systémů. Kompatibilní jak pro Arduino čipy, tak i Raspberry Pi [9].

HC-05 může pracovat ve dvou hlavních režimech:

Data Mode: V tomto režimu modul umožňuje obousměrný přenos dat mezi zařízeními. Je ideální pro aplikace, kde je potřeba jednoduchá a rychlá komunikace, například mezi mikrokontrolérem a chytrým telefonem.

Command Mode: Tento režim slouží ke konfiguraci modulu pomocí AT (Attention Commands) příkazů. Umožňuje nastavení různých parametrů, jako je název zařízení, heslo, role (master/slave) a další. AT příkazy jsou textové řídicí instrukce používané k ovládání komunikačních modulů prostřednictvím sériového rozhraní. Umožňují nastavovat provozní parametry, jako je název zařízení, heslo, role (master/slave), režimy, párování a další funkce bez nutnosti úprav firmwaru zařízení. Jsou nadále používány v modulech jako jsou GSM nebo Wi-Fi pro snadnou konfiguraci a testování [9].

1.5. RFID

RFID je technologie bezdrátové identifikace, která umožňuje automatické rozpoznání objektů nebo osob pomocí rádiových vln. Systém se skládá ze dvou hlavních komponent: RFID čtečky a RFID tagu (transpondéru). Čtečka vysílá elektromagnetické pole, které aktivuje tag, jenž následně odpovídá přenosem svých dat zpět do čtečky. Tato komunikace probíhá bez nutnosti přímé viditelnosti mezi čtečkou a tagem, což je výhodné oproti optickým identifikačním systémům, jako jsou čárové kódy [12].

RFID systémy se dělí podle frekvenčního pásma, ve kterém operují:

- LF (Low Frequency): 125–134 kHz, s dosahem až 10 cm, odolné vůči rušení kovovými předměty a kapalinami.
- HF (High Frequency): 13,56 MHz, s dosahem do 1 metru, často používané v přístupových systémech a platebních kartách.
- UHF (Ultra High Frequency): 860–960 MHz, s dosahem několika metrů, vhodné pro logistiku a sledování zboží [13].

Dále RFID dělí podle principu tagů, jedním typem jsou pasivní RFID tagy. Tyto tagy získávají potřebnou energii pro odeslání dat ze signálu vysílaného RFID čtečkou, který přeměňují na elektrický proud. Vzhledem k tomuto principu je jejich vysílací výkon velmi omezený, což

výrazně zkracuje dosah komunikace – obvykle jen na několik centimetrů až jednotky metrů. Dosah v řádu několika metrů je dosažitelný pouze u UHF RFID systémů, a to navíc jen za ideálních podmínek.

Z tohoto důvodu byla vyvinuta technologie aktivních RFID, kde jsou tagy vybaveny vlastní baterií. Díky tomu je možné výrazně navýšit dosah mezi čtečkou a tagem – až na stovky metrů. S tímto řešením však souvisí větší rozměry tagů (například velikostně připomínají polovinu krabičky cigaret) a také jejich výrazně vyšší cena. Aktivní RFID systémy se proto uplatňují především v oblastech, kde se sleduje dražší zboží nebo velké objekty, jako je například kontejnerová doprava, kde je cena tagu zanedbatelná vůči hodnotě přepravovaného nákladu [13].

Nadále se používají i tagy typu semi-pasivní, které komunikují identickým způsobem jako pasivní tagy s vlastním zdrojem energie, baterii využívá pro napájení mikročipu nebo případných senzorů, které jsou integrovány do čipu. Poskytují delší vzdálenost pro čtení než ty pasivní [14].

O konkrétním RFID modulu **RC522** s vestavěnou anténou, nahlédneme hlouběji v praktické části, jelikož je to zvolený snímač do navrhovaného zabezpečovacího systému pro čtení UID karet.

1.6. Magnetické kontakty (Reed spínače)

Magnetické kontakty, známé také jako reed spínače, jsou elektromechanické zařízení, která se aktivují přítomností magnetického pole. Skládají se z páru feromagnetických pružných kovových kontaktů uzavřených v hermeticky utěsněné skleněné ampuli. Při přiblížení magnetu se kontakty spojí, což umožňuje detekci otevření nebo zavření dveří či oken. Tyto senzory jsou běžně používány v zabezpečovacích systémech pro detekci neoprávněného vstupu [16].

1.7. Kombinované senzory (PIR + Ultrazvuk)

Kombinované senzory integrují technologii PIR a ultrazvukové detekce do jednoho zařízení, čímž zvyšují přesnost detekce pohybu. PIR senzory detekují pohyb na základě změn v infračerveném záření, zatímco ultrazvukové senzory měří změny v odražených zvukových vlnách. Tato kombinace minimalizuje falešné poplachy a zajišťuje spolehlivější detekci [17].

1.8. PIR senzory (Pasivní infračervené senzory)

Pasivní infračervené (PIR) senzory detekují pohyb na základě změn v infračerveném záření vyzařovaném objekty v jejich zorném poli. Senzor obsahuje dvě detekční oblasti, které reagují na rozdíly v teplotě mezi objektem a pozadím. Když teplokrevný objekt, jako je člověk, vstoupí do zorného pole senzoru, dojde k detekci pohybu. PIR senzory jsou široce používány v zabezpečovacích systémech a automatickém osvětlení [18].

1.9. Ultrazvukové senzory

Ultrazvukové senzory měří vzdálenost k objektu vysíláním ultrazvukových vln a měřením času, za který se odražený signál vrátí zpět. Tyto senzory jsou schopny detekovat změny v prostředí, například otevření dveří, na základě změny odraženého signálu. Jsou často používány v automatických dveřních systémech a robotice [19].

2. Nadřazené sítě a ukládání dat

2.1. Cloudové služby

Cloudové uložiště mají skvělou výhodu v tom, že k nim lze s povoleným přístupem dostat odkudkoliv a automaticky se mu synchronizují data a nejsou náročné na nastavení zabezpečení. Nevýhodou však může být připojení k internetu, pokud klient dbá i na off-line provoz systému.

2.1.1. Google Sheets jako jednoduché cloudové řešení

Google Sheets lze využít jako jednoduchý nástroj pro cloudový sběr a vizualizaci dat z mikrokontrolérů nebo jiných IoT zařízení. Díky přístupnému rozhraní Google Apps Script nebo pomocí HTTP GET/POST požadavků lze data z mikrokontrolérů (například Arduino či ESP32) ukládat přímo do tabulek. Tento způsob je vhodný pro malé projekty, kde není kladen důraz na zabezpečení, strukturu dat nebo vysokou škálovatelnost. Výhodou je snadná integrace, dostupnost a možnost rychlého prototypování bez nutnosti správy serverové infrastruktury.

Pro vývojáře, kteří preferují práci v lokálním prostředí, nabízí Google nástroj clasp (Command Line Apps Script Projects). Tento nástroj umožňuje vývoj a správu Apps Script projektů přímo z příkazového řádku, což usnadňuje integraci s verzovacími systémy (version control systems neboli VCS) jako Git a umožňuje využití oblíbených vývojových nástrojů. Clasp umožňuje

vytváření nových projektů, klonování existujících, stahování a nahrávání kódu mezi lokálním prostředím a Google Apps Script, správu verzí a nasazení projektů. Pro jeho použití je nutné mít nainstalovaný Node.js a nástroj nainstalovat pomocí npm. Po instalaci lze pomocí příkazů jako clasp login, clasp create, clasp push a dalších efektivně spravovat Apps Script projekty. [20].

Ačkoliv platforma Google Sheets díky své snadné implementaci, přehlednému rozhraní a dostupnosti představuje vhodné řešení pro základní prototypování a sběr dat z mikrokontrolérů, v kontextu požadavků na spolehlivý, rychlý a obousměrný přenos dat v reálném čase se v rámci této práce neukázala jako optimální volba, a proto byla nahrazena pokročilejším řešením v podobě platformy Firebase Realtime Database.

2.1.2 Firebase Realtime Database

Firebase je cloudová platforma od společnosti Google, která zahrnuje mimo jiné i službu Realtime Database. Tato databáze umožňuje ukládání a synchronizaci dat v reálném čase mezi více zařízeními a klienty. Je vhodná pro aplikace, kde je potřeba okamžitý přenos informací – například při detekci pohybu, řízení přístupů nebo sdílení stavů zařízení. Firebase navíc podporuje autentizaci uživatelů, zabezpečení pomocí pravidel a přehledné monitorování provozu. V teoretické rovině lze Firebase chápat jako pokročilou infrastrukturu pro vzdálené zpracování a sdílení dat mezi mikrokontroléry a nadřazeným systémem [21]. Detailní implementace této technologie bude popsána v praktické části práce.

2.2. On-premise systémy

On-premise systémy představují řešení, kde je veškerá IT infrastruktura – včetně serverů, úložišť a síťových zařízení – provozována a spravována přímo v rámci organizace. Na rozdíl od cloudových řešení, kde jsou data a služby umístěny na vzdálených serverech poskytovatele, jsou v on-premise modelu všechna data uložena lokálně – například na vlastním serveru, NAS jednotce (Network Attached Storage) nebo specializovaném zařízení [22].

Vlastní serverové řešení poskytuje maximální kontrolu nad konfigurací, zabezpečením a dostupností systému. Používá se například pro provoz databází, aplikací, přístupových systémů nebo zálohovacích serverů [22].

NAS zařízení pak slouží zejména pro centrální ukládání a sdílení dat mezi více zařízeními v rámci lokální sítě. Je vhodné pro menší organizace nebo domácí nasazení, kde je kladen důraz na jednoduchou správu a spolehlivost [22].

Výhody on-premise systémů spočívají zejména v nezávislosti na internetu, vyšší míře zabezpečení, a možnosti přizpůsobit hardware i software konkrétním potřebám uživatele. Nevýhodou může být vyšší pořizovací cena a nutnost pravidelné správy či aktualizací ze strany IT personálu [22].

2.3. IoT platformy a protokoly

IoT neboli internet věcí označuje síť fyzických zařízení, která jsou vybavena senzory, softwarem a dalšími technologiemi, které jim umožňují sbírat a vyměňovat si data přes internet (nebo jinou síť) aniž by byl nutný zásah člověka.

2.3.1 MQTT (Message Queuing Telemetry Transport)

MQTT je otevřený, jednoduchý a zároveň velmi účinný protokol navržený pro bezpečný, spolehlivý a nízkonákladový přenos zpráv mezi zařízeními v síti s omezenými prostředky. Díky své minimální režii a jednoduché struktuře se stal jedním z nejpoužívanějších komunikačních protokolů v oblasti internetu věcí [23].

Základní princip MQTT je postaven na modelu publish/subscribe. V tomto režimu zařízení označované jako „publisher“ (vysílač) odesílá zprávy na konkrétní tzv. téma (topic), zatímco jiná zařízení – „subscriber“ (příjemci) – se na toto téma přihlašují. Veškerou komunikaci zprostředkovává tzv. MQTT broker, což je centrální server zajišťující přenos zpráv mezi účastníky. Tento přístup umožňuje efektivní oddělení zařízení, která spolu komunikují, a tím výrazně zjednodušuje škálovatelnost celého systému [23].

Jednou z klíčových výhod MQTT je jeho nízká šířka přenosového pásma, která z něj činí ideální řešení pro prostředí, kde je připojení nestabilní, omezené nebo nákladné – typicky například při využití mobilních sítí, satelitní komunikace, nebo přenosu v energeticky omezených zařízeních napájených z baterie. Další výhodou je možnost nastavení kvality služby (QoS), která definuje, jak spolehlivě má být zpráva doručena (například jen jednou, nejvýše jednou nebo přesně jednou) [23].

MQTT je v současnosti široce nasazován v různých průmyslových odvětvích – včetně průmyslové automatizace, energetiky, logistiky, automobilového průmyslu či zemědělství – a to všude tam, kde je nutná komunikace mezi velkým množstvím zařízení s důrazem na efektivitu, spolehlivost a nízké nároky na přenosové kanály [23].

2.3.2 LoRaWAN (Long Range Wide Area Network)

LoRaWAN představuje specifikaci komunikačního protokolu a systémové architektury navrženou pro bezdrátový přenos dat na velké vzdálenosti při minimální spotřebě energie. Tento protokol je postaven na fyzické vrstvě využívající modulaci LoRa (Long Range), která umožňuje velmi citlivý příjem signálu a přenos malých datových paketů na vzdálenosti dosahující až několika desítek kilometrů, a to i v náročných podmínkách (např. městské zástavbě nebo zemědělských oblastech) [24].

LoRaWAN operuje v nelicencovaných pásmech ISM (např. 868 MHz v Evropě), což snižuje náklady na provoz sítě a umožňuje nasazení bez nutnosti licenčních poplatků. Architektura sítě je typicky hvězdicová – koncová zařízení (tzv. nody) komunikují s gateway, které přenášejí data do centrálního síťového serveru prostřednictvím IP infrastruktury (např. internetu). Tato topologie je velmi efektivní pro IoT aplikace, kde je potřeba monitorovat nebo sbírat data z mnoha zařízení rozmístěných ve velkém geografickém prostoru [24].

Typickými příklady využití LoRaWAN jsou monitoring životního prostředí (teplota, vlhkost, kvalita ovzduší), chytré zemědělství (detekce pohybu zvířat, zavlažování podle vlhkosti půdy), sledování majetku, nebo inteligentní městské aplikace (např. měření stavu odpadových nádob, parkovacích míst či měření spotřeby energií) [24].

Díky své nízké spotřebě energie, která umožňuje provoz zařízení na baterii i po dobu několika let, velkému pokrytí a nezávislosti na komerčním mobilním připojení, se LoRaWAN stává jedním z klíčových komunikačních řešení pro rozsáhlé IoT systémy.

Praktická část

3. Návrh systému a výběr komponent

Navrhovaný systém elektronického zabezpečení dveří je určen pro kontrolu a evidenci vstupu osob na základě bezkontaktní identifikace pomocí RFID karet. Hlavním cílem je tudíž zkompletování spolehlivého přístupového uzlu, který umožnuje automatizované ověření identity, mechanického ovládání zámku a posléze ukládání informací/dat o průchodu do vzdálené cloudové databáze.

3.1. Požadavky na funkčnost systému

Systém tedy musí splňovat nastávající klíčová kritéria pro správný celkový průběh:

Identifikace pomocí RFID: Uživatel přikládá kartu ke čtečce RC522, která načte jedinečné UID. Tato hodnota je následně předána hlavnímu mikrokontroléru (ESP32), který rozhoduje o oprávnění vstupu.

Přidělováni tagů pomocí Správce: Systém rozpozná speciální „master kartu“, jejíž UID je předem uloženo v databázi jako oprávnění ke správě přístupových práv. Po jejím přiložení k RFID čtečce dojde k aktivaci správního režimu.

Po načtení správní karty se otevře časový interval, během něhož může správce přikládat nové RFID karty. Každé nové UID, které dosud nebylo v databázi zaznamenáno, je po přiložení automaticky uloženo do Firebase.

Po uložení nového UID do databáze má správce možnost později přes webové rozhraní přiřadit ke konkrétnímu UID odpovídající jméno uživatele. Tím vzniká kompletní záznam, který lze dále spravovat.

Nová UID lze zapsat pouze během aktivního správního režimu, čímž je zajištěno, že běžní uživatelé nemohou svévolně rozšiřovat seznam oprávněných osob. Po uplynutí nastaveného času je správní režim automaticky deaktivován a systém se vrací do standardního režimu čtení.

Komunikace probíhá obousměrně mezi ESP32 a Firebase Realtime Database, přičemž záznam UID probíhá přes firebase.database().ref("access/") v reálném čase. Každý nový UID je uložen s časovou značkou a stavem „NovyUzivatel“, dokud není administrátorem doplněno.

Ověření proti databázi: UID je porovnáno s uloženými záznamy v nadřazené databázi. V případě shody je umožněn vstup, jinak je přístup odepřen.

Mechanické ovládání zámku: Při autorizaci je zaslán příkaz do sekundárního mikrokontroléru (Arduino Nano), který provede otevření zámku pomocí servomotoru a současně sleduje, zda došlo ke skutečnému otevření dveří.

Zaznamenání události: Každý úspěšný přístup je automaticky uložen do databáze včetně času a UID.

Zvuková a světelná odezva: Uživatel je informován o výsledku autorizace pomocí LED diod (zelená/červená) a akustického signálu (bzučák).

Vizuální výstup: Stav systému (např. UID, schválení/zamítnutí) je zobrazen na LCD displeji připojeném k ESP32

Reakce na pohyb a stav dveří: Systém detekuje pohyb pomocí PIR senzoru a kontroluje otevření dveří pomocí ultrazvukového měření vzdálenosti. Tato logika slouží pro potvrzení fyzického průchodu po otevření zámku.

Vzdálená správa UID: Webové rozhraní propojené s databází Firebase umožňuje správci přidávat, upravovat nebo mazat UID a sledovat historii přístupů.

3.2. Kritéria pro výběr mikrokontrolérů

Výběr vhodných mikrokontrolérů byl zásadní pro funkčnost a stabilitu celého přístupového systému. Vzhledem ke komplexnosti požadavků – zahrnujících komunikaci se senzory, řízení periferií, zpracování dat v reálném čase a připojení k nadřazené databázi – bylo nutné zvolit takovou kombinaci vývojových desek, která zajistí dostatečný výpočetní výkon, variabilní konektivitu a nízkou spotřebu energie.

3.2.1 ESP32 DEVKIT – hlavní řídicí jednotka

Pro hlavní řídicí úlohu systému byl zvolen výkonný mikrokontrolér **ESP32 DEVKIT V1**, který je díky integrovanému Wi-Fi a Bluetooth rozhraní ideální volbou pro IoT aplikace. Jeho dvoujádrový procesor, taktovaný od 80 MHz až na 240 MHz a dostatečná kapacita paměti umožňují současné provádění více funkcí – od čtení RFID karet přes obsluhu LCD displeje a bzučáku až po komunikaci s cloudovou databází Firebase Realtime Database.

- **Integrované Wi-Fi** – umožňuje přímé připojení k internetu bez potřeby externích modulů
- **Dostatečný výkon** – nutný pro obsluhu více periferií současně (např. používaná RFID čtečka, LCD, LED a bzučák)
- **Velký počet GPIO pinů** – pro připojení různých typů zařízení
- **Podpora moderních vývojových nástrojů** – Arduino IDE, PlatformIO, Firebase knihovny.

3.2.2. Arduino Nano

Mikrokontrolér Arduino Nano, konkrétněji jeho klon Arduino NANO CH340 byl zvolen jako sekundární jednotka pro ovládání servo motoru zámku a zpracování dat z PIR senzoru a ultrazvukového měřiče vzdálenosti (HC-SR04). Nano bylo preferováno kvůli svým kompaktním rozměrům, jednoduché integraci a schopnosti zajišťovat autonomní činnost v rámci podřízené logiky.

Jedním z technicky významných důvodů výběru bylo také napájecí napětí 5 V, které lépe vyhovuje potřebám klasických servopohonů (např. SG90) než 3,3 V logika ESP32. Díky tomu lze servo motor napájet přímo z výstupních pinů Arduino Nano, bez nutnosti samostatného zdroje nebo převodníků, což zjednodušuje zapojení a zvyšuje spolehlivost systému.

Hlavní důvody výběru Arduino Nano:

- Dostatečný výkon pro základní logiku a PWM řízení servo motoru
- Jednoduché a stabilní UART propojení s ESP32
- Napájení 5 V, které je vhodné pro servo motory a senzory vyžadující vyšší napěťovou úroveň

- Nízká spotřeba a malé rozměry, které jsou vhodné pro instalaci do krabičky vedle zámku
- Rozšířená komunita a snadná integrace knihoven

Volba dvou mikrokontrolérů přinesla výhodu v oddělení úloh:

- ESP32 zajišťuje veškerou „inteligenci“ systému – rozhodování, připojení k síti, přístup k databázi a reakci na uživatele.
- Arduino Nano plní funkci vykonavatele – zajišťuje fyzické ovládání zámku a hlídá stav dveří i pohyb osob.

Tímto způsobem bylo dosaženo lepší spolehlivosti, modularity a snadnějšího ladění systému, přičemž oba mikrokontroléry mezi sebou komunikují pomocí jednoduché sériové komunikace (UART).

3.3. Vybrané moduly a senzory – přehled

V rámci návrhu přístupového systému byly zvoleny takové moduly, které splňují požadavky na kompaktnost, snadnou integraci, spolehlivost a dostupnost pro mikrokontroléry ESP32 a Arduino Nano. Následující přehled popisuje jednotlivé komponenty, jejich hlavní vlastnosti a roli v celkovém systému.

3.3.1. RFID čtečka RC522

Modul MFRC522 viz Obrázek 5 je RFID čtečka pro identifikaci bezkontaktních karet standardu ISO/IEC 14443 A, které pracují na frekvenci 13,56 MHz. V projektu slouží k načtení UID karty nebo čipu, který je následně odeslán do ESP32 a porovnán s databází Firebase. Modul komunikuje přes rozhraní SPI, vyžaduje napájení 3,3 V a funguje spolehlivě při přiblížení karty na vzdálenost cca 2–4 cm.

Obrázek 5 Čtečka RC522 (25)

Použití v projektu: Identifikace uživatele bezkontaktní kartou

3.3.2. Servo motor SG90

Mikroservo motor SG90 s hmotností 9 g, schopný otáčení v rozsahu 0–180° viz Obrázek 6. V projektu je využíván k mechanickému ovládání elektronického zámku dveří. Servo je řízeno PWM signálem z Arduino Nano, přičemž napájení je zajištěno přímo z 5 V pinu Nano, což zajišťuje jeho plnou funkčnost bez nutnosti externího napájení. Servo reaguje na příkaz z ESP32, který je předán přes sériovou linku.

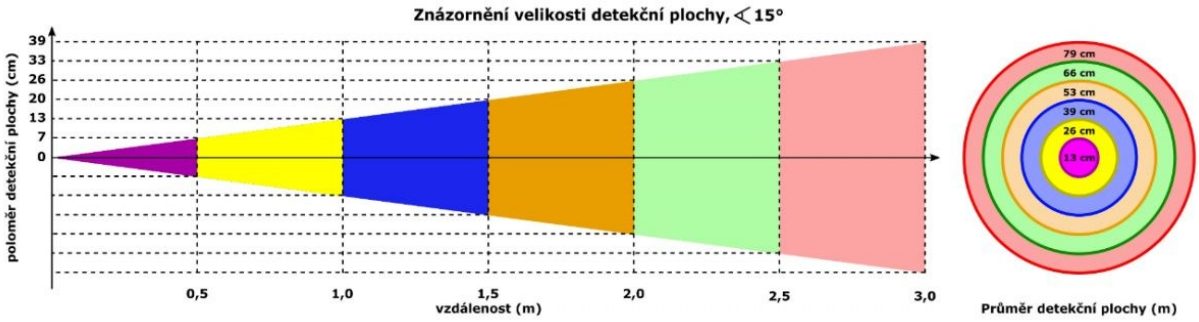
Obrázek 6 Servomotor mikro (26)

Použití v projektu: Otevření a zavření elektronického zámku po autorizaci

3.3.3. Ultrazvukový senzor HC-SR04

Ultrazvukový senzor viz Obrázek 7 HC-SR04 slouží k měření vzdálenosti od pevné překážky, a v tomto projektu konkrétně k určení, zda došlo k otevření dveří. Po přijetí povelu k otevření zámku Arduino sleduje změnu vzdálenosti podle detekční plochy znázorněné viz Obrázek 8 pokud se hodnota výrazně změní, považuje se dveře za otevřené. Senzor komunikuje pomocí digitálních signálů (TRIG a ECHO) a je připojen k Arduino Nano.

Obrázek 7 Ultrazvukový senzor HC-SR04(27)

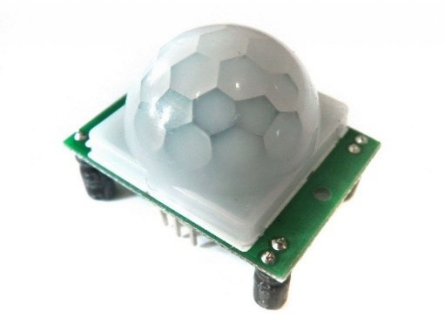


Obrázek 8 Velikost detekčni plochy ultrazvukové senzoru(27)

Použití v projektu: Detekce fyzického otevření dveří

3.3.4. PIR senzor

Pasivní infračervený senzor HC-SR501 viz Obrázek 9 detekuje pohyb osob na základě změn v infračerveném záření v místnosti. V systému slouží jako doplněk pro potvrzení průchodu osoby po otevření zámku. Pokud není detekován žádný pohyb, systém může například neuložit průchod nebo ho vyhodnotit jako falešný pokus. PIR je připojen k digitálnímu pinu na Arduino Nano.

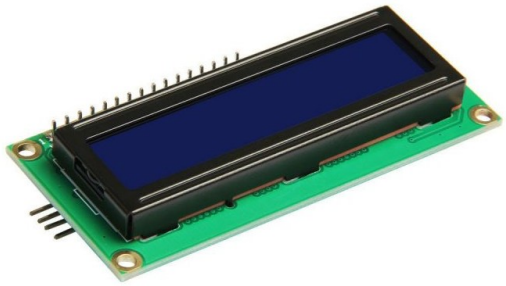


Obrázek 9 PIR senzor HC-SR501(28)

Použití v projektu: Detekce přítomnosti osoby v prostoru dveří

3.3.5. LCD I2C 16×2

Dvouřádkový displej LCD 16×2 s I2C převodníkem slouží jako vizuální výstupní zařízení, které informuje uživatele o stavu systému – např. „Přístup povolen“, „Karta neznámá“, nebo zobrazí UID karty. Komunikuje pomocí I2C sběrnice (dva vodiče – SDA a SCL) a je připojen k ESP32 viz Obrázek 10.



Obrázek 10 LCD displej s I2C převodníkem (29)

Použití v projektu: Zobrazení výsledků autorizace a systémových hlášení

3.3.6. Bzučák a LED diody

Pasivní bzučák a dvě LED diody (červená a zelená) slouží k akustické a vizuální signalizaci výsledku autorizace. V případě úspěšného ověření UID se aktivuje zelená LED a bzučák krátce pípne. Při neautorizovaném pokusu svítí červená LED a přehraje se výraznější zvukový signál.

LED diody a bzučák jsou připojeny k digitálním pinům ESP32 a jsou řízeny v reálném čase podle výsledku komunikace s Firebase.

Použití v projektu: Signalizace oprávnění/odmítnutí přístupu

Pro správnou funkci LED diody je nutné zařadit předřadný odpor, který omezí proud tak, aby nedošlo k poškození součástky. Využíváme Ohmův zákon, který popisuje rovnice 1.

$$R = \frac{U_{napájení} - U_{LED}}{I_{LED}} \quad (1)$$

Kde:

R = hodnota odporu [Ω].

$\mathbf{U_{napájení}}$ = napětí zdroje (3,3 V – napájení z EPS32).

$\mathbf{U_{LED}}$ = úbytek napětí na LED (např. 2 V pro červenou).

$\mathbf{I_{LED}}$ = doporučený proud (obvykle 20 mA).

Tabulka 1: Orientační zvolení odporů pro LED (napájení 3,3 V)

Barva LED	Úbytek napětí (V)	Doporučený proud (mA)	Doporučený odpor (Ω)
Červená	2	15-20	65-87
Oranžová	2,1	15-20	60-80
Žlutá	2,2	15-20	55-73
Zelená	2,4	15-20	45-60
Modrá	3,2	15-20	5-7
Bílá	3,2	15-20	5-7
Růžová	3	15-20	15-20
Fialová	3,1	15-20	10-13

Příklad pro červenou diodu v rovnici 2.

$$R = \frac{3{,}3V - 2V}{0{,}02A} = 65\Omega \quad (2)$$

Vzhledem k tomu, že výstupní piny mikrokontroléru ESP32 pracují s napětím 3,3 V, byl výpočet předřadného rezistoru upraven na základě tohoto napětí viz Tabulka 1. Pro červenou LED s úbytkem napětí přibližně 2 V a proudem 20 mA by teoreticky postačoval rezistor o hodnotě 65 Ω. Z praktických důvodů však byl použit rezistor 220 Ω, který snižuje proud na přibližně 6 mA, což je pro signalizační účely dostatečné a zajišťuje delší životnost diody. Tato hodnota byla zároveň nejnižší dostupná mezi použitými komponentami.

Použití v projektu: Signalizace oprávnění/odmítnutí přístupu

3.4. Zdůvodnění výběru platformy Firebase

Pro potřeby ukládání, ověřování a správy přístupových dat v reálném čase byla v projektu zvolena cloudová platforma Firebase Realtime Database od společnosti Google. Tato volba vycházela z požadavku na spolehlivou, rychlou a snadno integrovatelnou databázi, která by umožňovala komunikaci mezi mikrokontrolérem ESP32 a webovým rozhraním bez nutnosti provozování vlastního serveru.

Firebase nabízí přímou podporu pro REST API i JavaScript SDK [21], což umožnilo obousměrnou komunikaci s databází jak ze strany mikrokontroléru (odesílání UID a čtení oprávnění), tak z webového rozhraní (správa uživatelů a logů). Díky této integraci bylo možné vytvořit přehledný přístupový systém s možností vzdálené správy, a to i z mobilních zařízení nebo jiného počítače v síti.

Hlavní důvody, proč byla zvolena platforma Firebase:

- Synchronizace v reálném čase – veškeré změny se ihned projeví na připojených klientech
- Snadná integrace s ESP32 – prostřednictvím HTTP GET/POST požadavků a knihoven pro Arduino
- Bezplatná varianta – pro malé projekty postačuje bez nutnosti placeného tarifu
- Není nutné provozovat vlastní server nebo databázi – šetří čas i náklady
- Přístup odkudkoliv – ideální pro monitorování systému mimo fyzickou lokalitu

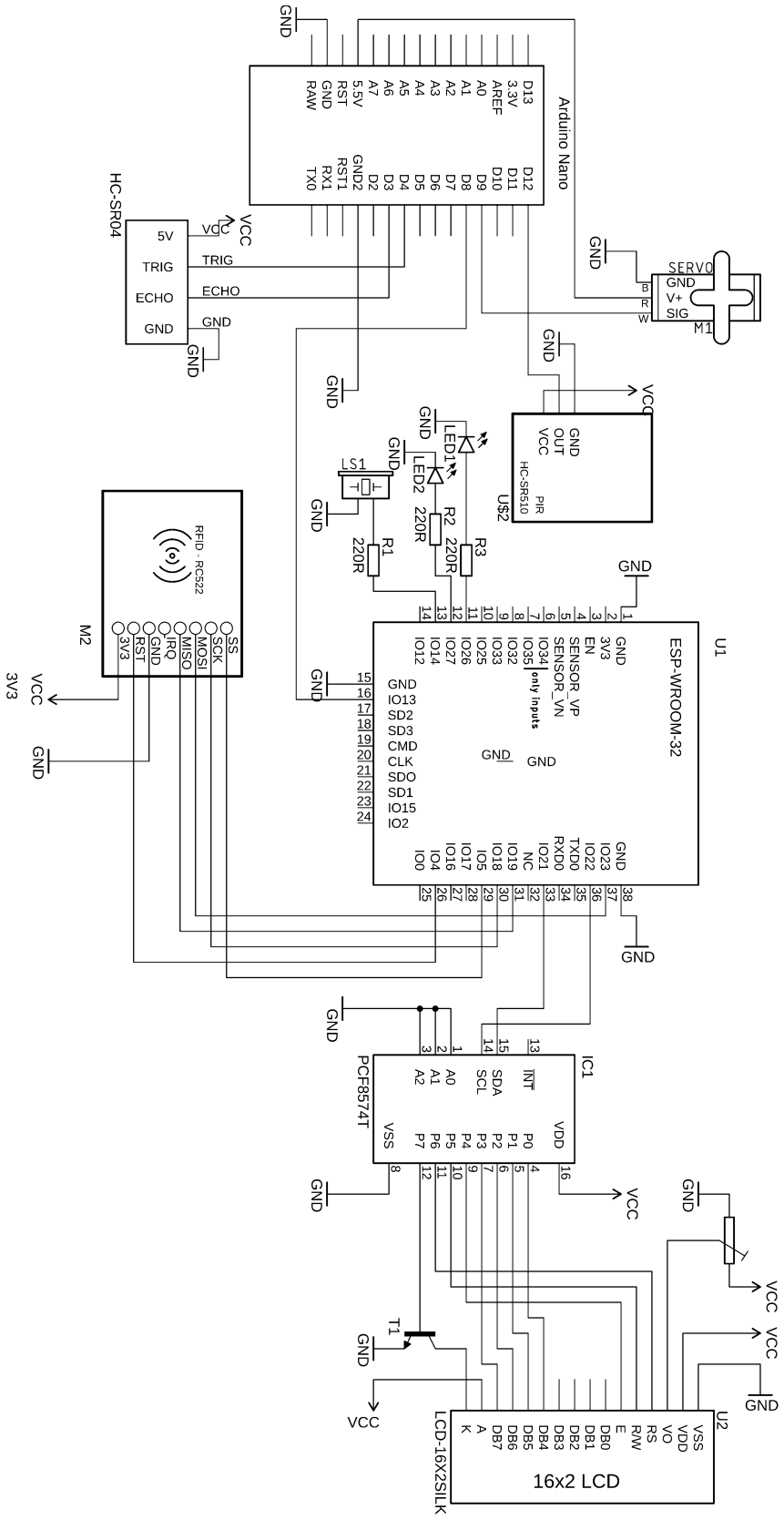
Na začátku vývoje byla zvažována i alternativa v podobě Google Sheets využívajícího Apps Script, avšak tento přístup se ukázal jako méně robustní a hůře škálovatelný. Z těchto důvodů byl zvolen přechod na Firebase, který nabízí lepší strukturu dat, vyšší rychlost odezvy a možnosti autentizace.

4. Návrh schéma zapojení

Systém pro elektronickou evidenci přístupů je založen na koordinaci dvou mikrokontrolérů Arduino Nano a ESP-WROOM-32, které komunikují pomocí UART rozhraní. ESP32 slouží jako hlavní řídicí jednotka pro bezdrátovou komunikaci a zpracování dat z RFID čtečky RC522, zatímco Arduino Nano má za úkol řízení periferií spojených s mechanickou obsluhou dveří a monitorováním fyzických změn prostředí. Data jsou zpracovávána a zobrazována lokálně na LCD displeji a také vzdáleně přes síťovou infrastrukturu pomocí Wi-Fi.

Schéma zahrnuje přesné propojení mikrokontrolérů s jednotlivými periferiemi. Napájecí zdroje jsou rozděleny podle úrovně napětí (3,3 V pro ESP32 a periferie k němu připojené, 5 V pro Arduino a další periferie připojené k tomu mikrokontroléru) viz Obrázek 11 na další straně.

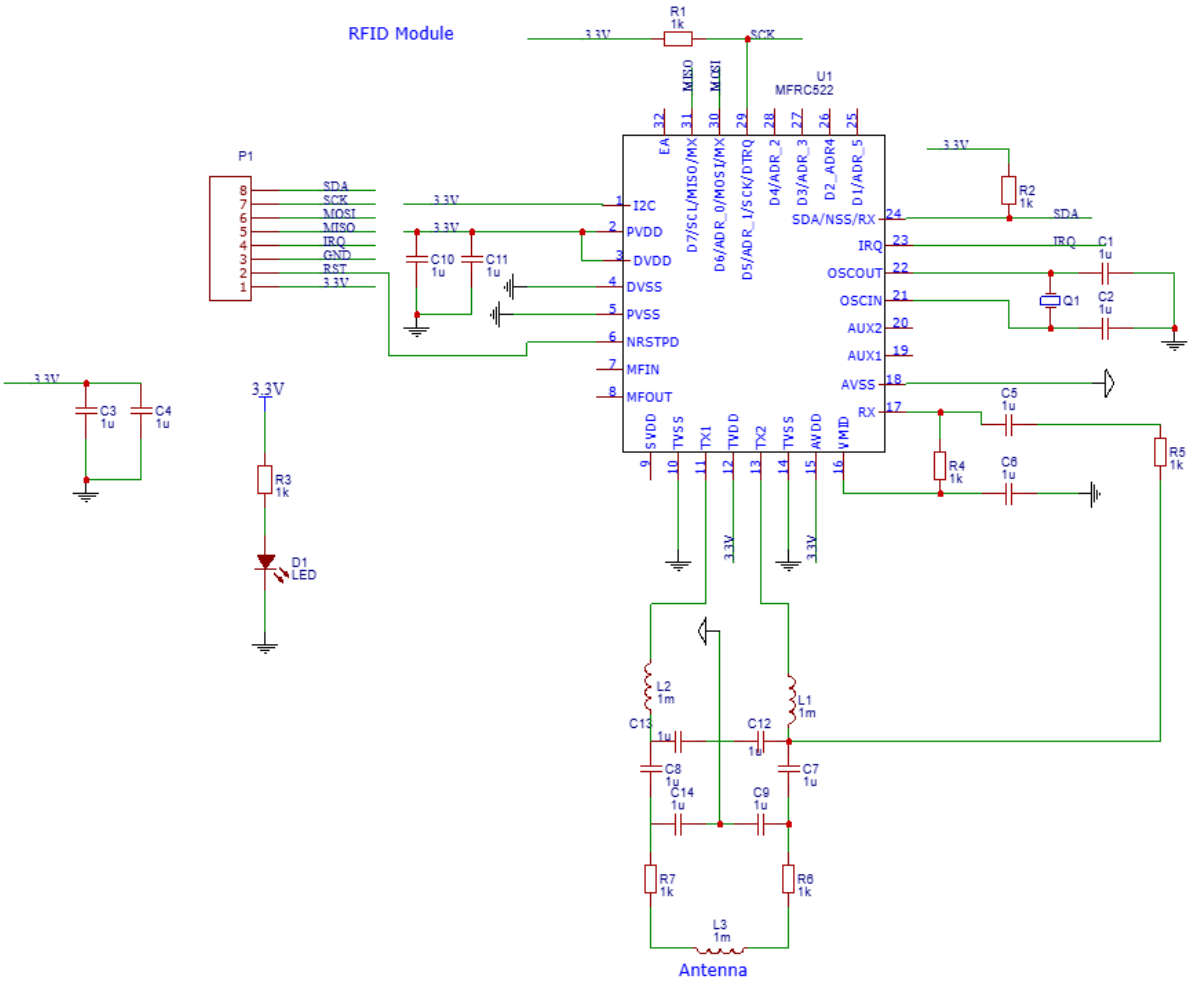
ESP32 je srdcem systému, propojeno pomocí SPI sběrnice s RFID čtečkou RC522. Pro řízení LED indikátorů a bzučáku jsou využity GPIO výstupy ESP32, přes rezistory omezující proud. Arduino Nano komunikuje s ESP32 pomocí UART sběrnice, což umožňuje synchronizovanou činnost. Nano ovládá servo motor pomocí PWM signálu generovaného z digitálního výstupu D9. Ultrazvukový senzor HC-SR04 je připojen k digitálním pinům D4 (Trig) a D3 (Echo), PIR senzor HC-SR510 je připojen k digitálnímu vstupu D12. LCD displej typu 16x2 znaků je propojen přes I2C převodník PCF8574T, který je napájen ze společné 5 V větve a komunikaci provádí přes sběrnici SDA a SCL s ESP32.



Obrázek 11 Celkové schéma zapojení s vybranými moduly

4.1. Vnitřní schéma RFID modulu

Znázorněné vnitřní zapojení modulu RC522 viz Obrázek 12, které je postaven na integrovaném obvodu MFRC522 od společnosti NXP. Schéma zachycuje jak připojení anténního obvodu, tak napájení, komunikační rozhraní SPI a podpůrné pasivní součástky nezbytné pro správnou funkci čtečky.

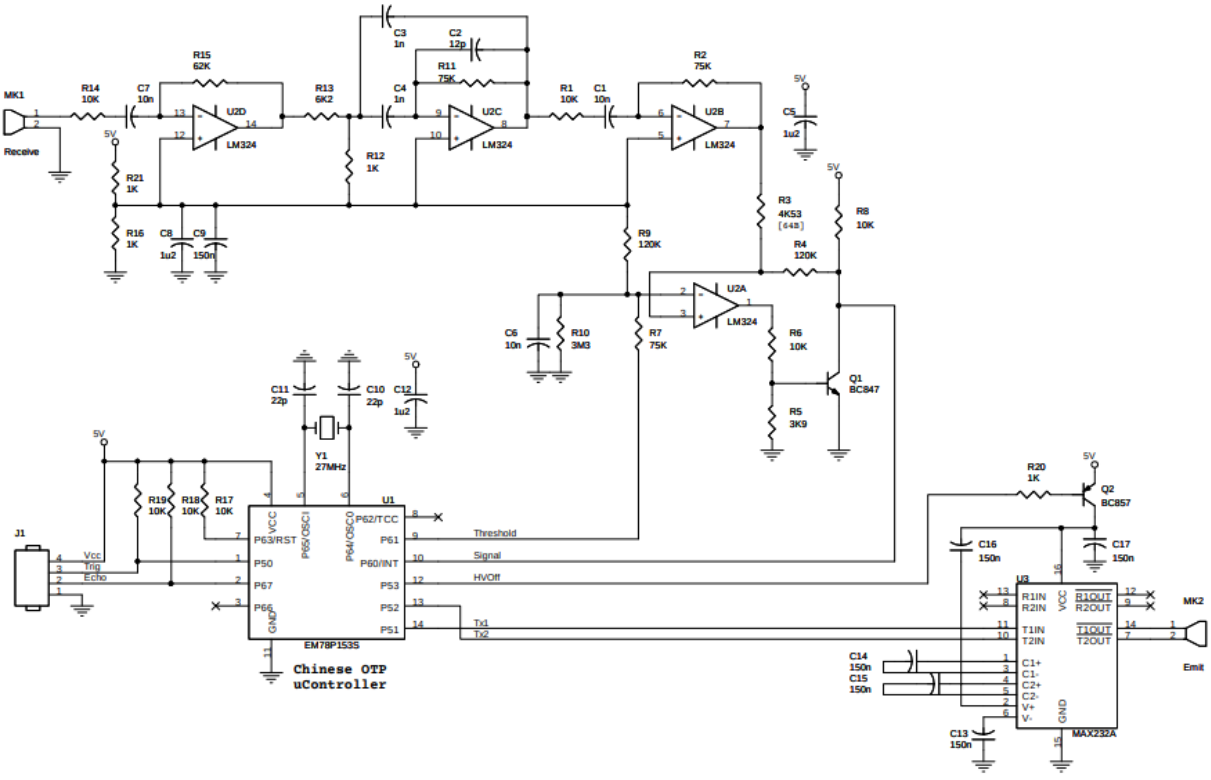


Obrázek 12 Schéma modulu RFID RC522(30)

4.2. Vnitřní schéma ultrazvukového modulu

Ultrazvukový senzor HC-SR04 slouží k měření vzdálenosti od překážky v rozsahu přibližně 2 cm až 4 metry, přičemž výrobce udává rozlišovací schopnost až 3 mm. Modul je kromě ultrazvukového vysílače a přijímače vybaven také budicím obvodem, čtyřmi operačními zesilovači (zapojenými jako zesilující pásmové propusti) a obvodem zajišťujícím vyhodnocení signálu a řízení celkové logiky. Tu typicky realizuje OTP mikrokontrolér nebo specializovaný integrovaný obvod (ASIC) v neoznačeném pouzdře, což je běžné u levných čínských modulů. Napájení modulu je realizováno napětím 5 V [31].

Znázorněné schéma jedné ze starších revizí modulu HC-SR04 viz Obrázek 13. Přestože novější verze mohou obsahovat mírné odlišnosti v zapojení, princip fungování zůstává obdobný. Schéma zachycuje kompletní strukturu signálové cesty od přijímače přes zesilovací a filtrační obvody až po digitální část s mikrokontrolérem a výstupy „Trig“ a „Echo“ [31].



Obrázek 13 Zapojení modulu HC-SR04 z roku 2014 – revize (31)

5. Datová komunikace a nadřazený systém

Cílem této části je popsat způsob, jakým probíhá výměna dat mezi jednotlivými částmi systému, zejména mezi mikrokontroléry a cloudovou databází. Komunikace je klíčová pro funkčnost celého přístupového systému, jelikož zajišťuje ověřování identity uživatelů a evidenci průchodů.

5.1. Popis komunikace mezi ESP32 a Arduino Nano

Komunikace mezi mikrokontroléry ESP32 a Arduino Nano probíhá prostřednictvím sériové linky UART. ESP32 funguje jako hlavní řídicí jednotka, která zajišťuje identifikaci RFID karet a ověřuje je přes nadřazenou databázi. Po úspěšné autorizaci odesílá příkaz do Nano ve formě jednoduchého znaku 'O' pro otevření.

Komunikační protokol je jednoduchý, což minimalizuje latenci a snižuje riziko chyb v přenosu. Arduino reaguje na přijatý znak okamžitým otočením servo motoru a sledováním otevření dveří.

5.2. Zpracování UID a ověřování v databázi

Po načtení RFID UID čtečkou RC522 předá ESP32 tento údaj dál – zkontroluje, zda aktuálně není blokováno čtení (např. po předchozím přístupu), a následně UID odešle pomocí HTTP požadavku do Firebase Realtime Database.

Základní logika zpracování je taková, že se UID přečte a formátuje jako hexadecimální řetězec. ESP32 odešle GET požadavek na adresu projektu ve firebase, která vypadá takto https://[NAZEV-PROJEKTU].firebaseio.com/users/UID.json. Pokud UID existuje, Firebase vrací odpovídající jméno. ESP32 podle výsledku povolí/zamítne vstup a zapíše záznam do log/. Tato forma komunikace umožňuje dynamicky spravovat uživatele i bez úpravy firmwaru.

5.3. Firebase Realtime Database – struktura a nastavení

Firebase Realtime Database je cloudová databáze, která umožňuje ukládání a načítání dat ve formátu JSON. V tomto formátu jsou veškerá data reprezentována jako stromová struktura klíč–hodnota, což umožňuje jejich snadné zpracování v reálném čase pomocí REST API požadavků. V projektu je databáze strukturována následovně:

```
{
    "access": {
      "masterUID": true
    },
  "log": {
    "-OPGu_2MM34pb2KaN_s6": {
      "name": "Nosek Filip",
      "timestamp": 1746204773,
      "uid": "2BC534A0"
    }
  },
  "users": {
    "2BC534A0": {
      "name": "Nosek Filip"
    }
  }
}
```


- **/access/** – seznam UID s oprávněním pro správce
- **/users/** – Uchovává seznam oprávněných uživatelů. Klíč je UID karty a hodnota obsahuje jméno osoby. Pokud přiložený UID existuje v této větvi, je přístup povolen.
- **/log/** – evidence přístupů s časovým razítkem. Každý má náhodně generovaný klíč

ESP32 přistupuje k těmto větvím pomocí standardních HTTPS požadavků (GET, PUT, POST). Oprávnění je řízeno jedním přístupovým tokenem.

5.4. Autentizace přístupu a správa oprávnění

Správa přístupových práv je navržena tak, aby umožňovala snadné přidávání i odebírání UID pomocí tzv. správcovského režimu. Po přiložení master karty se aktivuje časově omezený režim, během něhož mohou být nové RFID tagy automaticky přidány do databáze pod jménem NovyUzivatel, poté ho správce v databázi skrze webové rozhraní může upravit nebo smazat podle svých představ.

Proces autentizace začíná načtením UID z RFID čtečky, které je následně odesláno do databáze Firebase k ověření. Systém nejprve kontroluje, zda se daný UID nachází ve větvi /users. Pokud ano, přístup je automaticky povolen a uživateli je umožněno otevřít dveře.

V případě, že UID v databázi neexistuje, systém zjišťuje, zda je aktuálně aktivní režim správce. Pokud ano, nový UID je automaticky uložen do databáze jako nový záznam, který může být následně rozšířen o jméno uživatele.

Každý pokus o přístup ať už je úspěšný nebo neúspěšný, tak je zaznamenán do větve /log, která slouží jako průběžná historie všech interakcí se systémem.

Kromě samotné autentizace poskytuje systém také webové rozhraní, prostřednictvím něhož může správce přidělit konkrétnímu UID jméno, případně záznam později upravit nebo z databáze zcela odebrat. Tento přístup výrazně usnadňuje správu systému bez nutnosti přímé interakce s mikrokontrolérem nebo změn v kódu.

6. Implementace softwarového řešení

Softwarová část přístupového systému byla realizována primárně v prostředí Arduino IDE s využitím jazyka C/C++ pro mikrokontroléry ESP32 a Arduino Nano. Cílem implementace bylo vytvořit spolehlivý a modulární kód, který umožní řízení všech částí systému, komunikaci s cloudovou databází a uživatelskou správu přístupů.

6.1. Arduino Nano – ovládání serva a senzorů

Mikrokontrolér Arduino Nano slouží v navrženém systému jako podřízená jednotka, která reaguje na signály z ESP32 a zajišťuje obsluhu mechanické části přístupového systému. Jeho hlavním úkolem je řízení servo motoru, detekce pohybu osob a sledování stavu dveří pomocí ultrazvukového senzoru.

Arduino Nano bylo zvoleno kvůli jeho jednoduchosti, 5 V logice (vhodné pro napájení SG90) a samostatnosti při řízení mechanických komponent, čímž se odlehčilo hlavní jednotce ESP32.

6.1.1. Stav dveří (ultrazvuk)

Pro sledování stavu otevření či zavření dveří byl použit ultrazvukový senzor **HC-SR04**, který měří vzdálenost před sebou pomocí odraženého zvukového pulzu. Čidlo je připojeno k pinu **TRIG** na D4 a **ECHO** na D3. Funkce **zmerVzdalenost** zajišťuje odeslání pulzu a změří dobu jeho návratu a převede ji na vzdálenost v cm tímto způsobem:

```
float zmerVzdalenost() {
  digitalWrite(TRIG_PIN, LOW);
  delayMicroseconds(2);
  digitalWrite(TRIG_PIN, HIGH);
  delayMicroseconds(10);
  digitalWrite(TRIG_PIN, LOW);

  long trvani = pulseIn(ECHO_PIN, HIGH, 30000);
  if (trvani == 0) return -1;
  return trvani * 0.034 / 2;
}
```

Pro stabilnější měření je zavedena funkce zmerPrumerVzdalenosti(int pocet), která zpracuje více měření (standardně 5) a vypočítá průměrnou hodnotu, přičemž ignoruje neplatná měření (např. >300 cm, <0 cm nebo chybějící odraz).

Systém pracuje s hodnotami v rozsahu 2–8 cm jako s potvrzením, že jsou dveře zavřené. Jakmile je detekována odlišná vzdálenost, systém chápe, že došlo k otevření. Dveře jsou považovány za skutečně zavřené až po několika sekundách klidového stavu bez pohybu osob a při stabilní vzdálenosti opět v tomto rozsahu.

6.1.2. Zjištění průchodu (PIR)

Pro detekci skutečného průchodu osob byla na Arduino Nano připojena PIR čidla pohybu. Program reaguje na změnu výstupního signálu z digitálního pinu, na kterém je připojen PIR senzor. Pokud je detekován pohyb v definovaném časovém rámci po otevření dveří (zjištěném ultrazvukovým senzorem), systém jej vyhodnotí jako úspěšný průchod.

Detekce probíhá v hlavní smyčce loop, kde se pravidelně čte stav pinu **digitalRead(PIR_PIN)** a ukládá do proměnné pohyb. Tato informace se následně používá při rozhodování, zda došlo k otevření a opětovnému zavření dveří, aby bylo možné znovu uzavřít zámek.

6.1.3. Ovládání serva

Ovládání zámku je realizováno pomocí servomotoru, připojeného k pinu D9 na Arduino Nano. Servo motor slouží k mechanickému otevření a zavření dveří a je řízeno prostřednictvím knihovny **Servo.h.**

Po přijetí znaku 'O' přes sériovou linku UART se servo nastaví do odemčené polohy. Zároveň se aktivuje časové okno, během něhož Arduino sleduje změnu vzdálenosti z ultrazvukového senzoru a případný pohyb pomocí PIR senzoru.

Jakmile je detekováno otevření a následné zavření dveří, nebo po uplynutí stanoveného času bez akce, servo motor se vrátí do výchozí zamčené polohy. Tento proces zabraňuje nechtěnému opětovnému otevření a zajišťuje základní logiku bezpečného uzavření systému. Celý kód je v příloze.

6.2. ESP32 – řízení přístupu a komunikace

Mikrokontrolér ESP32 představuje hlavní řídicí jednotku celého systému. Zajišťuje bezdrátové připojení k síti Wi-Fi, čte RFID UID z karty přiložené ke čtečce, komunikuje s databází Firebase, rozhoduje o udělení nebo zamítnutí přístupu a předává příslušné povely do

podřízené jednotky. Zároveň poskytuje uživatelskou zpětnou vazbu pomocí LED diod, LCD displeje a akustického pasivního bzučáku. Celý ArduinoIDE kód je poskytnut v příloze.

6.2.1. Čtení RFID UID

Načítání RFID karet je v tomto systému realizováno pomocí knihovny **MFRC522.h**, která slouží k obsluze čtečky MFRC522 s frekvencí 13,56 MHz. Modul je připojen k ESP32 prostřednictvím sběrnice SPI, přičemž signál **SS** je připojen na pin GPIO 5 a RST na GPIO 4.

6.2.2. Blokování opakovaného čtení

Aby se předešlo opakovanému vyhodnocení stejné RFID karty, pokud ji uživatel ponechá na čtečce, je ve firmwaru implementována jednoduchá, ale účinná forma časového blokování opakovaného čtení UID.

Po každém úspěšném přečtení karty je identifikátor UID uložen do proměnné lastUID a současně se zaznamená aktuální čas pomocí funkce millis viz níže:

```
lastUID = uid;
lastReadTime = millis();
```

Na začátku hlavní smyčky loop je poté každý další nově načtený UID porovnáván s tímto posledním přečteným. Pokud je stejný jako lastUID a zároveň neuplynulo alespoň 5 sekund od předchozího načtení (definováno jako BLOCK_DURATION = 5000 ms), je přístup automaticky zablokován následujícím výrazem:

```
if (millis() - lastReadTime < BLOCK_DURATION && uid ==
lastUID) return; // ignoruj opakované čtení
```

Tímto se zamezuje opakovanému zpracování stejné karty během krátkého časového intervalu, což by jinak vedlo například k vícekrát odeslanému pokynu k otevření zámku nebo k opakovanému zápisu do logu. Systém tak zůstává stabilní, nereaguje na držení karty u čtečky a správně vyhodnocuje jen nové události.

6.2.3. Odesílání dat do Firebase

Pro komunikaci s cloudovou databází Firebase Realtime Database je v systému využita knihovna **HTTPClient.h**, která umožňuje odesílat HTTP požadavky přímo z ESP32 bez nutnosti dalšího serveru. Po úspěšném ověření UID (tedy zjištění, že karta existuje v lokálně

uloženém seznamu uživatelů) je nutné zaznamenat pokus o přístup do databáze jako logovací záznam.

Tyto záznamy se ukládají do větve /log, a každý nový záznam je přidán pomocí HTTP POST požadavku. Firebase při tom automaticky vygeneruje unikátní klíč (např. -NLOgKZxXAsdf123), pod který se uloží strukturovaný objekt ve formátu JSON.

K tomu slouží funkce **logujPristup** z kódu, jejíž klíčová část vypadá následovně:

```
void logujPristup(String uid, String jmeno) {
  time_t now = time(nullptr);
  String url = firebaseURL + "/log.json?auth=" + accessToken;
  HTTPClient http;
  http.begin(url);

  DynamicJsonDocument doc(256);
  doc["uid"] = uid;
  doc["name"] = jmeno;
  doc["timestamp"] = now;

  String jsonData;
  serializeJson(doc, jsonData);

  int httpCode = http.POST(jsonData);
  if (httpCode > 0) {
    Serial.println("Log přístupu uložen.");
  } else {
    Serial.println("Chyba při logování přístupu");
  }

  http.end();
}
```

doc["uid"] – obsahuje hexadecimální identifikátor RFID karty (např. "2BC534A0"), doc["name"] – obsahuje jméno uživatele, které bylo přiřazeno tomuto unikátnímu UID, doc["timestamp"] – ukládá aktuální čas ve formátu UNIX epoch, který je získán přes funkci time(nullptr) po synchronizaci s NTP serverem.

Data se serializují pomocí funkce serializeJson(), která převede strukturovaný JSON dokument do textové podoby vhodné pro přenos.

6.2.4. Přijímání zpětné odpovědi

V aktuálním řešení systému není UID ověřováno v reálném čase dotazem na Firebase při každém přiložení karty. Místo toho ESP32 při spuštění programu, a následně v pravidelném intervalu jedné minuty, provádí stažení celé větve /users z Firebase a ukládá si všechna UID a jim přiřazená jména lokálně do pole struktury **Uzivatel**.

Tato synchronizace je zajištěna funkcí **nactiUzivatele**, která pomocí HTTP GET požadavku stáhne kompletní seznam uživatelů ve formátu JSON a uloží jej do paměti mikrokontroléru:

```
String url = firebaseURL + "/users.json?auth=" + accessToken;
http.begin(url);
int httpCode = http.GET();

if (httpCode > 0) {
  String payload = http.getString();
  deserializeJson(doc, payload);
  ...
  uzivatele[i].uid = uid;
  uzivatele[i].jmeno = name;
}
```

Samotné ověření UID pak probíhá lokálně v hlavní smyčce programu loop, kdy se po načtení UID zavolá funkce **najdiJmeno(uid)**, která prohledá dříve načtené pole **uzivatele[]**. Pokud je UID nalezeno, funkce vrátí přiřazené jméno, v opačném případě vrací prázdný řetězec.

```
String jmeno = najdiJmeno(uid);
if (jmeno != "") {
  // přístup povolen
} else {
  // přístup zamítnut
}
```

Díky tomuto přístupu se zajišťuje rychlá odezva systému, protože není třeba čekat na odpověď serveru Firebase při každém přiložení karty. Tato architektura je vhodná zejména pro zařízení, kde není garantováno trvalé připojení k internetu, nebo kde je důležitá rychlost reakce.

6.2.5. Signalizace (bzučák, LED, LCD)

Signalizace slouží k informování uživatele o výsledku ověření přístupu pomocí zvuku, světla a textu.

LED diody: Zelená LED (GPIO 27) se rozsvítí při povoleném přístupu, červená (GPIO 26) při zamítnutí. Po zobrazení stavu se obě opět zhasnou.

Bzučák: Připojený na pin GPIO 14, vydá krátký tón při úspěchu nebo sérii výstražných tónů při zamítnutí.

LCD displej: 16×2 znakový displej přes I²C (adresa 0x27) zobrazuje zprávy typu „Povoleno: [jméno]“, „ZAMITNUTO“, nebo „Režim SPRÁVCE“.

Tato jednoduchá kombinace umožňuje okamžitou zpětnou vazbu bez nutnosti monitorovat výstup přes sériový port.

6.3. Kódové oddělení funkcí a optimalizace

Při vývoji softwarového řešení systému byla věnována pozornost nejen samotné funkčnosti, ale i vnitřní organizaci kódu. Kód byl záměrně rozdělen na dvě samostatné jednotky – ESP32 a Arduino Nano, přičemž každá plní odlišnou sadu úloh podle své hardwarové role. Tento přístup zajišťuje nižší složitost jednotlivých částí programu a zároveň umožňuje nezávislé ladění a rozšíření jednotlivých komponent systému.

ESP32 slouží jako hlavní komunikační a rozhodovací jednotka. Obsahuje funkce jako:

- **getUIDString** – převod načteného UID do hexadecimální podoby,
- **checkFirebaseAccess** – ověření UID přes Firebase,
- **logAccess** – vytvoření logovacího záznamu,
- **signalAccessGranted** / **signalAccessDenied** – zpětná vazba pomocí LED, LCD a bzučáku.

Arduino Nano je zodpovědné za mechanickou interakci – ovládání servo motoru, měření vzdálenosti a detekci pohybu. Kód je zjednodušený a optimalizovaný pro rychlé reakce na příchozí signály z ESP32.

Použité Optimalizační prvky:

- Byl použit neblokující časový management (millis místo delay), aby nedocházelo k zablokování hlavní smyčky.
- Použití objektu StaticJsonDocument z knihovny ArduinoJson.h umožňuje efektivní práci s JSON bez dynamické alokace paměti.
- Sériová komunikace mezi ESP32 a Nano je ošetřena jednoduchým protokolem založeným na jednom znaku, čímž je minimalizována latence a paměťová náročnost.
- Firebase dotazy jsou prováděny pouze při změně UID, nikoli v každém cyklu smyčky.

Tato oddělená architektura a modularita přispívají ke snadnější orientaci v kódu, vyšší stabilitě systému a možnosti jeho budoucího rozšíření o další funkce bez nutnosti zásadního přepisování stávajícího řešení.

7. Webové rozhraní

V rámci návrhu přístupového systému bylo vytvořeno také webové rozhraní, které umožňuje uživateli vzdálenou správu databáze UID, sledování historie přístupů a celkový dohled nad systémem. Tato část funguje jako nadstavba nad Firebase Realtime Database a přispívá k uživatelskému komfortu zejména při provozu v reálném prostředí.

Cílem návrhu webového rozhraní bylo vytvořit nástroj, který by umožnil pohodlnou a efektivní správu celého přístupového systému bez nutnosti fyzického připojení k mikrokontroléru či zásahu do zdrojového kódu. Webové rozhraní slouží především správci systému, kterému poskytuje přehledné prostředí pro administraci oprávněných uživatelů a monitorování historie přístupů.

Díky přímému propojení s cloudovou databází Firebase umožňuje toto rozhraní přidělovat jména k jednotlivým UID, tedy přiřadit konkrétní identifikátor RFID karty konkrétní osobě. To zajišťuje vyšší přehlednost v přístupových záznamech a usnadňuje identifikaci jednotlivých vstupů. Kromě toho má správce možnost prohlížet kompletní logy přístupů, které jsou ukládány do větve /log, a tím sledovat, kdo a kdy do systému vstoupil. V případě potřeby lze odstraňovat záznamy uživatelů, například při ztrátě karty nebo změně oprávnění.

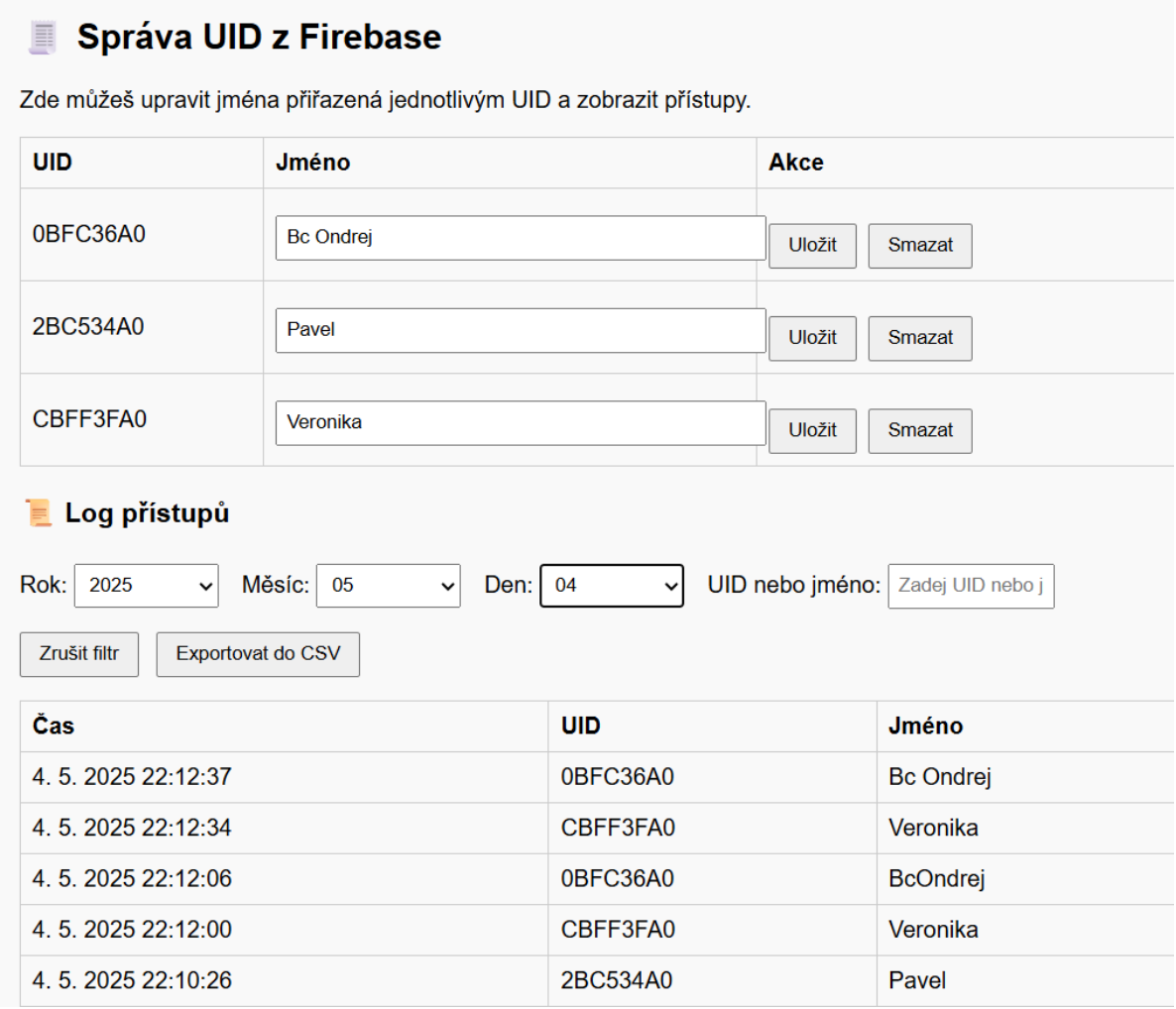
Webové rozhraní může také sloužit pro sledování aktuální aktivity v systému v reálném čase, protože Firebase Realtime Database podporuje živou synchronizaci dat. Díky tomu se veškeré změny v databázi s maximálním zpožděním jedné minuty načtou, jako je nový záznam logu nebo přidaný uživatel okamžitě promítnou do zobrazeného obsahu stránky bez nutnosti ručního obnovení. Tento přístup umožňuje správci vzdáleně a bezpečně spravovat přístupový systém bez přímého kontaktu s hardwarem nebo nutnosti programátorských zásahů. Webové rozhraní se tak stává klíčovým nástrojem pro praktické použití systému v reálném nasazení.

7.1. HTML struktura a skripty

Webové rozhraní bylo implementováno jako jednoduchá klientská aplikace využívající kombinaci jazyků **HTML**, **CSS** a **JavaScript**, přičemž datová logika a interakce s databází Firebase je zajištěna prostřednictvím Firebase JavaScript SDK. Celý systém je navržen tak, aby bylo možné jej provozovat bez serveru, pouze jako statickou webovou stránku spuštěnou v libovolném moderním prohlížeči.

Struktura webové stránky je rozdělena do několika základních částí, které odpovídají požadavkům na správu uživatelů a přehledné zobrazení záznamů uložených v databázi Firebase. Po zadaní přístupových údajů (RFID@identifikace.cz, RFID123) je jednou z hlavních komponent formulář pro přiřazení jména k UID, kde se skrze kartu správce přidá hexadecimální identifikátor RFID karty s popisem „NovyUzivatel“. UID samotné je neměnné, protože je pevně dané čipem; měnit lze pouze přidružené jméno, nebo celý záznam v případě potřeby odstranit.

Další částí rozhraní je tabulka všech aktuálně uložených uživatelů, kde jsou zobrazena všechna UID a jejich přiřazená jména. Tato tabulka obsahuje rovněž funkce pro odstranění záznamu z databáze, což umožňuje například odebrání přístupu při ztrátě karty. Ve spodní části stránky se nachází sekce pro výpis historie přístupů, která zobrazuje jednotlivé logy uložené ve větvi /log, včetně UID, času a jména, pokud bylo přiřazeno. Celý systém je doplněn o interaktivní tlačítka pro provádění jednotlivých operací, jako je „Přidat uživatele“ nebo „Smazat uživatele“, dále se pod částí log přístupů nachází tlačítko pro export CSV souboru o záznamech přístupu spolu s filtrováním datumu, tím si správce může udělat výpis osob za den nebo třeba za celý měsíc. Systém tedy lze spravovat přímo z webového prohlížeče bez nutnosti zásahu do kódu viz Obrázek 14.



Obrázek 14 Webové rozhraní RFID databáze

7.2. Komunikace mezi webem a Firebase

Po načtení stránky je prostřednictvím inicializačního bloku navázáno spojení s databází pomocí **firebase.initializeApp** a **firebase.database**.

Při načítání záznamů se používá metoda once("value"), která stáhne aktuální obsah dané větve databáze – např. /log – a umožní jeho zpracování ve formě dynamicky generované tabulky na stránce. Veškeré změny provedené ve webovém rozhraní se tedy okamžitě promítají do databáze, a tím pádem i do logiky systému běžícího na mikrokontroléru ESP32.

Velkou výhodou tohoto řešení je, že Firebase zajišťuje přímou obousměrnou synchronizaci dat, a to v reálném čase. Webové rozhraní tak může být kdykoli otevřeno na libovolném zařízení a správce má okamžitý přehled o změnách v systému bez nutnosti ručního obnovení stránky.

Tento způsob komunikace umožňuje efektivní vzdálenou správu přístupových oprávnění, přidávání a odebírání uživatelů, stejně jako dohled nad historií vstupů. Správce přitom nemusí mít žádné znalosti programování ani přímý přístup k mikrokontroléru – všechny klíčové funkce jsou přístupné přes jednoduché webové prostředí. Celý html kód je poskytnut v příloze.

7.3. Mechanická konstrukce a návrh krabičky

Pro potřeby fyzické instalace systému byla navržena vlastní krabička, která slouží k uchycení všech komponent viz Obrázek 15. Zejména ESP32, RFID čtečky, LCD displeje a LED signalizace. Konstrukce byla vytvořena v softwaru Fusion 360 a následně vytištěna na 3D tiskárně Bambu Lab A1 z materiálu PLA.

Obrázek 15 Návrh krabiček ve Fusion 360

Závěr

Tato bakalářská práce se zabývala návrhem a realizací přístupového systému s využitím technologie RFID a bezdrátové komunikace. Cílem bylo vytvořit funkční elektronický systém pro zabezpečení dveří, který bude schopen identifikovat jednotlivé uživatele, řídit přístup na základě přiřazených oprávnění a zaznamenávat všechny přístupové události do vzdálené databáze.

V teoretické části byly podrobně rozebrány jednotlivé technologie používané pro elektronickou identifikaci osob. Byly popsány principy biometrických metod, čárových a QR kódů, technologie RFID, NFC a Bluetooth, včetně přehledu vhodných hardwarových modulů, jejich výhod, nevýhod, úrovně bezpečnosti a složitosti implementace. Dále byla provedena rešerše dostupných řešení pro detekci otevření dveří a možností připojení systému k nadřazeným platformám, jako jsou Firebase, Google Sheets nebo MQTT.

Praktická část práce byla zaměřena na realizaci samotného přístupového systému. Hlavními prvky byly mikrokontrolér ESP32, sloužící jako centrální jednotka systému, a Arduino Nano, které zajišťovalo obsluhu výstupního mechanismu. RFID čtečka MFRC522 byla využita k načítání identifikátorů karet, zatímco komunikace s databází probíhala pomocí protokolu HTTP a cloudové platformy Firebase Realtime Database. Součástí systému byla také webová aplikace umožňující správu UID a zobrazení historie přístupů. Signál ke spuštění zámku byl po ověření UID předáván přes UART z ESP32 do Arduino Nano, které následně řídilo servomotor a vyhodnocovalo stav dveří pomocí PIR senzoru a ultrazvukového měření.

Systém byl rovněž doplněn o akustickou a vizuální signalizaci, která zajišťuje okamžitou zpětnou vazbu uživateli. Zvuková signalizace pomocí bzučáku informuje o úspěšném nebo zamítnutém přístupu, zatímco dvojice LED diod zobrazuje stav systému zrakově. Textová komunikace probíhá přes LCD displej o velikosti 16×2 znaků, na kterém jsou zobrazovány klíčové informace jako výzvy k přiložení karty, jméno identifikovaného uživatele nebo hlášení o odmítnutí přístupu.

Důležitou součástí návrhu byla i implementace bezpečnostních opatření, jako je blokování opakovaného čtení UID, detekce reálného otevření dveří a potvrzení jejich opětovného zavření.

V rámci práce byl rovněž vytvořen vlastní model krytu pro systém v prostředí Fusion 360, který byl vytištěn na 3D tiskárně a uzpůsoben pro praktické použití.

Výsledkem práce je funkční, modulární a rozšiřitelný přístupový systém, který umožňuje snadnou správu přístupových práv, zaznamenávání událostí v reálném čase a přehlednou správu přes webové rozhraní. Systém může být dále upraven pro větší provozní prostředí, doplněn o notifikace, mobilní aplikaci nebo podporu dalších autentizačních metod.

Literatura

1. **VALTEROVÁ, Sandra.** *Biometrické identifikační systémy* [online]. Bakalářská práce. Brno: Vysoká škola AMBIS, 2022 [cit. 15. 4. 2025]. Dostupné z: https://is.ambis.cz/th/hti6j/

2. **Adafruit**. *Optical Fingerprint Sensor.* [Online] [cit. 16. 4 2025.] https://learn.adafruit.com/adafruit-optical-fingerprint-sensor.

3. **DRÁTEK.cz**. *Modul optického snímače otisků prstů R305 – dokumentace* [online]. [cit. 16. 4. 2025]. Dostupné z: https://dratek.cz/docs/produkty/0/323/1496818942.pdf

4. **Kuongshun.** In: Kuongshun [online]. [cit. 17. 4. 2025]. Dostupné z: https://cz.szks-kuongshun.com/search/R305.html

5. CANADIAN CENTRE FOR CYBER SECURITY. Security considerations for QR codes ITSAP.00.141 [online]. 2021 [cit. 7. 5. 2025]. Dostupné z: https://www.cyber.gc.ca/en/guidance/security-considerations-qr-codes-itsap00141

6. **DYScan**. *2D Barcode Scanner Setting Manual – DE2120*. [online]. [cit. 17. 4. 2025]. Dostupné z: https://cdn.sparkfun.com/assets/6/4/6/1/f/DY_SCAN_Specification-DE2120_1___2_.pdf

7. **NFC Forum**. *NFC Technology*. [online]. [cit. 18. 4. 2025]. Dostupné z: https://nfc-forum.org/learn/nfc-technology/

8. **NEVEN.cz.** PN532 NFC RFID V3 modul [online]. [cit. 18. 4. 2025]. Dostupné z: https://www.neven.cz/p/pn532-nfc-rfid-v3-modul/

9. **Components101.** HC-05 Bluetooth Module Pinout. [online]. [cit. 20. 4. 2025]. Dostupné z: https://components101.com/wireless/hc-05-bluetooth-module

10. **NIST.** *Guide to Bluetooth Security*. [online]. [cit. 20. 4. 2025]. Dostupné z: https://www.nist.gov/publications/guide-bluetooth-security-2

11. **Bluetooth SIG**. *Bluetooth Security*. [online]. [cit. 20. 4. 2025]. Dostupné z: https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/

12. **SMART-TEC**. *Jak fungují čtečky RFID*. [online]. [cit. 21. 4. 2025]. Dostupné z: https://www.smart-tec.com/cs/kompaktni-know-how/znalost-auto-id/technologie-rfid

13. **AUTOMA.** ***RFID*** *– principy, typy, možnosti použití*. [online]. [cit. 21. 4. 2025]. Dostupné z: https://www.automa.cz/cz/casopis-clanky/rfid-principy-typy-moznosti-pouziti-2011_07_44083_5207

14. **GS1 Czech Republic.** EPC/RFID. [online]. [cit. 21. 4. 2025]. Dostupné z: https://www.gs1cz.org/wp-content/uploads/2024/02/publikace_EPC_RFID.pdf

15. **DRÁTEK.cz.** *Bluetooth modul HC-05 – produktový popis*. [online]. [cit. 22. 4. 2025]. Dostupné z: https://dratek.cz/arduino/1005-bluetooth-modul-hc-05.html

16 **Wikipedia.** *Reed switch*. [online]. [cit. 26. 4. 2025]. Dostupné z: https://en.wikipedia.org/wiki/Reed_switch

17. **Lighting Supply Outlet.** *150° Dual-Technology PIR/Ultrasonic Low Voltage Occupancy Sensor*. [online]. [cit. 26. 4. 2025]. Dostupné z: https://www.lightingsupplyoutlet.com/150-dual-technology-pir-ultrasonic-low-voltage-occupancy-sensor-mdw-l/

18. **Adafruit** Learning System. How PIRs Work. [online]. [cit. 26. 4. 2025]. Dostupné z: https://learn.adafruit.com/pir-passive-infrared-proximity-motion-sensor/how-pirs-work

19. **Hackster.io**. *Automatic Gate open and close Using ultrasonic sensor*. [online]. [cit. 26. 4. 2025]. Dostupné z: https://www.hackster.io/Techatronic/automatic-gate-open-and-close-using-ultrasonic-sensor-ac5579

20. **Google Developers.** *Apps Script Overview*. [online]. [cit. 28. 4. 2025]. Dostupné z: https://developers.google.com/apps-script/guides/clasp

21. **Firebase.** *Realtime Database*. [online]. [cit. 28. 4. 2025]. Dostupné z: https://firebase.google.com/docs/database

22. **Synology**. *Co je NAS? A proč byste ho měli používat?* [online]. [cit. 28. 4. 2025]. Dostupné z: https://www.synology.com/cs-cz/knowledgebase/DSM/tutorial/General/What_is_NAS

23. **MQTT.org.** *MQTT: The Standard for IoT Messaging*. [online]. [cit. 28. 4. 2025]. Dostupné z: https://mqtt.org/

24. **The Things Network**. *What are LoRa and LoRaWAN?* [online]. [cit. 28. 4. 2025]. Dostupné z: https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/

25. **DRÁTEK.CZ.** RFID čtečka s vestavěnou anténou [online]. [cit. 4. 5. 2025]. Dostupné z: https://dratek.cz/arduino/833-rfid-ctecka-s-vestavenou-antenou.html

26. **DRÁTEK.CZ.** ESES Servo motor 9g [online]. [cit. 4. 5. 2025]. Dostupné z: https://dratek.cz/arduino/897-eses-servo-motor-9g.html

27. **DRÁTEK.CZ.** ESES Ultrazvukový měřič vzdálenosti HC-04 pro jednodeskové počítače [online]. [cit. 4. 5. 2025]. Dostupné z: https://dratek.cz/arduino/846-eses-ultrazvukovy-meric-vzdalenosti-hc-04-pro-jednodeskove-pocitace.html

28. **DRÁTEK.CZ.** HC-SR501 pohybové čidlo pro jednodeskové počítače [online]. [cit. 4. 5. 2025]. Dostupné z: https://dratek.cz/arduino/839-hc-sr501-pohybove-cidlo-pro-jednodeskove-pocitace.html

29. **DRÁTEK.CZ.** IIC/I2C display LCD 1602 16x2 znaků, LCD modul modrý [online]. [cit. 4. 5. 2025]. Dostupné z: https://dratek.cz/arduino/1570-iic-i2c-display-lcd-1602-16x2-znaku-lcd-modul-modry.html

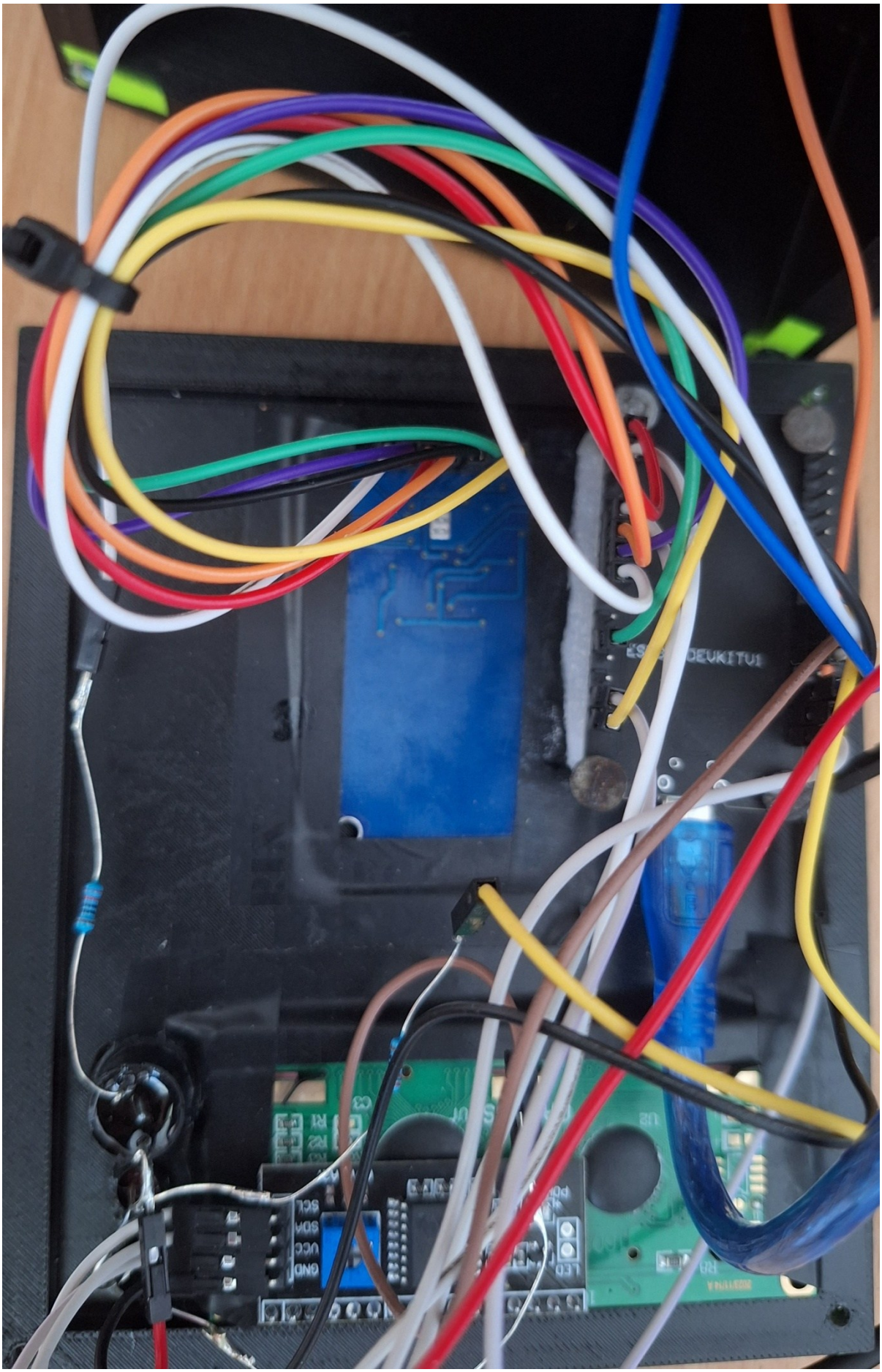
30. **EASYEDA**. *RFID-RC522 Schematic* [online]. [cit. 13. 5. 2025]. Dostupné z: https://easyeda.com/modules/RFID-RC522-Schematic_a6f34cba9dbb4bb8afa14e116ab160cc

31. **ČVUT V PRAZE**, Fakulta elektrotechnická. *Ultrasonic Sensor HC-SR04* [online]. [cit. 13. 5. 2025]. Dostupné z: https://embedded.fel.cvut.cz/sites/default/files/kurzy/lpe/ultrasonic_hc-sr04/Ultrasonic_HC-SR04.pdf

Příloha A – Elektronické přílohy

- Text práce: NosekF_ElektronickeZabezpeceni_PR_2025.pdf
- Projekt ArduinoIDE pro Nano mikrokontrolér: Arduino_NANO_verze.ino
- Projekt ArduinoIDE pro ESP mikrokontolér: ESP_WROOM_32_verze.ino
- HTML dokument: RFID_DATABAZE_HTML.html
- Projekt Fusion: Navrh_krabicek.stl
- Složka použitých nestandartních knihoven v ArduinoIDE: Knihovny_IDE

Příloha B – Fotografie


GND
VCC
SDA
SCL
LED