UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Inteligentní zámek

Jiří Svatoň

Bakalářská práce
2021

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jiří Svatoň**
Osobní číslo:	**I18058**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Komunikační a mikroprocesorová technika**
Téma práce:	**Inteligentní zámek**
Zadávající katedra:	**Katedra elektrotechniky**

Zásady pro vypracování

Zabezpečení dveří mechanickým zámkem patří stále k nejpoužívanějším metodám, ale kromě bezpečnosti přináší určité komplikace v podobě nutnosti nosit klíč fyzicky sebou, ale obzvláště v možnosti správy klíčů. Například ztráta klíče znamená výměnu kompletního zámku, a tím i všech klíčů k němu přiřazených. Tyto nevýhody částečně, nebo úplně odstraňují elektronické systémy zabezpečení a identifikace.
Cílem práce je návrh zařízení pro ověření totožnosti / autorizace vstupu do uzamčených prostor s možností správy klíčů bez jejich přítomnosti.
Teoretická část práce bude obsahovat rozbor možných metod identifikace od použití biometrických metod, po metody využívající přístupové karty, případně jiné metody jednoznačné identifikace.
Teoretická část práce tyto metody porovná z hlediska možností implementace do návrhu systému se stávajícím stavem dostupných komponent pro čtení údajů, případně dalšího zpracování dat.
Praktická část práce bude pak obsahovat návrh přístupového systému za využití zvoleného řešení. Zvolený systém by měl implementovat uživatelsky přívětivou správu osob autorizovaných ke vstupu.

Rozsah pracovní zprávy: **30-60**
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 elektrotechniky

Datum zadání bakalářské práce: **15. listopadu 2020**
Termín odevzdání bakalářské práce: **14. května 2021**

L.S.

Ing. Zdeněk Němec, Ph.D. v.r.
děkan

Ing. Jan Pidanič, Ph.D. v.r.
vedoucí katedry

V Pardubicích dne 29. ledna 2021

Prohlášení autora

Prohlašuji:
Tuto práci 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., autorský zákon, 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. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 13. 8. 2021 Jiří Svatoň

Poděkování

Těmito slovy bych rád poděkoval svému vedoucímu bakalářské práce Ing. Pavlu Rozsívalovi za jeho odbornou pomoc a cenné rady, které jsem využil pro tvorbu bakalářské práce. Rád bych také poděkoval rodině, blízkým a přátelům za pomoc a podporu v průběhu celého studia.

Anotace

Tato práce se zabývá využitím inteligentního zámku ve vybrané společnosti. Práce je rozdělena na část teoretickou, kde se nachází důležité poznatky z oblasti elektronické kontroly vstupu, biometrických systémů a systému s využitím RFID. V části aplikační je představena vybraná společnost, analýza požadavků společnosti na inteligentní zabezpečení a samotný návrh včetně sestavení modelu inteligentního zámku.

Klíčová slova

Biometrie, RFID, EKV, inteligentní zámek, autentizace, autorizace

Title

Smart lock

Annotation

This Bachelor's thesis is focused on the use of intelligent locks in a selected company. The work is divided into a theoretical part, where there is important knowledge in the field of electronic access control, biometric systems and systems using RFID technology. The application part presents a selected company, an analysis of the company's requirements for intelligent security and the design itself, including the construction of a smart lock model.

Keywords

Biometric, RFID technology, electronic access control, smart lock, authentication, authorization

Obsah

Seznam zkratek

EKV	Elektronická kontrola vstupu
FAR	False acceptance rate
FRR	False rejection rate
NFC	Near field communication
SPI	Serial Peripheral Interface
HF	High frequency
UHF	Ultra high frequency
CCD	Charge-Coupled Device
ROM	Read-Only Memory
LF	Low frekvenci
RFID	Radio Frequency Identification
DNA	Deoxyribonucleic acid
IT	Information technology
WIFI	Wirelles Fidelity
PC	Personal computer
USB	Universal Serial Bus
LED	Light-Emitting Diode
PIN	Personal identification number

Seznam obrázků

Seznam tabulek

Úvod

Zabezpečení firemního objektu s využitím moderních technologií je v současnosti aktuálním tématem. Využití inteligentních řešení otevírá nové možnosti v podnikatelské sféře. Využitím inteligentního zámku se firmě nabízí chytré řešení pro docházkový systém, monitoring pohybu v budově či zvýšení míry zabezpečení. Objekt je možné spravovat bez přítomnosti odpovědné osoby.

Cílem této práce je návrh zařízení pro ověření totožnosti / autorizace vstupu do uzamčených prostor s možností správy klíčů bez jejich přítomnosti.

V teoretické části této práce nejdříve zabývá přístupovým systémem elektronické kontroly vstupu, kde se zabývá tématy od historie, architektury a identifikace až po přiblížení co je to autentizace a autorizace. Dále jsou v práci rozebrány možnosti identifikace od použití biometrie až po využití nosičů pomocí technologie RFID. Práce se poté zabývá analýzou firmy a vybráním nejvhodnějšího systému.

V praktické části je potom navržený a vypracovaný systém pro jednoduchou a přívětivou správu osob autorizovaných ke vstupu. Jsou zde rozebrány využité prvky a nastíněna softwarová stránka této práce.

1 Elektronická kontrola vstupu (EKV)

Elektronickou kontrolu vstupu (EKV) lze definovat jako elektronický systém určený k automatizovanému řízení vstupů v kontrolované oblasti. Přičemž kontrolovanou oblastí se rozumí oblast, v níž se nachází chráněný majetek a kterou má majitel zabezpečovacího systému pod svou kontrolou. Přístupové karty pomáhají monitorovat pohyb osob v budově. Chování systému EKV definuje tzv. autorita, což je osoba, která určuje jaké vstupy může která osoba a v jakém čase používat. Pro zajištění bezpečnosti se musí spolehlivě zjistit identita osoby, která žádá o povolení k použití vstupu. Ke spolehlivému zjišťování identity osob se používají autentizační techniky. Pomocí čteček je možné monitorovat zaměstnance na pracovišti, rozlišují se na kontaktní, kdy osoba přímo přikládá zdroj informace a nekontaktní kdy jsou informace snímány nepřetržitě ve vzdálenosti 1-2m. Pokud objekt v chráněné oblasti není identifikován, nebude vpuštěn [3],[8].

1.1 Historie EKV

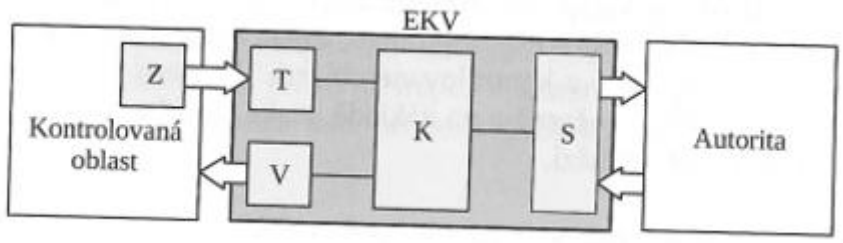
První zmínky o zámku jako zabezpečovacím systému vznikaly již ve starověkém Egyptě. Archeologické nálezy dřevěných zámků a klíčů z Ninive ukazují, že se ochranou majetku zabývali i starověcí Asyřané. Ve starověku se poté začalo rozvíjet zámečnictví jako řemeslo, kvýrobě se používal kov. Čím více byly zahnuté a propracované klíčové praporky, tím bylo zabezpečení kvalitnější. V roce 1778 přišel důležitý vynález anglického zámečníka Roberta Barrona, který zkonstruoval zámek vybavený stavítky. Stavítka se nazývaly páky, které zvedaly klíč do správné polohy, aby bylo možné odemknout zámek. V roce 1817 proběhla loupež v Portsmouthu, kde zloději použili falešný klíč. Britská vláda na tento popud vyhlásila soutěž na výrobu zámku, který by se otevíral jedinečným klíčem. V této soutěži zvítězil Jeremiah Chubb jehož zámek nebyl ani po třech měsících prolomen. Cylindrická vložka, která se používá dodnes byla vynalezena vědcem, který nese jméno Linus Yale. Válec s otvorem obsahoval několik stavítek a blokovacích kotlíků. což umožnilo vyrábět velké množství klíčů. Tento vynález se do Evropy dostal se zpožděním, po skončení první světové války. Systémy EKV se začaly používat zhruba od šedesátých let minulého století s cílem odstranit problémy související se ztrátami klíčů, elektronicky evidovat přístupy osob a zrychlit procesy související jak s přidělováním, tak i s rušením přístupových práv osob. K autentizaci osob se nejprve používaly klávesnice k zadávání hesel a později nastoupily tzv. Wiegandovy karty. Rozvoj elektroniky následně přinesl nástup bezkontaktních karet a v poměrně nedávné době se začala k autentizaci osob využívat také biometrika a smartfony [4],[3].

1.2 Architektura EKV

Mezi základní prvky systému EKV patří kontrolér K (řídící jednotka), terminál T (klávesnice, čtečka), elektronicky ovládaný vstup V (např. dveře osazené elektrickým zámkem) a správní jednotka S.

Celý systém EKV je řízen jednotkou Kontroler a v rámci tohoto řízení zejména ovládá vstupy V v kontrolované oblasti v souladu s přístupovým seznamem. Uvedený seznam je vytvořen autoritou a obsahuje ID a práva všech uživatelů. Dalším prvkem architektury je terminál T,

který žadatelům Z o použití vstupu umožňuje komunikaci se systémem EKV. Vstup umožňuje osobám pohyb do prostoru za překážkou. Posledním základním prvkem je správní jednotka S, která je určena ke správě systému EKV. Autorita jejím prostřednictvím provádí správu přístupového seznamu a případně získává informace o událostech v systému. Ke komunikaci mezi výše uvedenými prvky se vytváří komunikační systém. Většinou se jedná o kombinaci smyček a sběrnic nebo počítačové sítě [3].



Obrázek 1 Blokové schéma EKV [3]

Na obrázku výše je vyobrazeno fungování systému EKV. Žadatel Z nejprve systému umožní, aby o něm získal autentizační data. Autentizační data systému získá pomocí terminálu, jehož prostřednictvím žadatel například zadá PIN, nechá si sejmout otisk prstu nebo si jím nechá vyčíst data ze své přístupové karty. Zjištění a ověření identity se nazývá autentizace a provádí ji buď kontrolér nebo v modernějších systémech terminál. Po úspěšné autentizaci kontrolér z přístupového seznamu zjistí, zda autorita danému žadateli udělila právo pro vstup. Pokud ano, tak kontrolér vyšle do jím ovládaného vstupu příkaz k otevření a osoba může vstupem projít. V opačném případě zůstane vstup zamčený [3].

1.3 Identifikace v systémech EKV

Aby bylo možné uživatele v systémech jednoznačně rozlišovat, tak je nutné každému z nich přidělit unikátní identifikátor ID. Tento identifikátor by neměl být sdílený, měl by být používán pouze jedním subjektem. V systémech EKV se jako identifikátory nejvíce používají tzv. Wiegandova slova [3], [6].

Identifikace je tedy proces pro jednoznačné určení identity uživatele. Může se jednat například o prohledání databáze biometrické informace systému pro otisku prstu. Mluvíme tedy o vyhledávání a systém se snaží odpovědět na otázku„Kdo to je?" [15].

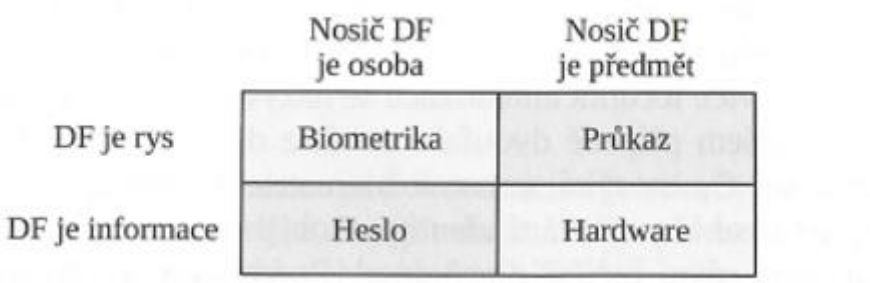
1.4 Autentizace

Autentizaci osob provádí zařízení, které nazveme autentizátor, přičemž v systémech EKV tuto funkci plní buď kontrolér nebo terminál. Každý uživatel s ID = X má k dispozici svůj dokazovací faktor. Autentizace uživatele je založená na tom, že[6]:

- **Uživatel něco ví** – nejčastěji používaná metoda založená na tom, že systém uživatele vyzve k zadání jeho hesla, nevýhodou této metody je snadné prolomení, odposlech, uhádnutí hesla jiným uživatelem.

- **Uživatel něco má** - metoda založená na vlastnictví předmětu (USB, karta, čip...), uživatel je vyzván k použití vlastněné věci, v případě ztráty předmětu je však nutné se osobně dostavit na místo, kde se vydávají předměty nové.
- **Uživatel něco je** – metoda založena na biometrických znacích, uživatel je vyzván například k otisku svého prstu.

Podle kombinací dokazovacího faktoru DF a druhu nosiče lze autentizaci řadit do čtyř skupin jak je vidět na obrázku níže.



Obrázek 2 Třídy autentizace [3]

Pokud je tedy zmíněná autentizace, tak se jedná o proces ověření identity uživatele, při kterém uživatel předloží tvrzení o své identitě. Systém se tedy zabývá otázkou: „Je osoba opravdu tou, za kterou se vydává?". Podle udaného tvrzení o identitě se srovnávají např. biometrické charakteristiky s uloženými charakteristikami v autentizační databázi. Autentizace je také známá pod názvem verifikace [15].

1.5 Autorizace

Pro vstup do kontrolované oblasti je potřeba aby proběhla tzv: autorizace osoby. Autorizace je proces, v němž osobě autorita sdělí její přístupová práva (např: jaký vstup a kdy může využít), specifikuje, co konkrétní uživatel může či nemůže. Autorita přiřadí osobě její identifikátor ID, dokazovací faktor DF a ověřovací faktor OF. Identifikátor je využíván jako unikátní označení, pod kterým je osoba nadále v systému EKV zařazena [3], [15].

2 Biometrie

Biometrické technologie jsou založeny na měření fyziologických vlastností člověka (otisk prstu, obraz krevního řečiště, rohovky) nebo na chování člověka (dynamika podpisu, vzorek hlasu...). Měření probíhá automatizovaným způsobem[15].

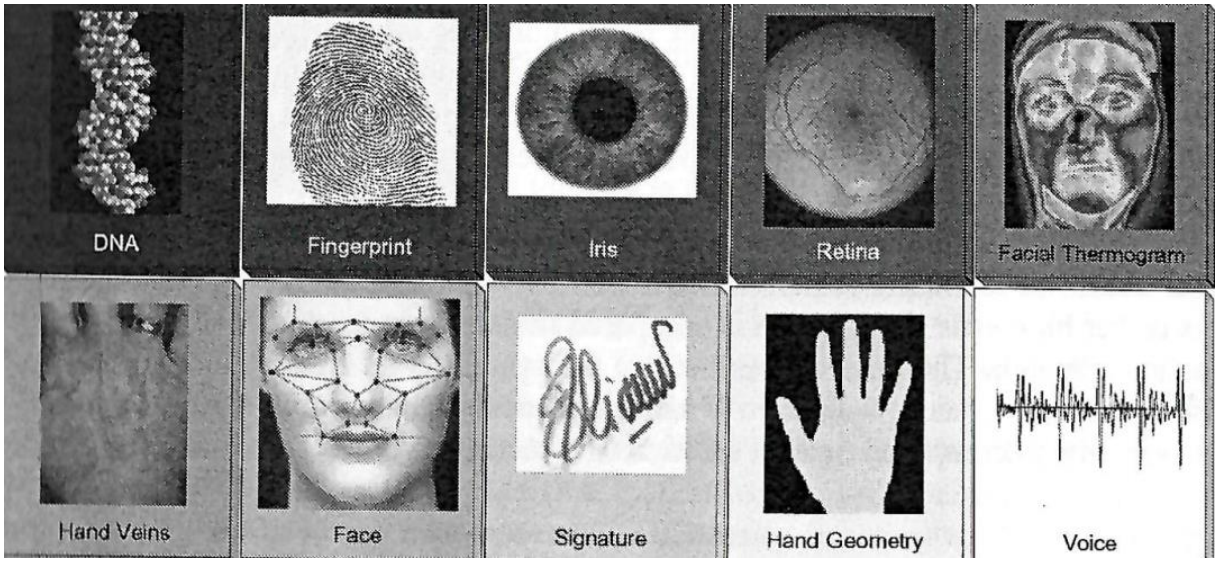
2.1 Úvod do biometrie

Biometrie se v oboru IT zabývá identifikací člověka podle unikátních charakteristických rysů daného člověka. Tyto rysy dělíme na anatomické (fyzické), kam patří například: otisk prstu, žíly ruky, obličej, sítnice, duhovka, dentální obraz, tvar ucha, DNA. Tyto vlastnosti jsou vždy přítomné a je těžké je ovlivnit. Druhá skupina je skupina behaviorálních rysů (dynamických) mezi které patří: hlas, chůze, mimika obličeje s pohybem rtů. Dynamické vlastnosti můžeme lehce ovlivnit, to po nasnímání může vést k různým odlišným výsledkům, jelikož do této skupiny zapadá ovlivnění psychického i fyzického stavu, který může změnit pouhý stres nebo nemoc. V některých případech je možné zvýšit míru zabezpečení použitím fyzické ostrahy u snímače, která zamezí nežádoucí manipulaci se zařízením. Za nejspolehlivější biometrickou metodu lze považovat DNA, za tu nejméně spolehlivou poté hlas [2], [6], [9].

Spolehlivost biometrického systému je možné určit pomocí ukazatele FRR (False Rejection Rate), který vyjadřuje počet zamítnutých přístupů člověku, jemuž přístup zamítnut neměl být. Dále FAR (False Acceptance Rate) kolik neoprávněných uživatelů mělo přístup do systému povoleno, ačkoliv měl být zamítnut. Čím nižší je tato hodnota, tím je systém spolehlivější. Výhodou autentizačních metod s využitím biometrie je, že není možné zapomenout či ztratit autentizační klíč, ani se časem nemění. Mezi nevýhody patří nutnost speciálního softwarového a hardwarového vybavení v místě autentizace [6].

Biometrické systémy se dělí na přístupové a forenzní. Tyto systémy se liší dle využití. Přístupové systémy mají funkci verifikační, která vyhodnocuje přístupová práva do objektu s omezeným přístupem. Forenzní biometrické systémy jsou využívány k identifikaci osoby například zjištění totožnosti v policejních databázích. Biometrii je možné využít i v oblasti ověřování podpisu, kdy se posuzuje sklon písma, stisk pera či hloubka podpisu [9],[10].

Dále je možné dělit systémy podle toho, zda vyhodnocují jednu či více biometrických charakteristik na unimodální a multimodální. Unimodální vyhodnocuje pouze jednu biometrickou vlastnost. Multimodální vyhodnocuje více vlastností současně, je tedy zaručena vyšší bezpečnost systému, než u systému s unimodálním zabezpečením [9].



Obrázek 3 Ukázka biometrických atributů [2]

2.2 Otisk prstu

Všichni lidé mají na povrchu prstů papilární linie, tyto linie jsou pro jednotlivé osoby jedinečné. Vyskytují se na prstech rukou i nohou. Díky jedinečnému tvaru můžeme jednoznačně určit identitu člověka. Papilární linie má přibližnou výšku 0,1 až 0,4mm a šířka se pohybuje okolo hodnot 0,2 až 0,5mm. Výjimkou mohou být lidé postižení různými druhy onemocnění, poraněním a poruchami kůže, které by nenávratně změnily jedinečný vzor prstu. Nauka, která se zabývá zkoumáním otisků obrazců papilárních linií se nazývá Daktyloskopie. V tomto oboru platí tři zákony [2], [5]:

1. Neopakovatelnost – na světě neexistují dva jedinci, kteří mají absolutně shodné obrazce papilárních linií.
2. Relativní neměnnost – obrazce papilárních linií jsou po celý život relativně neměnné (jedinec se stále v průběhu života částečně mění a dochází k zhrubnutí, tvorbě vrásek nebo jizev).
3. Neodstranitelnost – obrazce papilárních linií jsou trvale neodstranitelné, pokud není odstraněna zárodečná vrstva pokožky (pokud je odstraněna zárodečná vrstva, vznikne jizevnatá tkáň)

Papilární linie tvoří poté vzor, který je znám jako třída otisku prstu. Mezi tyto třídy patří[5]:

- oblouk,
- klenutý oblouk,
- spirála (také známá jako závit nebo vír),
- levá smyčka,
- pravá smyčka.

Obrázek 4 Základní dermatoglyfy[7]

Při autentizaci pomocí otisku prstů se ukládají pouze určité charakteristiky prstu, není tedy možné dle nich celý otisk zrekonstruovat. [6]

Pro systémy EKV se používají nejčastěji snímače optické a kapacitní. Optické fungují na principu fotoaparátu. Na získaném snímku se porovnávají v počítači typy markantů a jejich souřadnice. Optické snímače existují dotykové a bezdotykové[3].

2.3 Geometrie ruky

Za instalaci úplně prvního biometrického zařízení je považováno zařízení Identimat, které bylo nainstalováno jako jedna z částí docházkového systému Shearson Hamill firmy Wall Street Investments už v sedmdesátých letech minulého století a využíval rozpoznávání pomocí geometrie ruky. S Pomocí 2D a 3D technologie dokážeme využít geometrii ruky pro rozpoznávání, jelikož je tvrzeno že lidská ruka je taky jedinečná pro každého jedince. Rozpoznávání pak využívá tyto charakteristiky ruky:

- délka prstů,
- šířka prstů,
- výška prstů,
- zakřivení a lokální anomálie.

Zařízení pro rozpoznávání geometrie ruky je nákladnější a větší než zařízení pro snímání otisku prstu. Tato metoda se používá pro zabezpečení strategicky významných prostor. Výhodou této

metody je, že není lehce kopírovatelná, snižuje se zde riziko zneužití. Většinou je snímána pouhá silueta ruky vrchní, nebo spodní část. Pomocí zrcadla lze získat i třetí rozměr. Dokonce i rozlišení kamery je menší než u použití senzoru otisku prstu. Pro rozlišení ruky od pozadí se používá reflektující dopadající světlo pod ruku, tím se kontrast ruky a podložky zvýší a usnadní proces[5],[6].

2.4 Rozpoznání podle obličeje

Metoda rozpoznávání obličeje je obecně založena na vzdálenosti mezi specifickými body. Měří se velikost očí, úst, nosu a vzdálenost mezi nimi. Spolehlivost metody však ovlivňuje osvětlení a úhel snímání. S autentizací pomocí rozpoznávání obličeje je možné se setkat u některých typů chytrých telefonů, kdy je možné s jejich pomocí zaplatit v bance či přihlásit se do aplikací.

Pokud dochází ke skenování obličeje pomocí infračerveného světla, které na obličej promítne pomyslnou mřížku a změří i hloubku obličeje, je možné systém považovat za spolehlivý. V rámci této metody totiž vytvoří 3D model tváře, který se porovná se vzorkem uloženým v databázi. Pro zvýšení bezpečnosti této metody je možné použít termosnímky obličeje[6].

2.5 Geometrie oka – oční duhovka, oční sítnice

Rozpoznávání duhovky a sítnice je další metodou pro autentizaci. Sledován je pohyb oka, změna zornice či mrkání, což zamezuje zneužití pomocí fotografie. Tato metoda patří mezi nejspolehlivější. V případě rozpoznávání sítnice se snímá obraz struktury okolo slepé skvrny pomocí zdroje světla s nízkou intenzitou. Mezi výhody použití duhovky v biometrii patří[5]:

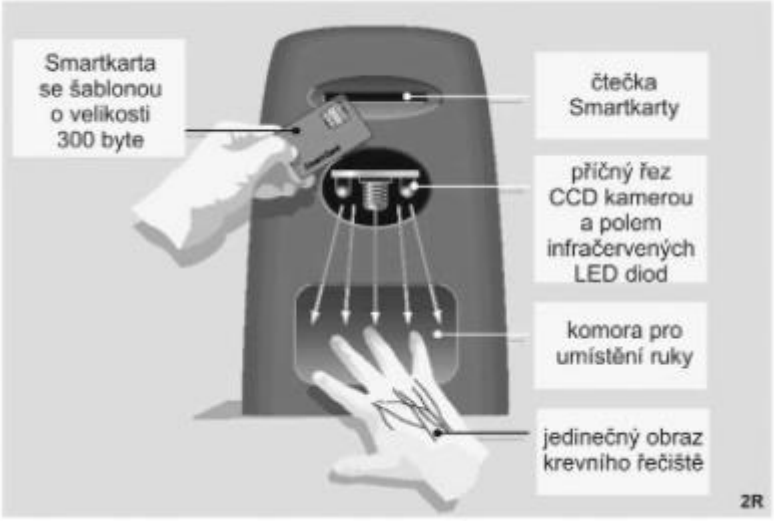
- stabilita během života – duhovka se nemění,
- jedná se o vnitřní orgán – chráněn proti vnějším vlivům,
- neinvazivní pořízení snímků.

Mezi nevýhody lze zařadit [5]:

- nutnost spolupráce uživatele, který musí být v předepsané poloze a vzdálenosti,
- vysoké náklady na pořízení systému,
- obraz duhovky může mít nízkou kvalitu, což může způsobit chyby ve verifikaci, autentizace či registraci[6].

2.6 Rozpoznání podle žil na rukách

Tvar, velikost a orientace cév je unikátní pro každého člověka. I proto je možné použít žíly na rukou pro biometrickou autentizaci. Obraz krevního řečiště se formuje již v prenatálním období. Odlišuje se na ruce levé i pravé. Porovnávací vzorek se pořizuje na ploše skeneru, který používá infračervené diody a ruce jsou snímány černobílou CCD kamerou s šestnácti stupních šedi, díky tomu jsou žíly dobře vidět. Díky snímání tepelného vyzařování je možné zároveň ověřit, že je uživatel živý. Snímání krevního řečiště je bezkontaktní formou, je zde tedy zaručen vyšší hygienický standard[14].



Obrázek 5 Schematický řez skenerem, který je vybaven čtečkou na smart karty, kde je uložena biometrická šablona držitele

2.7 Rozpoznání podle hlasu

U metody rozpoznávání hlasu je nutné nejprve vytvořit voiceprint neboli otisk hlasu. Proti tomuto otisku se porovnává hlas osoby, která se autentizuje. Tuto metodu však ovlivňuje prostředí, ve kterém se systém nachází, okolní ruch může rušit systém při rozpoznávání hlasu. Dalšími rušivými faktory může být nachlazení uživatele, použití různých druhů mikrofonů s různou frekvencí a kvalitou.

Ověření je možné provést buď opakováním fráze, o kterou systém požádá, nebo z přirozené řeči. Nejčastějším řešením je přečtení náhodně vygenerovaných čísel. Tato metoda zabraňuje útoku v podobě nahrání hlasu určité osoby. Bezpečnost lze posílit kombinací se zadáním určitého hesla, PIN či jiného biometrického znaku. [11], [6].

2.8 Proces biometrické identifikace

Biometrická identifikace se skládá ze šesti kroků[14]:

1. **Získání biometrických dat –** v tomto kroku se uživatel poprvé setká se systémem, získá se uživatelův vzorek, který bude později porovnáván. V této fázi je nutné, aby byla přítomna proškolená obsluha zařízení, která zajistí kvalitu vzorku.
2. **Vytvoření vzorových charakteristik –** po snímání charakteristik následuje jejich zpracování, obecně je vyžadováno 3-5 vzorků. Vzorky se neuchovávají v originální podobě, pouze již zpracované, které dokáží člověka rozlišit. Pomocí zpracovaných vzorků již nelze rekonstruovat celý odebraný vzorek.
3. **Uložení vzorových charakteristik –** poté, co se naleznou důležité charakteristiky je potřeba vzorek uložit. Registrační záznamy se ukládají na kartu, do centrální databáze či do autentizačního terminálu.
4. **Snímání –** v této fázi je důležité, aby podmínky byly podobné ve fázi získávání. Například okolní hluk při rozpoznávání hlasu či vlhkost při otisku prstu. V této fázi se

testuje také, zda systém správně odhalí “živost” člověka, tedy že se nejedná o maketu či obrázek.

5. **Vytvoření nových charakteristik –** biometrická data získaná z fáze snímání se dále zpracují a tím se získají nové biometrické charakteristiky.
6. **Srovnání –** získané biometrické statistiky se porovnají s těmi, které byly získány ve fázi registrace.
7. **Rozhodování –** konečná fáze verifikace, kdy systém vyhodnotí na základě prahové hodnoty, zda se jedná o autorizovaný přístup.

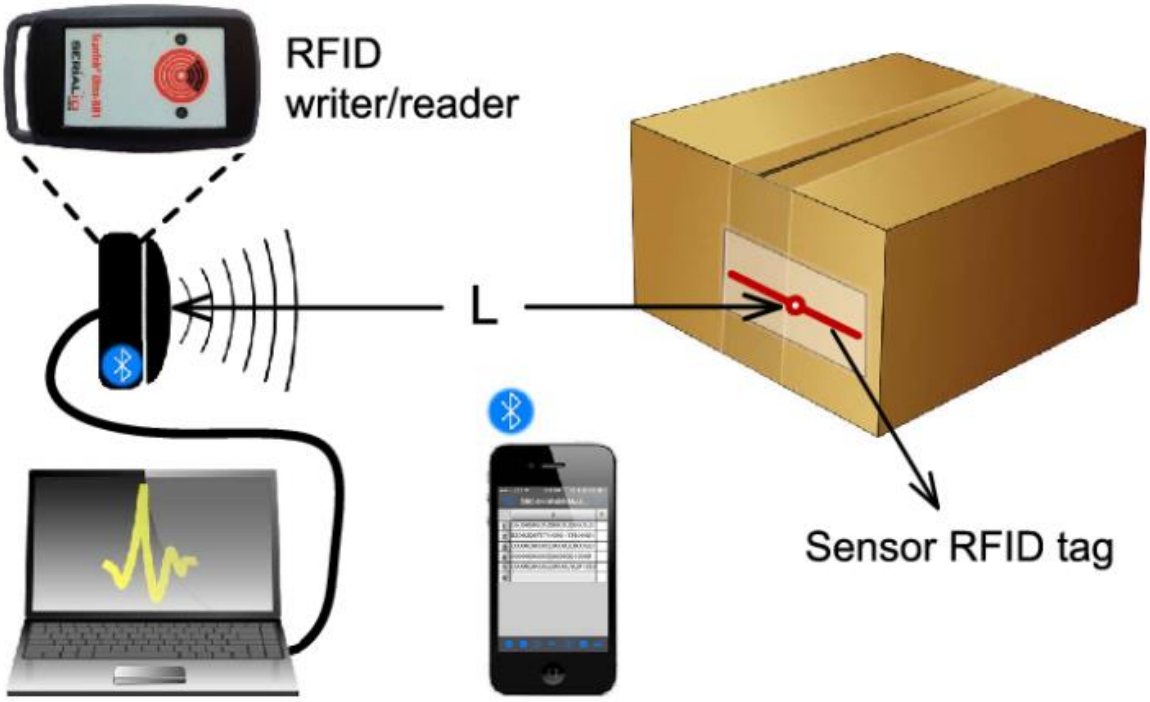
3 RFID (Radio frequency identification)

RFID se řadí mezi metody autentizace založené na vlastnictví předmětu. Nevýhodou této formy autentizace oproti biometrii je možnost ztracení autentizačního předmětu. Nejčastěji se s touto technologií můžeme setkat ve formě přístupových karet.

RFID technologie pracuje na bezkontaktním typu přenosu dat s využitím rádiových frekvencí, které slouží pro získání dat v rámci určité vzdálenosti mezi transpondérem a čtečkou. Tato technologie se využívala už při druhé světové válce k rozpoznání neboli identifikaci bojových letadel. RFID systémy se dělí na pasivní, které nemají v tagu (přívěsku, který je nosičem dat) vlastní zdroj napájení a využívají potom elektromagnetickou energii přijímanou z RFID čtečky. Díky absenci napájecího zdroje, jsou jednoduché, malé a jejich cena je nízká. Jejich životnost, není omezená a pokud nejsou poškozeny. Hlavní využití mají v docházkových a vstupních systémech, ale využívají se i jako chytré etikety nebo pro identifikaci produktů. Naopak aktivní RFID systémy obsahují zdroj napájení, který vysílá vlastní signál. Vysílací signál lze využít k trasování polohy produktu a sledovat jeho pohyb. Jejich cena je značně dražší a velikost větší, ale dosahující vzdálenost mnohonásobně vzrůstá. Bohužel jejich životnost je omezená kvůli napájení baterie a jejich životnost může být přibližně 3 až 5 let, poté je nutno vyměnit celý tag. Aktivní RFID tagy potom dělíme na tři kategorie,, transponders", „beacons" a semipasivní. Beacons (maják) vysílá opakovaně informaci každých 3 až 5 vteřin a nezabývá se, zda je v dosahu čtení, nebo ne. Pro úsporu baterie můžeme zmenšit vysílací výkon, ale s tím se nám taky úměrně snižuje čtecí dosah. Transponders je naopak šetrný na baterii, protože se aktivuje až při zachycení signálu čtečky, čímž šetří spoustu energie v případě, že tag není v jejím dosahu. Transponders (odpovídač) se využívají hlavně pro bezpečnostní přístupové systémy. Semipasivní tag obsahuje baterii, ta se nepoužívá pro vysílání signálu, ale pouze pro napájení přijímače, tím se oproti pasivním tagům zvýší vysílací výkon, který vede k delšímu dosahu. RFID pracuje na různých frekvencích, které můžeme rozdělit jako: [12],**[13].**

- Nízkofrekvenční (LF – Low Frequency) 125-134 kHz,
- Vysokofrekvenční (HF – High Frequency) 13,56 Mhz,
- Ultra-vysokofrekvenční (UHF – Ultra-High Frequency) 865-960 Mhz,
- Mikrovlny 2,45 GHz.

Tento systém většinou má tři části, a to RFID tag, čtečku a systém zpracování dát zvaný middleware. Tag je nosičem informace, na kterém je uložen. Může se skládat z čipu, antény a obalu. Pro bezkontaktní čtení informace z tagu se používá čtečka, která vysílá rádiové vlny. Tag na tyto rádiové vlny reaguje, pokud je v dostatečné vzdálenosti. Čtečka se skládá z antény a kontrolní jednotky. Kontrolní jednotka má za úkol kódovat, dekódovat a uchovávat data. Může být i propojena s databází. Middleware zpracovává informace a propojuje data zachycené čtečkou s daty uživatele [12].



Obrázek 6 Princip fungování RFID technologie [1]

Používají se tři základní formáty:

1. Chytré etikety
2. Tokeny a chytré karty
3. implantáty

Chytré etikety mají malou velikost a nízkou cenu, takže jsou vhodné pro stejnou funkci jako čárové kódy. Většinou využívají paměti ROM a jsou pasivní RFID tagy. Po načtení tagu je zobrazeno jedinečný identifikátor a je spojen s příslušnou databází.

Token je označení čipu využívajícího k rozpoznání a autorizaci osoby. Může být zahrnutý v kartách využívající pro bankovnictví nebo oprávnění vstupu do prostoru. Chytrou kartou značíme pak jako lepší variantu tokenu pro bezkontaktní čtení chytrou čtečkou. Pasivní RFID čip lze pak přečíst na vzdálenosti centimetrů. Pro prodloužení čtecí vzdálenosti se zase využívá aktivní RFID čip. Legolend dokonce využívá náramky s aktivním RFID čipem pro hledání ztracených děti.

V dnešní době už jsou i RFID čipy implantovány do zvířecího nebo dokonce i lidského těla. Využití je shodné s tokeny ohledně rozpoznání a autorizace nositele. Výhodou je že implantát je velice nepravděpodobné zneužít cizí osobou nebo jej ztratit jako například tokeny a karty. Nizozemský klub Baja Beach Club sídlící v Rotterdamu údajně využívá implantáty pro VIP členy klubu [12].

4 Analýza

Pro výběr správného zařízení pro konkrétní společnost, je důležité provést základní analýzu firmy, zjistit její požadavky a u nich následně provést analýzu. V následující kapitole se nachází popis firmy, definice požadavků, jejich analýza a shrnutí s výběrem vhodného systému na závěr.

4.1 Popis firmy

V rámci této bakalářské práce bude navržen elektronický zámek pro firmu S-Auto.cz s.r.o. Jedná se o firmu, která se zabývá nákupem, prodejem, servisem vozů značky Audi. V současné době má pronajatý areál v blízkosti Pardubic, kde se nachází dílny, garáže a parkování pro skladové vozy.

Firma v současné době nemá interní zaměstnance, pouze externí pracovníky. V areálu není výrazně frekventovaný pohyb. V současné době firma nevyužívá moderních systémů zabezpečení. Ve firmě se používají standardní klíče a dálkové ovládání pro otevírání brány a garáží. Nevýhodou tohoto systému je nutnost půjčování klíčů a být přítomen v areálu pro kontrolu, zda externí pracovníci nevstupují do prostor, kam by vstupovat neměli.

V rámci zadání byly uskutečněny osobní schůzky s majitelem firmy spojené s prohlídkou areálu a společnou diskusí na téma zabezpečení pomocí elektronického zámku. Z tohoto rozhovoru vzešla myšlenka, že největším problémem je vyzvedávání aut klientů, případně jejich příjem a vypůjčení náhradního vozidla. Klienti, kteří jsou z celé České republiky z pravidla využívají služeb pozdě k večeru, někdy i v noci, případně o víkendu mimo pracovní dobu. Elektronický zámek by umožnil vydání či vypůjčení auta v případě, že si klient potřebuje své auto vyzvednout po servisní prohlídce pozdě odpoledne, kdy již není přítomen majitel firmy. Tento systém je možné použít u dlouholetých zákazníků, areál je pod kamerovým systémem. Po předchozí dohodě (při příjmu auta) lze vystavit zákazníkovi kartu se vstupem v předem sjednaný den.

Další situací, kterou by firma pomocí elektronického zámku ráda vyřešila, je spolupráce s externisty, kteří nezřídka kdy mají čas večer, po pracovní době, případně o víkendu. Zde by bylo vhodné sledovat také pohyb osoby po areálu, tedy sklad, kancelář, dílny, garáže apod.

Jelikož se do firmy pravidelně dováží objednané zboží v sjedaných hodinách, tento systém by mohl využívat i pravidelný dovozce pro bezkontaktní vyložení objednávky.

4.2 Zadání řešení

Firma si tedy přeje vytvoření systému, který umožní vstup povolaných osob do areálu mimo pracovní dobu i v nepřítomnosti majitele firmy. Tento systém by neměl být složitý, měl by jej umět obsloužit každý při prvním setkání a v rámci možností i cenově dostupný.

4.3 Rozbor možných řešení

Dle požadavku zákazníka budou posuzována následující kritéria:

- uživatelská přívětivost,
- komfort,
- náklady,
- vhodnost použití,
- dostupnost (získání autentizačních dat),
- praktické použití,
- údržba systému.

4.3.1 Uživatelská přívětivost

Prvním posuzovaným kritériem je uživatelská přívětivost, v rámci toho kritéria je třeba zhodnotit, jak budou se systémem zacházet zákazníci, kteří jej uvidí poprvé, zda bude nutné k systému speciální proškolení, či jej bude možné používat intuitivně.

Biometrie

Při využití řešení pomocí biometrie je třeba získat souhlas zákazníka pro odběr a uložení dané biometrické informace, s touto okolností zákazník nemusí souhlasit z hlediska svého soukromí. Znamená také jedno setkání s majitele firmy navíc, kdy bude nutné biometrické informace odebrat. Uchovávání takových údajů znamená pro firmu komplikaci v podobě uchovávání osobních údajů a jejich zabezpečení. Dále je vhodné uživatele se systémem seznámit a proškolit, například v jaké vzdálenosti by měl pro snímání stát, nebo jak přiložit posuzovaný znak, případně říci že je zapotřebí sundat šperky.

RFID

V rámci uživatelské přívětivosti je dle mého názoru vhodnější využití RFID technologie. Není zde potřeba provést schůzku předem, kartu je možné zaslat klientovi poštou. Zaznamenání čísla karty do databáze a její předání zákazníkovi je rychlé. V rámci uživatelské přívětivosti je tento systém velice intuitivní, je potřeba pouze přiložit kartu ke čtečce, která zajistí otevření dveří. Karty se v dnešní době používají běžně, nepředpokládá se tedy problém s obsluhou čtečky.

4.3.2 Komfort

Dalším posuzovaných kritériem je komfort, který je důležitý z hlediska zákazníka i firmy. Nový systém by měl poskytovat komfort pro klienta, který bude vědět, jak jej využít a nebude pro něj představovat potíže.

Biometrie

Významnou výhodu biometrie spatřuji v nemožnosti ztráty klíče. Majitel vozu může vždy použít otisk prstu či jiný biometrický znak. Klíč nelze zapomenout nebo ztratit, tedy je zde nižší riziko zneužití. Oproti tomu není možné, aby auto vyzvedl někdo jiný, například blízká osoba

klienta, což může být vnímáno jako nevýhoda tohoto systému s ohledem na klientelu, kdy se jedná například o firemní vůz, který může vyzvedávat při každé návštěvě jiný zaměstnanec. Tento aspekt se promítá i do zásobování, kdy s potřebnými součástkami nejezdí pouze jeden zaměstnanec.

RFID

Při použití RFID technologie je třeba mít u sebe kartu či tag. Výhodou je, že se nosič může zvolit ve vhodné velikosti, nemusí se jednat přímo o kartu. V případě ztráty, kdy klient nebude mít kartu u sebe, je možné ji kdykoliv z databáze vymazat – učinit ji neaktivní. To vnímám jako výhodu z důvodu, že není potřeba měnit zámkovou vložku, jako je tomu u klasických zámků. Pokud se klient nebude moci dostavit osobně, může za sebe poslat kohokoliv, kdo bude mít kartu u sebe.

4.3.3 Náklady

V rámci tohoto kritéria je nutné zhodnotit náklady na pořízení a provoz.

Biometrie

Při zakoupení systému s využitím biometrie nevznikají žádné vedlejší náklady v podobě karet či tokenů. Pořizovací cena je proměnná pro každý systém, ale může být mnohonásobně vyšší při zaměření na kvalitu než u RFID.

RFID

Zařízení na bázi RFID technologie je cenově dostupnější. Je však nutné hlídat počet karet/tagů či tokenů, které jsou k dispozici pro zákazníky, cena jednoho tokenu je dle objednaného počtu od 7 Kč. Cena karty je podobná, orientačně 8-10 Kč.

4.3.4 Vhodnost použití

U tohoto kritéria je potřeba zohlednit vhodnost řešení ve vztahu k areálu, klientům a majitele firmy. Hledá se řešení pro cca 30 osob – stálých zákazníků a partnerů. Areál je monitorován bezpečnostními kamerami.

Biometrie

V rámci kritéria vhodnosti použití je nutné opět přihlédnout k faktu odebrání a uchovávání biometrických znaků, které jsou pro firmu nevýhodou. Biometrický systém není dle mého názoru intuitivní, mohl by působit na klienty složitě, případně by mohlo docházet k opakovaným pokusům o autentizaci nevhodným použitím, což by se však mohlo negativně projevit ve vztahu k firmě.

RFID

Systém založený na RFID technologii se jeví jako jednodušší, intuitivnější. S ohledem na servis firemních automobilů i vhodnější. Automobil může vyzvednout držitel karty, nemusí se jednat

o majitele vozu. Systém by měl být zvládnutelný i pro neinformované uživatele. Dalším přínosem bude jednoduchá registrace nových karet pomocí RFID čtečky. Registraci nových karet tedy bude moci provést majitel firmy, aniž by byl ohrožen správný odběr autentizačního vzorku. Navíc jsou dostupné různé vzory karet či tokenů, může se tedy jednat i o stylový propagační materiál, nutno podotknout, že tímto krokem může být snížena míra bezpečnosti.

4.3.5 Dostupnost (získání autentizačních dat)

Důležité kritérium z hlediska firmy, kdy je potřeba zhodnotit způsob získání autentizačních dat. Tento proces by měla firma zvládnout sama, je tedy důležité počítat s tím, že by jej do budoucna prováděl některý ze zaměstnanců, v současné době majitel firmy.

Biometrie

Při využití systému s použitím prvků biometrie se klient musí fyzicky dostavit pro sejmutí biometrického znaku a jeho uložení do databáze. Odběr vzorku by měla provádět proškolená osoba ve stabilním prostředí, aby se předešlo budoucí chybovosti při autentizaci. To představuje pro vybranou firmu problém v podobě neproškolené obsluhy. Proces je časově náročnější než u využití RFID.

RFID

V rámci tohoto kritéria je RFID technologie představuje přívětivější řešení. Výhodou je, že zákazník nemusí být u vytváření nové karty či tagu, karta mu může být předána preferovanou cestou. Pokud si zákazník bude přát, je možné ji doručit zcela bez osobního kontaktu prostřednictvím pošty. Další výhodou je, že firma nemusí ukládat biometrické znaky klientů.

4.3.6 Praktické použití

Zařízení pro autorizaci bude umístěno vně areálu ve venkovních podmínkách. Bude tedy náchylné k vandalismu a vnějším vlivům.

Biometrie

Potřeba vhodného umístění, podle daného biometrického snímání. Systém s použitím biometrie může budit pozornost okolí, stále se jedná o zařízení, se kterým se není možné prozatím běžně setkat.

RFID

Není potřeba vizuální kontakt mezi fyzickým nosičem dat a čtecím systémem. Velice dobrá implementace systému. Tento systém nebudí výraznou pozornost, většina jeho části je schovaná mimo dosah veřejnosti.

4.3.7 Údržba systému

U tohoto kritéria bude vyhodnocena náročnost údržby v průběhu používání systému.

Biometrie

Z hlediska údržby je vhodnější, když se využívá biometrický systém, při kterém se uživatel nedotýká snímače, jelikož plocha bude později namáhaná nebo dokonce může být poškozená. Je vhodné i jednou za čas fyzické prvky systému zkontrolovat, zda například čočka není znečištěná nebo očistit snímače otisku prstu / dlaně z hygienických důvodů. V souvislosti s COVID 19 je vhodnější použití bezdotykových zařízení.

RFID

Jelikož se jedná o bezkontaktní systém a dochází k malému množství kontaktu čipu se čtečkou, tak tento systém je vhodnější z hlediska údržby.

4.4 Shrnutí

Na základě analýzy požadavků firmy bylo rozhodnuto o implementaci zařízení se systémem RFID. Jak již bylo zmíněno, majitel firmy chce jednoduchý a uživatelsky přívětivý systém, což předání karty či tagu a zařazení do systému vychází jako vhodnější možnost. Zákazník nebo dopravce obdrží kartu, kterou si provozovatel firmy zapíše a poté při potřebě jí může zařadit nebo vyloučit z databáze pro povolený vstup. Pokud se zákazník sám nemůže dostavit, tak kartu může předat další osobě, ať už partnerovi nebo třetí straně, která si po domluvě auto může přijet vyzvednout. Na takové předávání karty je možné pohlížet jako nevýhodu při ztrátě, jelikož ji může využít kdokoliv. Využití biometrie je zde složitější, ať už z hlediska odebrání biometrických znaků, tak z hlediska zásahu do soukromí, protože né každý zákazník je ochoten sdílet takové informace. Důležité je přihlédnout k faktu, že se jedná o venkovní prostor, kde může být systém vlivem počasí více namáhán oproti vnitřním prostoru, kde nepůsobí vlivy počasí.

5 Návrh řešení

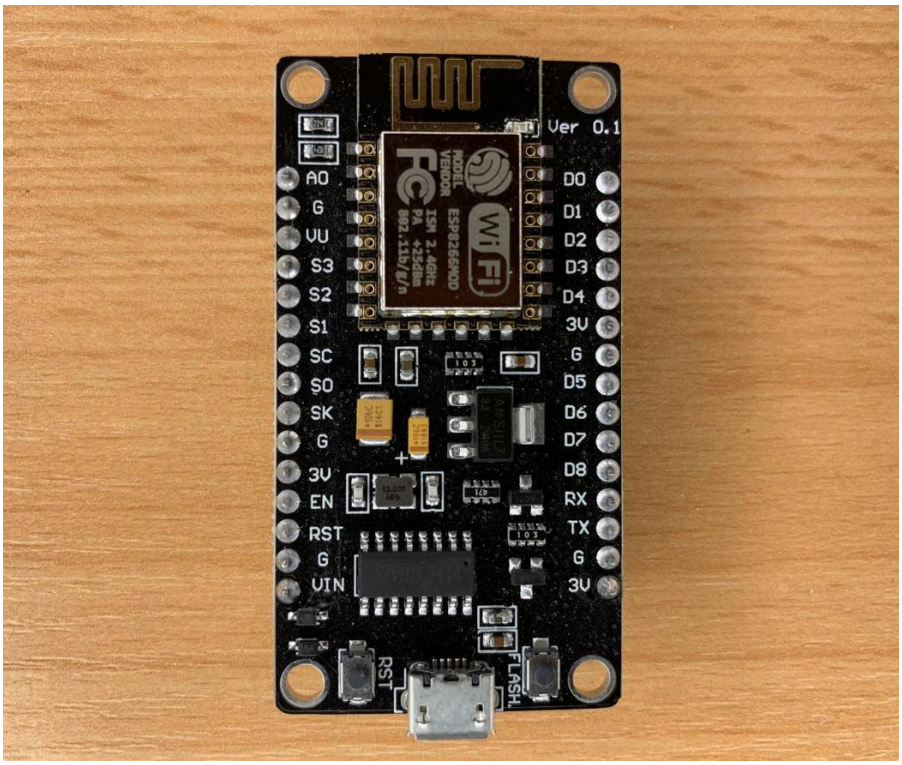
V této kapitole se nachází popis tvorby systému zabezpečení. Jsou zde popsány všechny komponenty pro realizaci zařízení, použité součástky společně s popisem řešení systému a schématem zapojení celého obvodu.

5.1 Použité součástky

Níže jsou popsány součástky použité v projektu.

NodeMcu Lua WI-FI ESP8266

Vývojový modul je založen na čipu ESP8266. Je vybrán především díky jeho bezproblémové práci s WIFI, dobré velikost FLASH paměti 4MB a využití jednoduchosti programovacího jazyku wiring. Tento modul lze lehce připojit k PC pomocí USB mikro konektoru a USB kabelu, ale ovládá i funkci nahrání programu přes WIFI bez připojení k počítači. Deska obsahuje mikrokontrolér ESP-12E, USB serial převodník CP2102, jedenáct digitálních pinů pro input / output a jeden analogový vstup. Potřebné napájecí napětí pro desku je 5 V. Je třeba dát pozor na pracovní napětí desky, které je 3,3 V. Díky menší velikosti modulu, je implementace do systému jednodušší, protože má nižší nároky na prostor.



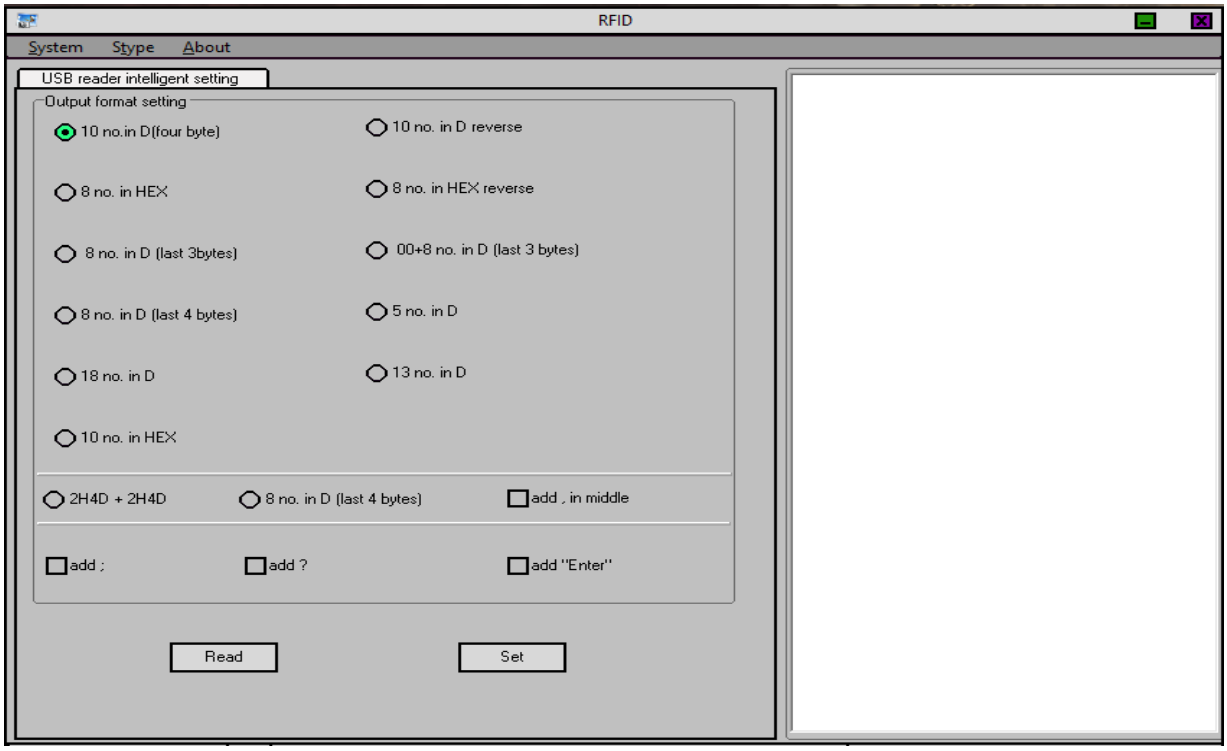
Obrázek 7 Modul NodeMCU Lua WiFi ESP8266 CP2102

Čtečka kódů RFID

Tato čtečka pracuje na frekvenci 13,56 MHz. Pomocí čtečky se zajistí zjištění konkrétního kódů, který je nutný znát pro zápis do databáze. Do projektu byla vybrána z důvodu jednoduchosti práce s tímto modelem, jelikož jí stačí připojit pomocí USB kabelu do počítače a po připojení se do počítače automaticky nainstalují ovladače. Jakmile je takto připojená, tak v momentu přiložení datového nosiče se ozve zvukové upozornění a okamžitě vypíše kód nosiče na obrazovku počítače do místa kde je nakliknut kurzor myši.

Obrázek 8 Čtečka kódů RFID

K vybrané čtečce lze volně stáhnout i program pro změnu formátu, ve kterém čtečka data vypisuje. Je důležité, aby formát dat z této čtečky byl shodný s formátem dat ze čtečky modelu RC522, jelikož by pak data z databáze byla v jiném tvaru než příchozí data z nosiče k porovnání. Po zjištění formátu čtečky RC522, je tato čtečka nastavena na stejný formát 8 no in HEX reverse. Prostředí programu těchto možností je vidět na obrázku níže. Je možnost také přidat automatickou funkci enter po přiložení nosiče, což může urychlit práci v případě, že data zadáváme například do excelu, jelikož se po přiložení dostaneme hned na další řádek.



Obrázek 9 Prostředí pro změnu formátu výpisu nosiče

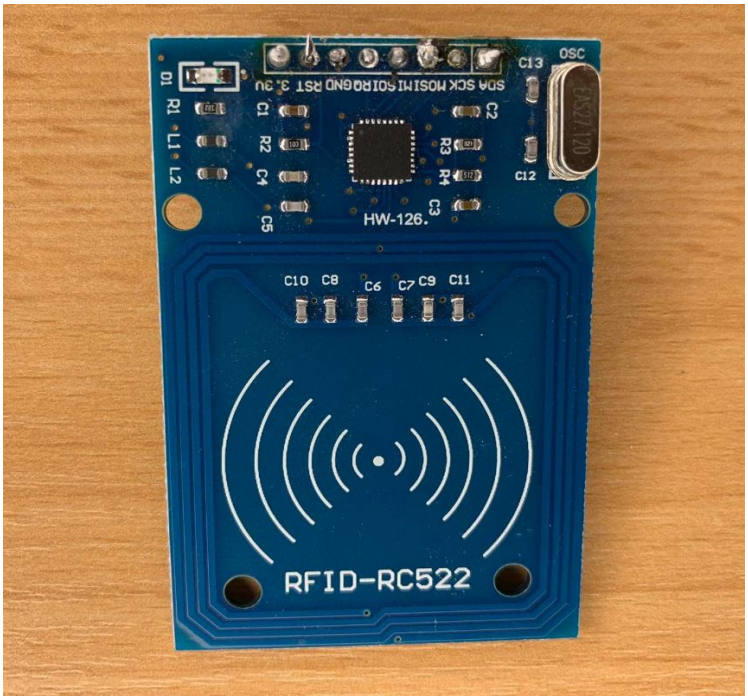
Čtečka funguje jako emulátor klávesnice a je potřeba dát pozor na nastavený jazyk klávesnice, kterým je v tomto případě ENG. Jak lze pozorovat v tabulce níže, klávesnice s jazykovým nastavením CES vypisuje odlišné znaky, které nechceme kvůli obtížím dalšího zpracování. V tabulce je zapsána vypsaná ukázka hodnoty pro tagové nosiče a karty.

Tabulka 1 Ukázka výpisu kódu podle jazyka klávesnice

	ENG klávesnice	CES klávesnice
Vypsaný kód tagu	4C9BD816	čCíBDá+ž
Vypsaný kód karty	EBB9B822	EBBíBáěě

Modul RFID čtečky s vestavěnou anténou RC522

Druhá čtečka v tomto projektu slouží pro přiložení nosiče a následné zjištění kódu uživatele, který se chce dostat do prostoru. Obsahuje integrovaný obvod MFRC522 s integrovanou anténou. Pro komunikaci čtečky s čipem je využívána technologie s bezdrátovou komunikací NFC (Near field communication). Modul také využívá rozhraní SPI komunikační sběrnice. Čtečka je umístěna v blízkosti vstupu do prostoru. Protože se jedná o čtečku o rozměrech 40 x 60 mm, krabička nemusí mít velké rozměry a usnadňuje její montáž do prostoru vchodu. Pracuje na frekvenci 13,56 MHz, efektivní vzdálenost pro komunikaci je do 3 cm. Potřebné napájení této čtečky je 3,3 V.



Obrázek 10 Modul RFID čtečka s vestavěnou anténou

Modul RC522 má celkově osm pinů pro propojení, ale v této práci je zapotřebí pouze sedm a pin číslo 5, tedy IRQ nepropojujeme. Tyto piny jsou vypsány do tabulky uvedené níže.

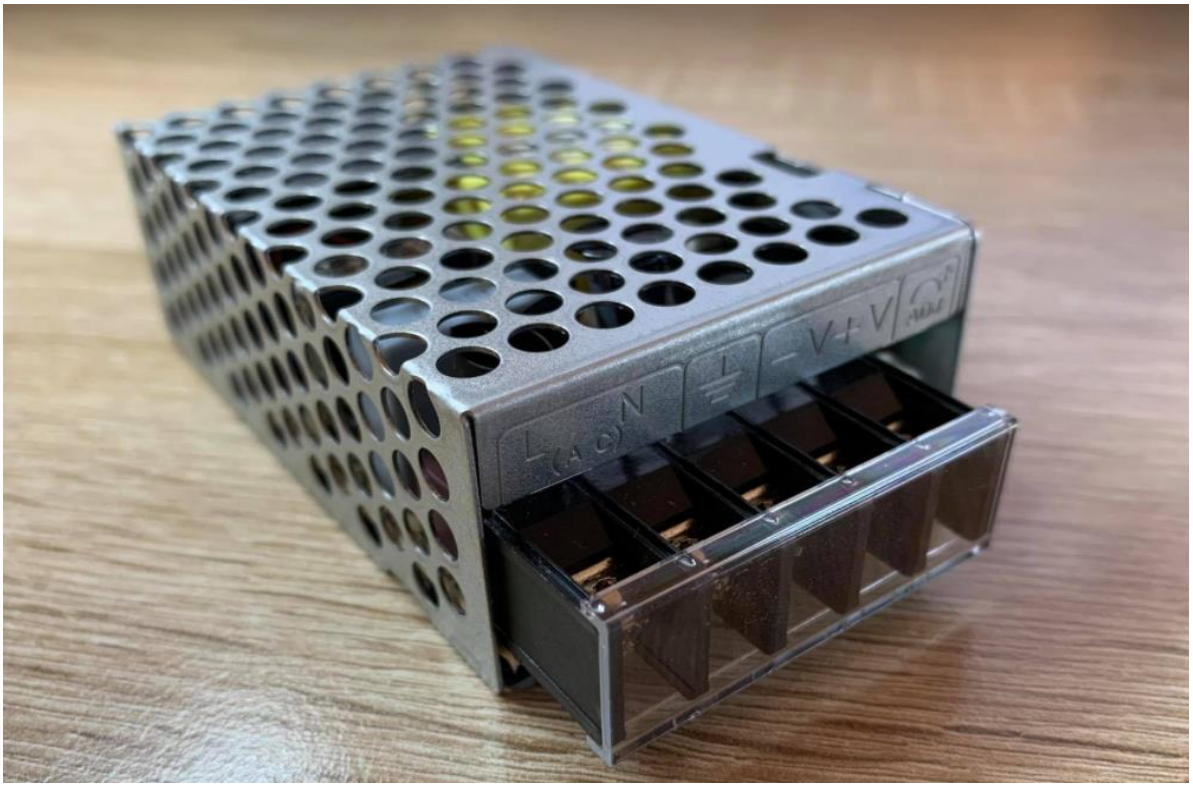
Tabulka 2 Popis jednotlivých pinů

Pin	Popis
1	SDA (synchronous data)
2	SCK (clock)
3	MOSI (master OUT, slave IN)
4	MISO (master IN, slave OUT)

Pin	Popis
5	IRQ (interrupt request)
6	GND (ground)
7	RST (reset)
8	3V3 (napájecí napětí 3.3.V)

Spínaný zdroj

Pro napájení celého projektu slouží spínaný síťový zdroj od výrobce MEAN WELL. Jedná se o zdroj s malými rozměry o velikosti 78 x 51 x 28 mm. Do zdroje je přivedena flexo šňůra s průřezem 3x1 mm^2, ta je připojena k zásuvce, která zajišťuje pro zařízení konstruované napětí ze sítě nízkého napětí. Vybraný zdroj obstarává výstupní napětí 12 V, výstupní proud 2,1 A, skutečný výkon 25,2 W. Obsahuje také integrované ochrany proti přetížení, zkratu a přepětí. Chlazení je pasivní, podle manuálu, není zapotřebí zvláštní údržba, ale je nutné zařídit dobrou cirkulaci vzduchu kvůli dostatečnému chlazení. Je žádoucí dát pozor na čistotu průchodných větracích otvorů.



Obrázek 11 Spínaný zdroj MEAN WELL RS-25-12

LED dioda

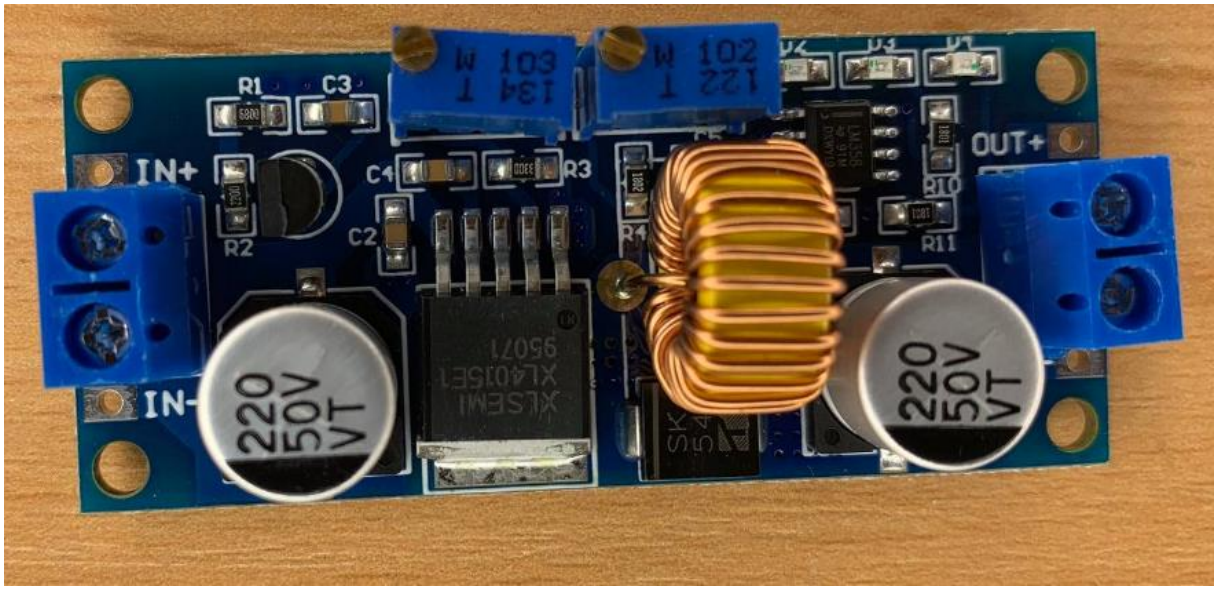
V projektu jsou dvě LED diody a každá z nich má vlastní úkol po přiložení nosiče ke čtečce. Zelená dioda se rozsvítí v moment, kdy byl nosič přijat, zámek se otevře a osoba může vstoupit do prostoru. Červená dioda zase poukazuje na nepřijatý nosič, takže zámek zůstane zamčený a dveře nejdou otevřít.

Bzučák

Systém obsahuje jeden aktivní bzučák, který má dva úkoly lišící se podle přijetí nebo odmítnutí nosiče dat. Správný nosič přijatý systémem osobu zvukově upozorní, po celou dobu bude zvuk bzučáku nepřetržitě doprovázet otevření zámku. Pokud bude nosič dat odmítnut, bzučák osobu zvukově upozorní pomocí dvou pípnutí.

Modul DC/DC měnič step-down

Tento modul slouží k regulaci výstupního napětí v mezi 1,25 - 36 V při maximálním proudu 5 A je potřeba dát pozor na to, aby vstupní napětí bylo minimálně o 1,5V vyšší než výstupní. Využívá první trimr k nastavení výstupního napětí a druhý k proudovému omezení. Je zde i integrovaná tepelná pojistka a protizkratová pojistka. Jsou zde 3 LED pro signalizaci aktivace funkcí. Červená LED značí proudové omezení, modrá LED odebíraný proud a zelená značí že není odebíraný žádný proud. V zapojení pro tuto práci slouží pro regulaci napětí ze spínaného zdroje, které je 12V a reguluje ho na 5V na výstupu. Výstupních 5V slouží pro napájení desky NodeMcu Lua WI-FI ESP8266 a relé modulu.



Obrázek 12 Modul DC/DC měnič step-down

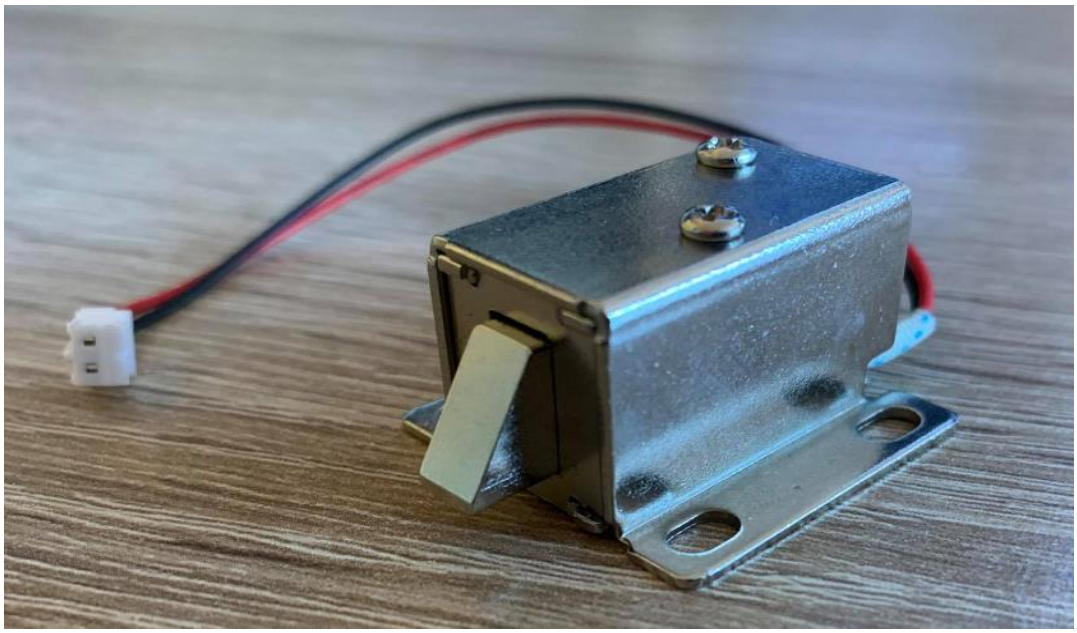
RFID přístupové čipy a karty

Pro autentizaci vstupu jsou zvoleny RFID přístupové čipy různých barev a RFID bílé karty. Mnoho firem zařizuje různé potisky na zakázku, ale zde je vybrán klasický neutrální design, jelikož cena se s potiskem zvedá a navíc, aby nebylo poznat v případě ztráty, kde konkrétně se dá nosič použít. Produkt pracuje na frekvenci 13,56 MHz, nedá se přepisovat a je kompatibilní s NFC (near field communication) technologií, která slouží k bezdrátové komunikaci mezi přístroji.

Obrázek 13 RFID tagy a karty

Elektromagnetický zámek

Jako výstupní periferie je zvolen model elektromagnetického zámku 99-S12 pro dveře. Jedná se o zámek malých rozměrů, který reprezentuje ukázku fyzického otevření za požadovaných podmínek. Pro napájení zámku podle specifikací je zapotřebí napětí 8-12 VDC a spotřeba proudu je 0,6 A. Podle informací prodejce, tento zámek není vhodný pro dlouhodobý stav otevření a doporučený stav otevření by měl maximálně dosahovat 10 s. Při nedodržení pokynu může dojít kvůli přehřátí ke zničení cívky zámku. Západka zámku je bez napájení vysunutá.



Obrázek 14 Zámek

Relé

Pro spínání zámku je zvolené jedno kanálové 5V relé. Relé modul slouží v této práci k vysunutí a zasunutí západky zámku, jelikož tato funkce potřebuje k provozu větší proud a napětí než může modul NodeMcu Lua WI-FI ESP8266 dodat. Zařízení je také vybaveno signalizační LED diodou, která svítí při aktivaci relé.

Obrázek 15 Relé Modul

Tranzistor

Do tohoto projektu bylo zapotřebí přidání tranzistoru BC546B NPN. Z důvodu že vývod desky NodeMcu Lua WI-FI ESP8266 nedokáže dodat takové hodnoty z pinu, jako například Arduino Uno, proto je tranzistor potřeba pro správné pracování relé.

5.2 Použité programy

V následující kapitole jsou popsány využité programy pro tvorbu systému inteligentního zámku.

Apache

Jedná se o softwarový program nainstalovaný na hardwarovém zařízení, které je připojené k internetu, v tomto případě na stolním počítači a zařizuje obsluhu prohlížečů pro zprostředkování internetové stránky. Mezi jeho výhody patří dostupnost pro hlavní platformy jako jsou Windows a Linux, bezplatná dispozice a bezproblémová jednoduchá instalace.

MySQL

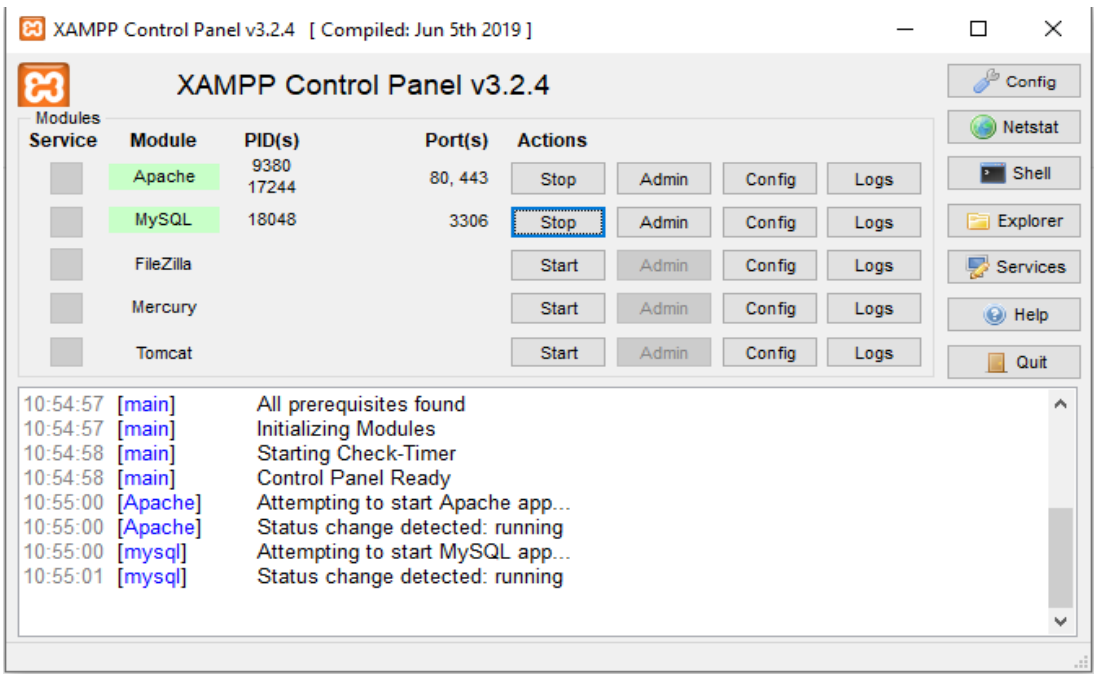
MySQL je databázový server, který komunikuje pomocí SQL jazyku. Pomocí těchto databází lze pracovat s daty různého druhu, kam může zapadat i text a obrázky. Je schopen vytvořit tabulky i s editací nebo mazáním dat. Je podporován všemi hlavními platformami a je k dispozici volně ke stažení.

Myphpadmin

Patří mezi nástroje v jazyce PHP pro jednoduchou správu databází MySQL ve webovém prostředí. V tomto prostředí lze vytvářet a mazat databáze, ale i vytvářet, mazat a upravovat tabulky a využívat SQL příkazy. V Myphpadmin se nachází databáze zákazníků, kterou je možné skrze tento nástroj upravovat.

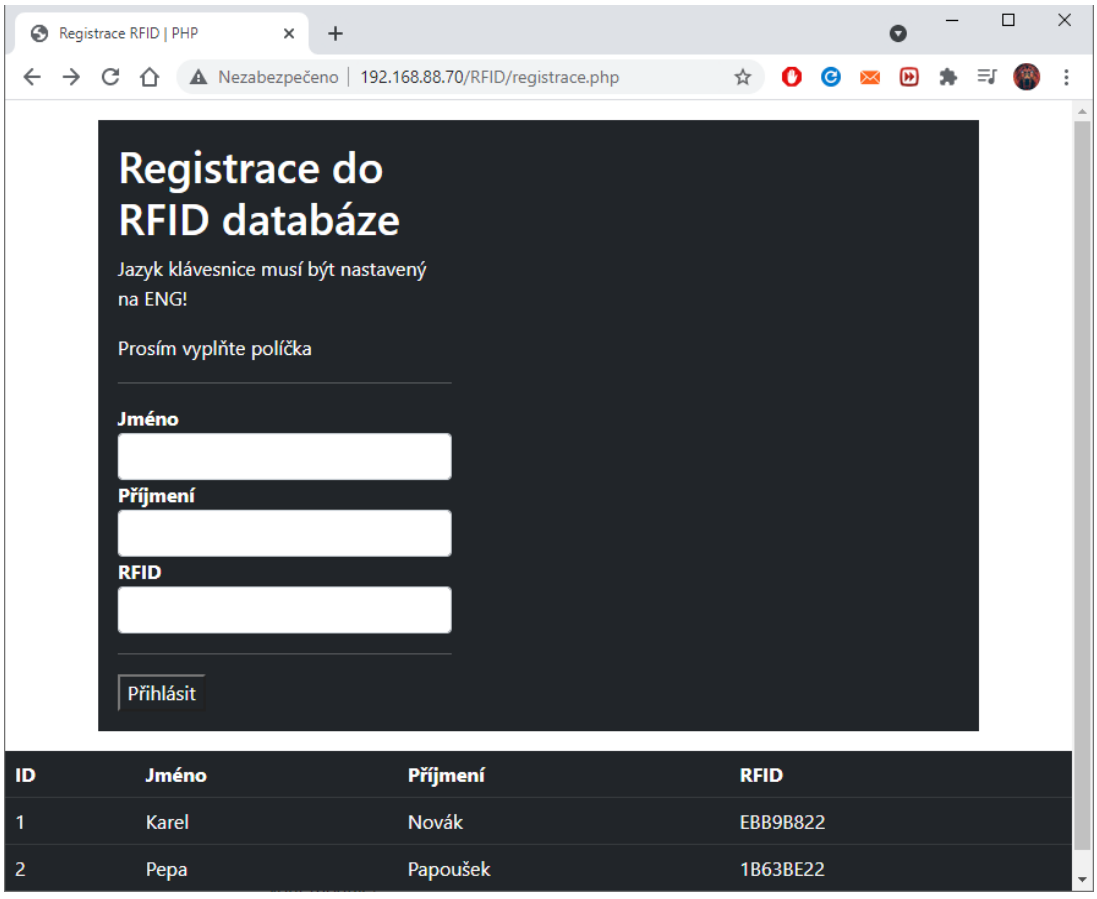
5.3 Princip fungování

Jako první je potřeba zprovoznit Apache a MySQL, pro tento účel je stažen software XAMPP na obrázku číslo 16 Control Panel, kde je ovládací panel pro dobrou správu. Díky ovládacímu panelu je možné spouštět Apache a MySQL, nebo je případně zastavit. Tento program musí být nepřetržitě zapnutý pro správnou funkci zařízení.



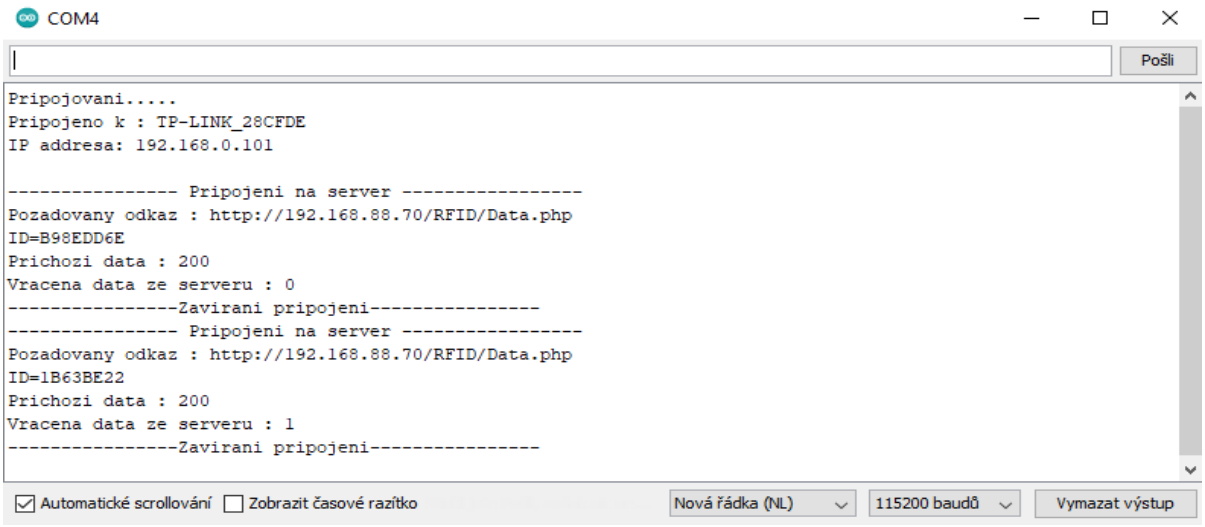
Obrázek 16 Xamp ovládací panel

Jakmile jsou podmínky splněny, tak je v provozu databázový nástroj phpMyAdmin pro správu MySQL databází ve webovém prostředí. V tomto prostředí je spousta možností úprav databáze ať od vytváření, mazání až po provádění SQL příkazů. V tomto prostředí je vytvořena databáze, která je dále propojena s vytvořenou webovou stránkou, která je ukázána na obrázku číslo 17, pomocí programovacího jazyka PHP. V tomto případě je to webová stránka, kde je tabulka vypsaných dat z databáze společně s registrací do databáze. Na obrázku je vidět, že je zde potřeba vyplnit Jméno, Příjmení a RFID. Pro vyplnění RFID poté slouží výše zmíněná čtečka RFID kódů se správně nastaveným formátem výpisu. V případě že jedno z polí není vyplněno, zobrazí se upozornění, že je dané pole potřeba vyplnit. Pokud jsou všechny pole vyplněna, tak se hned po potvrzení tlačítka přihlásit vypíší do daných kolonek a vlevo nahoře se zobrazí upozornění proběhlého uložení. Na stránce je ještě upozornění ohledně nastavení jazyku do ENG pro správnou funkci čtečky. Vypsaná tabulka dále obsahuje kolonku ID, jejímž účelem je větší přehlednost ve správě uživatelů.



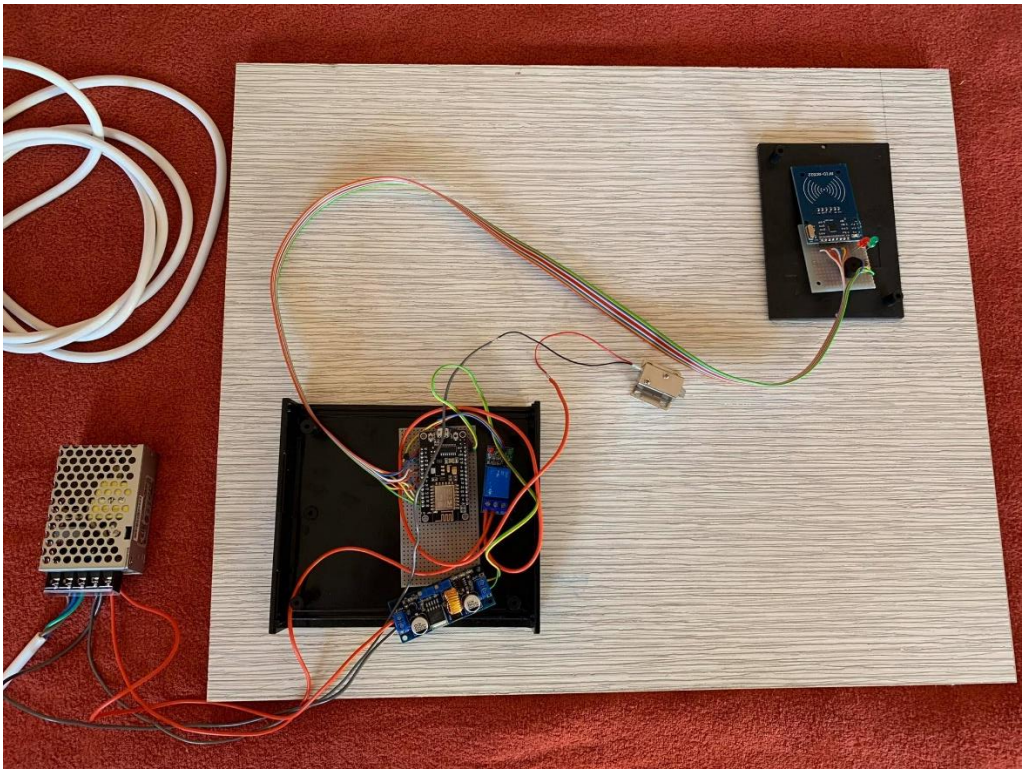
Obrázek 17 Ukázka webové stránky

Pro bezdrátovou komunikaci s tímto systém je zvolen výše zmíněný modul NodeMcu Lua WI-FI ESP8266, který obsahuje program vytvořený z prostředí Arduino IDE. Do tohoto prostředí bylo zapotřebí stáhnout knihovny ať už pro vývojovou desky, tak i další komponenty a jejich správnou funkci celku. V programu jsou zadána potřebná data, jako jméno wi-fi, heslo pro připojení k wi-fi a IP adresa, aby mohlo dojít k propojení s webovou stránkou. Po začátku napájení modulu, se modul snaží připojit k síti a poté co je připojen, vypíše jméno připojené sítě a IP adresu. Jakmile tento proces proběhne, tak čtečka s integrovanou anténou RC 522 která je umístěná v blízkosti přístupového místa je připravena pro přečtení nosiče.



Obrázek 18 Výpis sériového monitoru Arduino IDE

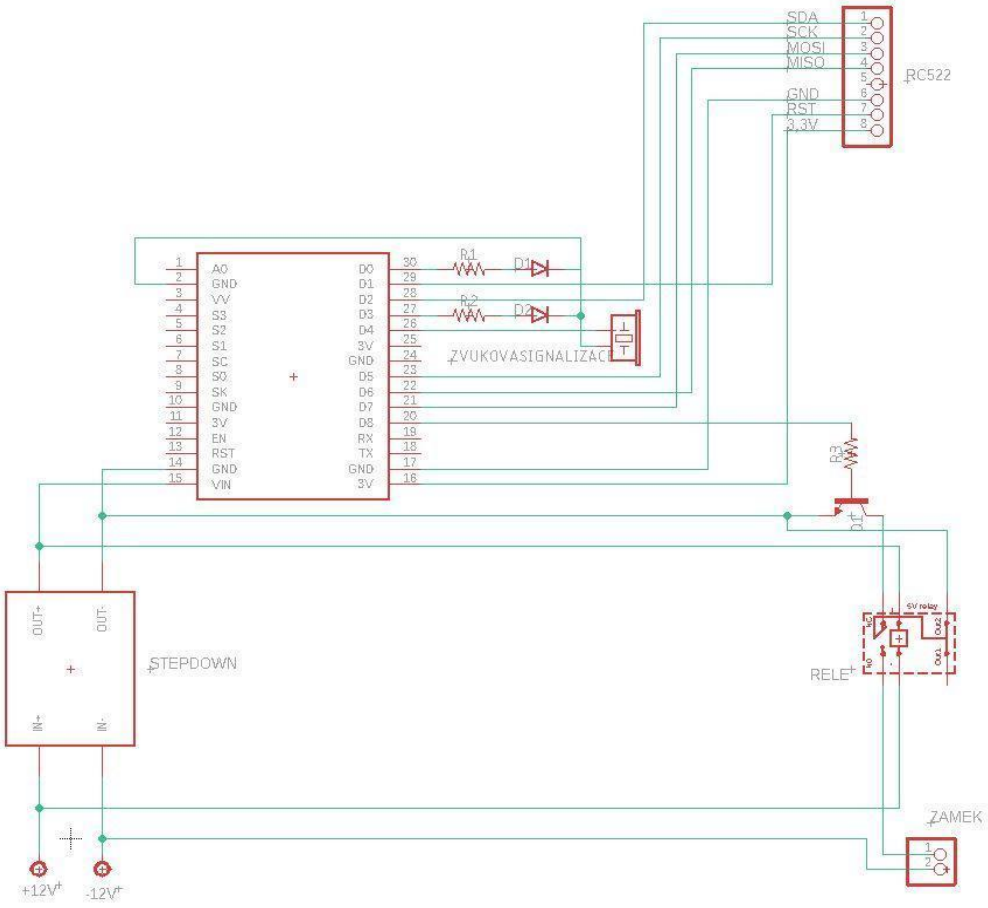
Při přečtení nosiče a zjištění jejího kódu se modul NodeMcu Lua WI-FI ESP8266 dotazuje serveru, zda takový kód je obsažen v databázi. Pokud databáze takový kód neobsahuje, tak modulu vrátí zpět hodnotu „0“, která značí neznámý nosič a podle programu se zámek neotevře, červená LED dioda dvakrát blikne a bzučák udělá dvě zvukové upozornění. V opačném případě pokud je přiložen známý nosič, modulu je vrácena hodnota „1“, rozsvítí se zelená LED dioda, rozezní se zvuková signalizace pomocí bzučáku, zámek se zatáhne a tohle všechno bude trvat po dobu pěti vteřin, pro vstup do prostoru.



Obrázek 19 Model vytvořeného systému

5.4 Schéma zapojení

Na obrázku níže je celé schéma zapojení práce vytvořené v programu Eagle.



Obrázek 20 Schéma zapojení

5.5 Popis kódu webových stránek

Jak bylo zmíněno v kapitole Princip fungování systému, tak bylo za potřebí vytvořit databázi v softwaru phpMyAdmin, která je propojena s webovou stránkou. Toto propojení databáze a vytvoření webové stránky je pomocí jazyku PHP. Pod tento text je přidána ukázka kódu propojení.

```
$db_user = "root";

$db_pass = "";

$db_name = "rfid";

$db = new PDO('mysql:host=localhost;dbname=' . $db_name .
';charset=utf8', $db_user, $db_pass);

$db->setAttribute(PDO::ATTR_ERRMODE,
PDO::ERRMODE_EXCEPTION);
```

V části kódu uvedeným níže je vidět vytvoření registračního formuláře. Ta obsahuje tvorbu nadpisu a doplňkových informací pro zadávání do polí, následně jsou definovány i velikosti jednotlivých polí a jejich název. Poslední příkaz je pro vytvoření tlačítka „Příhlásit,“.

```
<div class="row">

     <div class="col-sm-5">

          <h1>Registrace do RFID databáze</h1>

               <p>Jazyk klávesnice musí být nastavený na ENG!</p>

               <p>Prosím vyplňte políčka</p>

               <hr class="mb-3">

               <label for="Jméno"><b>Jméno</b></label>

               <input class="form-control" id="Jméno" type="text"
name="Jméno" required>

               <label for="Příjmení"><b>Příjmení</b></label>

               <input     class="form-control"     id="Příjmení"
type="text" name="Příjmení" required>

               <label for="RFID"><b>RFID</b></label>

               <input class="form-control" id="RFID"  type="text"
name="RFID" required>

               <hr class="mb-3">

               <input  class="bg-dark  text-white"  type="submit"
id="registrace" name="vytvoř" value="Přihlásit">

     </div>

</div>
```

Poté co bylo tlačítko „Přihlásit“ využito, spustí se další část kódu, která vypisuje data z polí do databáze, za pomocí metody $_POST, která je využívaná k předávání proměnných. Pokud tento proces proběhne správně, tak je na stránce vypsáno „Proběhlo uložení“, v jiném případě bude vypsáno „Něco se pokazilo“

```
if(isset($_POST['vytvoř'])){

          $Jméno    = $_POST['Jméno'];

          $Příjmení = $_POST['Příjmení'];

          $RFID     = $_POST['RFID'];

          $sql = "INSERT INTO uzivatel (Jméno, Příjmení, RFID)
     VALUES(?,?,?)";

          $stmtinsert = $db->prepare($sql);

          $vysledek  =  $stmtinsert->execute([$Jméno,  $Příjmení,
$RFID]);

          if($vysledek) {

               echo'Proběhlo uložení.';

          }

          else 'Něco se pokazilo';}
```

Pro tvorbu a výpis hodnot do tabulky slouží následující část programu. Nejdříve vyčteme hodnoty z takzvaného„table“, který je vytvořen v phpMyAdmin„ pro tuto databázi to je „uživatel“ a poté s nimi pracujeme dále a tvoříme tabulku.

```
$sql = "SELECT * from uzivatel";

     $vysledek2 = $conn-> query($sql);

     if($vysledek2-> num_rows > 0) {

          while($row = $vysledek2->fetch_assoc()) {

               echo     "<tr><td>".     $row["ID"]     ."</td><td>".
$row["Jméno"]     ."</td><td>".     $row["Příjmení"]     ."</td><td>".
$row["RFID"] ."</td></tr>";

          }
```

5.6 Popis kódu uloženém na modelu NodeMcu

Nejdříve je zapotřebí přidat potřebné knihovny pro správnou funkci programu, vytvořit konstanty a proměnné pro jednoduší práci a definovat výstupy.

```
// Knihovny

#include <ESP8266WiFi.h>

#include <WiFiClient.h>

#include <ESP8266HTTPClient.h>

#include <SPI.h>

#include <MFRC522.h>
```

```
//Výstupy

#define SDA_PIN D2  // SDA

#define RST_PIN D1  //  RST

MFRC522  mfrc522(SDA_PIN,  RST_PIN);    //  Vytvoreni
MFRC522

#define LED_na_desce 2

#define LED_zelena D0

#define LED_cervena D3

#define Bzucak D4

#define Zamek D8
```

Ještě předtím, než se modul začne připojovat na zadanou WI-FI, tak v programu proběhne určení sériového přenosu dat, inicializace SPI sběrnice, inicializace MFRC522 čipu a poté se nastaví režim station (STA) pro připojení k WI-FI.

```
Serial.begin(115200);

SPI.begin();

mfrc522.PCD_Init();

delay(500);

WiFi.mode(WIFI_STA);
```

Jakmile je modul připojen k WI-FI, tak je připraven pro čtení nosičů. Zde je ukázka kódu, která ukazuje postup pro čtení a získání ID z nosiče.

```
int prectiKartu() {
  if(!mfrc522.PICC_IsNewCardPresent()) {
    return 0;
  }
  if(!mfrc522.PICC_ReadCardSerial()) {
    return 0;
  }
  for(int i=0;i<4;i++){
    readcard[i]=mfrc522.uid.uidByte[i];    //ukládání   UID
karty/tagu do čtečky
    array_to_string(readcard, 4, str);
    StrUID = str;
  }
  mfrc522.PICC_HaltA();
  return 1;}
```

Pro správnou funkci zpracování dat je zapotřebí převedení přečtených dat array na string a k tomu slouží tato část kódu.

```
void array_to_string(byte array[], unsigned int len, char
buffer[]) {
    for (unsigned int i = 0; i < len; i++)
    {  byte nib1 = (array[i] >> 4) & 0x0F;
        byte nib2 = (array[i] >> 0) & 0x0F;
        buffer[i*2+0] = nib1  < 0xA ? '0' + nib1  : 'A' + nib1
- 0xA;
        buffer[i*2+1] = nib2  < 0xA ? '0' + nib2  : 'A' + nib2
- 0xA;}
```

V poslední části poté zjišťujeme, zda je přečtené ID nosiče uložené v databázi. K tomu slouží deklarace httpclienta a určení kde žádaná data získáme.

```
void htth_zprava(String rfid_id){

  HTTPClient http;

  String adresaPHP, Sql_rfid_id;

  adresaPHP = host + String("RFID/Data.php");

  Sql_rfid_id = "ID=" + rfid_id;

  http.begin(adresaPHP);

  http.addHeader("Content-Type",    "application/x-www-form-
urlencoded");

  int httpCodeGet = http.POST(Sql_rfid_id);

  String informace = http.getString();
```

Tyto informace jsou vyčteny z PHP kódu, který je propojený s naší databázi a slouží pro vyčtení dat z databáze a pro následnou odpověď v podobě 1 nebo 0 zpátky do původního programu v modulu NodeMcu. V původním programu je poté napsaný scénář, pro nosiče uložené v databázi a nosiče neuložené v databázi, podle přijaté hodnoty.

```
if (!empty($_POST)) {

    $id=$_POST["ID"];

    $pdo = Database::connect();

    $pdo->setAttribute(PDO::ATTR_ERRMODE,
PDO::ERRMODE_EXCEPTION);

    $sql = 'SELECT * FROM uzivatel WHERE RFID = ?';

    $q = $pdo->prepare($sql);

    $q->execute(array($id));

    $data = $q->fetch(PDO::FETCH_ASSOC);

    Database::disconnect();

    if($data != null){echo 1; }else{echo 0; }
```

6 Vylepšení do budoucna

Systém, který je vytvořený v rámci této bakalářské práce je funkční, firma jej může v budoucnu rozšířit. Vhodné by bylo rozšíření inteligentního zámku do všech prostor firmy, kdy by bylo možné monitorovat pohyb externích pracovníků, případně dalších osob. Tento krok by umožnil nejen monitoring, ale také možnost nastavení autorizace jednotlivých osob. Tedy například osoba A může mít povolen přístup do objektu 1, ale vstup do objektu 2 bude zakázán, osoba B může mít nastavenou autorizaci opačně. Tedy například zaměstnaný technik bude moci vstoupit do skladu náhradních dílů, ale nebude mu nastavena autorizace pro vstup do kanceláře, u pozice sekretářky by tato autorizace byla opačná.

Mezi další případná opatření do budoucna by se určitě mohlo zařadit přidání druhého systému pro ověření osoby, která se chce dostat do prostoru. Druhým systémem by mohlo být například zadání PIN kódu do klávesnice.

Dalším možný vylepšení by mohlo padnout na vzhled webové stránky a možnosti úprav na ní společně se zlepšením uživatelského prostředí. Vhodné by bylo přidat kolonku, kde by byl vidět čas poslední aktivace systému.

Závěr

V rámci této bakalářské práce jsem se rozhodl věnovat se inteligentnímu zámku pro konkrétní firmu, zhodnotit vhodný typ zařízení a zkonstruovat jej.

Hned na začátku této práce jsou shrnuty poznatky Elektronické kontroly vstupu, jeho historie, architektura a identifikace v rámci systému, následně je část věnovaná systémům s využitím biometrických znaků a systémům založeným na RFID technologii.

Pro výběr správného řešení byla provedena analýza vybraného podniku, stanovena kritéria pro hodnocení výběru systému a byl proveden konečný výběr řešení na základě shrnutých poznatků.

Následuje kapitola návrh řešení systému, kde jsou popsány použité součástky a programy, dále jsou v této kapitole popsány principy fungování systému. V další podkapitole této práce se nachází schéma zapojení systému.

V závěrečné části je uveden popis kódu systému s ukázkou a návrhy na rozšíření systému do budoucna.

Literatura

[1] Wireless Biosensing Using Silver-Enhancement Based Self-Assembled Antennas in Passive Radio Frequency Identification (RFID) Tags - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Illustration-of-the-RFID-tag-integrated-inside-a-package-and-being-interrogated-by-an_fig1_275236749 [accessed 28 Jul, 2021]

[2] DRAHANSKÝ, Martin. Biometric security systems fingerprint recognition technology: Biometrické bezpečnostní systémy technologie rozpoznávání otisků prstů : short version Ph.D. Thesis. [Brno: VUTIUM, 2005]. ISBN 80-214-2969-0.

[3] BURDA, Karel. Základy elektronických zabezpečovacích systémů. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.

[4] Vylepšení zámků motivovala velká loupež [online]. 2019, 11.12.2019 [cit. 2021-7-7]. Dostupné z: https://epochalnisvet.cz/vylepseni-zamku-motivovala-velka-loupez/

[5] DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6.

[6] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

[7] [online]. 3. 2017 [cit. 2021-7-7]. Dostupné z: http://na-dotek.cz/wp-content/uploads/2018/05/casopis-na-dotek-c.-11.pdf

[8] ŠČUREK, Radomír a Daniel MARŠÁLEK. Technologie fyzické ochrany civilního letiště. Brno: Akademické nakladatelství CERM, 2014. ISBN 978-80-7204-862-5.

[9] PAVLÍK, Pavel. Biometrie jako základ současné i budoucí identifikace a autentizace. Kontakt [online]. 2007, 9(2), 427-430 [cit. 2021-7-8]. ISSN 1212-4117. Dostupné z: doi:10.32725/kont.2007.066

[10] RIESEN, Kaspar a Roman SCHMIDT. Online signature verification based on string edit distance. International journal on document analysis and recognition [online]. Berlin/Heidelberg: Springer Berlin Heidelberg, 2019, 22(1), 41-54 [cit. 2021-7-8]. ISSN 1433-2833. Dostupné z: doi:10.1007/s10032-019-00316-1

[11] ORSÁG, Filip. Biometrické bezpečnostní systémy = Biometric security systems: technologické rozpoznávání mluvčích. Brno: University of Technology, 2004, 32 s. ; 21 cm. ISBN 80-214-2771-X

[12] FIALOVÁ, Eva. Bezkontaktní čipy a ochrana soukromí. Praha: Leges, 2016, 230 stran ; 21 cm. ISBN 978-80-7502-150-2.

[13] KLAUZ, Milan. Jaký je rozdíl mezi aktivním a pasivním RFID? DPS: Elektronika od A do Z [online]. 2017, 2017(5) [cit. 2021-6-20]. Dostupné z: https://www.dps-az.cz/vyvoj/id:53208/jaky-je-rozdil-mezi-aktivnim-a-pasivnim-rfid-

[14] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. : il. ; 24 cm. ISBN 978-80-247-2365-5

[15] MATYÁŠ, Vašek a Jan KRHOVJÁK. Autorizace elektronických transakcí a autentizace dat i uživatelů. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.

Příloha

Zdrojové kódy jsou nahrány na univerzitní portál STAG.