

ŽILINSKÁ UNIVERZITA V ŽILINE

**FAKULTA ELEKTROTECHNIKY
A INFORMAČNÝCH TECHNOLOGIÍ**

Katedra multimédií a informačno-komunikačných technológií

28260120241020

KAMEROVÝ MONITOROVACÍ SYSTÉM S VYUŽITÍM IOT

2024

Ľuboš Prekop



ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta elektrotechniky
a informačných technológií

**Katedra multimédií a informačno-komunikačných
technológií**

KAMEROVÝ MONITOROVACÍ SYSTÉM S VYUŽITÍM IOT

BAKALÁRSKA PRÁCA

Študijný odbor:	informatika
Študijný program:	komunikačné a informačné technológie
Vedúci bakalárskej práce:	Jarinová Darina, Ing. PhD.
Pracovisko vedúceho práce:	Katedra multimédií a informačno-komunikačných technológií, 010 26 Žilina, Univerzitná 1, 010 08 Žilina

Žilina, 2024

Ľuboš Prekop



ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta elektrotechniky
a informačných technológií

Katedra multimédií
a informačno-komunikačných technológií



Akademický rok 2023/2024

ZADANIE BAKALÁRSKEJ PRÁCE

Meno, priezvisko: **Luboš Prekop**

Študijný odbor: **informatika**
Študijný program: **komunikačné a informačné technológie**

Téma bakalárskej práce: **Kamerový monitorovací systém s využitím IoT**

Pokyny na vypracovanie bakalárskej práce:

1. Stručný prehľad IoT technológií a ich aplikačných možností.
2. Návrh HW riešenia pre monitorovací systém na platforme ESP32.
3. Funkcionality systému budú konzultované s vedúcou práce.
4. Návrh a SW realizácia používateľského rozhrania.
5. Realizácia a vyhodnotenie funkčnosti navrhnutého systému.

Vedúci bakalárskej práce: Jarinová Darina, Ing. PhD., Katedra multimédií a informačno-komunikačných technológií, FEIT, Žilinská univerzita v Žiline

Dátum odovzdania bakalárskej práce: 13. 05. 2024

ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA ELEKTROTECHNIKY
A INFORMAČNÝCH TECHNOLOGIÍ
KATEDRA MULTIMÉDIÍ A INFORMAČNO-
KOMUNIKAČNÝCH TECHNOLOGIÍ
Univerzitná 8215/1, 010 26 Žilina

prof. Ing. Róbert Hudec, PhD.
vedúci katedry

V Žiline dňa 31. 10. 2023

ANOTAČNÝ ZÁZNAM

Žilinská univerzita v Žiline

Fakulta elektrotechniky a informačných technológií

Katedra multimédií a informačno-komunikačných technológií

Typ práce:	Bakalárska práca
Meno a priezvisko:	Ľuboš Prekop
Akademický rok:	2023/2024
Názov práce:	Kamerový monitorovací systém s využitím IoT
Počet strán:	36
Počet obrázkov:	25
Počet tabuliek:	2
Počet grafov:	0
Počet príloh:	0
Počet použ. lit.:	32

Anotácia v slovenskom jazyku:

Práca sa zameriava na implementáciu monitorovacieho systému s využitím internetu vecí (IoT), konkrétne na navrhnutie a implementáciu dochádzkového systému s použitím biometrických metód na zaznamenávanie príchodov a odchodov zamestnancov. Obsahuje podrobný opis architektúry systému a procesu implementácie softvéru na správu kamery a snímača odtlačkov prstov. Okrem toho sleduje aj pohyb v definovaných priestoroch a poskytuje služby na archiváciu fotografií a zasielanie bezpečnostných upozornení. Výsledky tejto práce môžu prispieť k rozvoju a využitiu IoT pre efektívne monitorovanie dochádzky a zlepšenie bezpečnosti pracovného prostredia

Annotation in foreign language (english/deutsch):

The thesis focuses on the implementation of a monitoring system using the Internet of Things (IoT), specifically the design and implementation of an attendance system using biometric methods to record employee arrivals and departures. It includes a detailed description of the system architecture and the process of implementing the camera and fingerprint scanner management software. In addition, it also monitors movement in defined areas and provides services for archiving photographs and sending security alerts. The results of this work can contribute to the development and use of IoT for effective attendance monitoring and improving the security of the work environment

Kľúčové slová:	IoT, monitorovací systém, ESP32, kamera, odtlačok prsta, FaceNet
Vedúci bakalárskej práce:	Jarinová Darina, Ing. PhD.
Dátum odovzdania ZP:	13.5.2024

POĎAKOVANIE

Chcel by som sa úprimne poďakovať vedúcemu práce, Jarinová Darina, Ing. PhD., za neoceniteľnú podporu, odborné rady a cenné vedenie počas celej prípravy a realizácie mojej bakalárskej práce.

ABSTRAKT

Abstrakt v slovenskom jazyku

Bakalárska práca sa zaoberá implementáciou monitorovacieho systému. Presnejšie ide o návrh a implementáciu IoT dochádzkového systému využívajúceho biometrické metódy na zaznamenávanie príchodov a odchodov zamestnancov. Podrobne sme predstavili architektúru systému a proces implementácie softvéru na správu kamery a senzora odtlačku prsta. Tieto kroky viedli k vytvoreniu komplexného dochádzkového systému, ktorý umožňuje jednoduché prihlásenie zamestnancov pomocou biometrických údajov. Okrem toho sme sa venovali aj monitorovaniu pohybu v určenom priestore a implementácii služieb pre archiváciu fotografií a odosielanie upozornení pri narušení bezpečnosti. Výsledky tejto práce môžu prispieť k rozvoju a využitiu IoT, kde sa zabezpečuje jednoduché a efektívne používanie aplikácie zamestnancom a minimalizuje riziko chýb v procese sledovania dochádzky. Monitorovanie pohybu v určených priestoroch môže prispieť k zvýšeniu efektivity, bezpečnosti v pracovnom prostredí.

Kľúčové slová: IoT, monitorovací systém, ESP32, kamera, odtlačok prsta, FaceNet,

Abstract in foreign language (english)

Our bachelor's thesis deals with a particular aspect of the use of IoT - the design and implementation of a monitoring system. More specifically, it is the design and implementation of an IoT attendance system using biometric methods to record the arrivals and departures of employees. We have presented in detail the system architecture and the implementation process of the camera and fingerprint sensor management software. These steps led to the creation of a comprehensive attendance system that allows easy employee login using biometric data. In addition, we also worked on monitoring movement in the designated area and implementing services for archiving photos and sending alerts when security breaches occur. The results of this work can contribute to the development and use of IoT, where the simple and efficient use of the application by employees is ensured and the risk of errors in the attendance tracking process is minimized. Monitoring movement in designated areas can contribute to increasing efficiency and safety in the work environment.

Keywords: IoT, monitoring System, ESP32, camera, fingerprint, FaceNet,

OBSAH

Anotačný záznam.....	i
PodĎakovanie	ii
Abstrakt.....	iii
Abstrakt v slovenskom jazyku	iii
Abstract in foreign language (english).....	iii
Obsah	iv
Zoznam obrázkov a tabuliek.....	v
Zoznam skratiek.....	vi
Úvod.....	1
1 Internet vecí	3
1.1 IoT architektúra a komponenty	4
1.2 Aplikačné možnosti	7
1.3 IoT konektivita	11
2 Navrh hardvérového riešenia s využitím biometrických metód pre monitorovací systém	17
2.1.1 Hardvérové zapojenie dochádzkového systému.....	19
2.1.2 FaceNet.....	20
3 Softvérová realizácia monitorovacieho systému	22
3.1.1 Registrácia užívateľa	23
3.1.2 Extrakcia údajov a evidencia do databázy.....	26
3.1.3 Prihlásenie užívateľa do dochádzkového systému	27
4 Monitorovanie pohybu v priestore pomocou IoT bezpečnostného systému	31
5 Výsledky práce a diskusia.....	33
Záver	36

ZOZNAM OBRÁZKOV A TABULIEK

Obr. 1: Očakávaný nárast IoT technológie [3].....	3
Obr. 2: IoT architektúra – jednotlivé bloky	4
Obr. 3: Oblasť využitia IoT	7
Obr. 4: Hviezdicová topológia [16] Obr. 5: Mesh topológia [17]	11
Obr. 6: Porovnanie rôznych typov IoT sietí a ich aplikačné možnosti [18].....	12
Obr. 7: ESP32 PSRAM Timer Camera X [29].....	17
Obr. 8: Senzor AS608 [30]	18
Obr. 9: Hardvérové zapojenie kamery X a senzoru odtlačku prsta	19
Obr. 10: Architektúra modelu Facenet [31]	20
Obr. 11: Trojitá strata a učenie [31]	21
Obr. 12: MJPEG streamu s rozlíšením 800x600 vo webovom prehliadači	22
Obr. 13: Bloková schéma softvérovej realizácie dochádzkového systému	23
Obr. 14: Aplikácia pre registráciu zamestnanca.....	23
Obr. 15: Priečink zamestnanca po registrácii	24
Obr. 16: Neoptimálne umiestnenie tváre – červený obdĺžnik	25
Obr. 17: Proces registrácie odtlačku prsta	25
Obr. 18: Konceptuálna schéma dochádzkového systému	26
Obr. 19: Neúspešné prihlásenie do systému	27
Obr. 20: Úspešné prihlásenie zamestnanca do dochádzkového systému	28
Obr. 21: Zobrazenie dochádzky zamestnanca.....	29
Obr. 22: Vývojový diagram dochádzkového systému pre detekciu tváre	29
Obr. 23: Hardvérové zapojenie IoT bezpečnostného systému.....	31
Obr. 24: Zachytené fotografie v Google Drive.....	32
Obr. 25: Upozornenie prostredníctvom mailu	32

Zoznam tabuliek

Tabuľka 1: Detekcia rýchlosti pre rôzne rozlíšenia obrazu.....	33
Tabuľka 2: Testovanie detekcie pri rôznej prahovej hodnote	34

ZOZNAM SKRATIEK

Skratka	Anglický význam	Slovenský význam
IoT	Internet of Things	Internet vecí
AI	Artificial intelligence	Umelá inteligencia
M2M	Machine to machine	Komunikácia medzi zariadeniami
AP	Access Point	Prístupový bod
BLER	Block Error Rate	Bloková chybovosť
LTE	Long Term Evolution	LTE – dlhodobá evolúcia
mmWave	Millimeter waves	Milimetrové vlny
mMIMO	Multiple inputs and outputs	Viacnásobné vstupy a výstupy
LTE-M	LTE for Machines	LTE pre zariadenia
NB-IoT	Narrowband-IoT	Úzkopásmový internet vecí NB-IoT
LPWAN	Low-power wide-area network	Rozľahlá sieť s nízkym výkonom
UNB	Ultra Narrowband	Ultra úzkopásmové
BLE	Bluetooth Low Energy	Bluetooth s nižšou spotrebou energie
RX	Receive	Prijímať
TX	Transmit	Vysielat'
CNN	Convolutional neural network	konvolučnú neurónovú sieť (CNN)
API	Application programming interface	Aplikačné programovacie rozhranie API
FPS	Frames per seconds	Obrazová frekvencia
SMTP	Simple Mail Transfer Protocol	Jednoduchý protokol na prenos pošty
RTOS	Real-Time Operating System	Jednotky spracovania v reálnom čase

ÚVOD

V súčasnej dobe technologický pokrok prináša otvorené možnosti a výzvy na zlepšenie efektívnosti a bezpečnosti v rôznych oblastiach života. Rozvoj internetu vecí (IoT) nám umožňuje vytvoriť prepojené a inteligentné prostredie, kde môžeme monitorovať a riadiť rôzne aspekty nášho života. IoT nám poskytuje schopnosť sledovať fyzické a virtuálne systémy prostredníctvom senzorov a zariadení, ktoré zhromažďujú dáta a umožňujú nám ich analyzovať a využívať na zlepšenie procesov.

V tejto práci sa zameriavame návrhom a implementáciou monitorovacieho systému. Konkrétne ide o IoT dochádzkový systém, ktorý využíva biometrické metódy na presné zaznamenávanie príchodov a odchodov zamestnancov.

V prvej kapitole podrobne skúmame technológie IoT a ich aplikačné možnosti v rôznych oblastiach života. Zameriavame sa na komunikačné technológie v rámci IoT prostredia, ktoré umožňujú zariadeniam v IoT sieti komunikovať medzi sebou a vymieňať si údaje. Preskúmali sme ich využitie pre spoľahlivú a efektívnu komunikáciu medzi senzormi, aktuátormi a ďalšími zariadeniami v IoT systéme.

V druhej kapitole predstavujeme komplexnú architektúru systému, ktorá zahŕňa hardvérové komponenty ako je kamera ESP 32 Timer Camera X a senzor odtlačkov prstov AS608. Popisujeme ich správne zapojenie do systému a ich vlastnosti a funkcie. Taktiež predstavujeme implementáciu algoritmu FaceNet pre rozpoznávanie tvári.

Tretia kapitola sa zaoberá implementáciou softvéru pre správu kamery a senzoru odtlačku prsta. Popisujeme jednotlivé kroky dochádzkového systému ako je registrácia užívateľa, extrakcia údajov a evidencia do databázy, prihlásenie užívateľa do dochádzkového systému. Tieto kroky vedú k vytvoreniu komplexného dochádzkového systému, ktorý umožňuje registrovaným používateľom jednoduché prihlásenie pomocou biometrie tváre alebo odtlačku prsta.

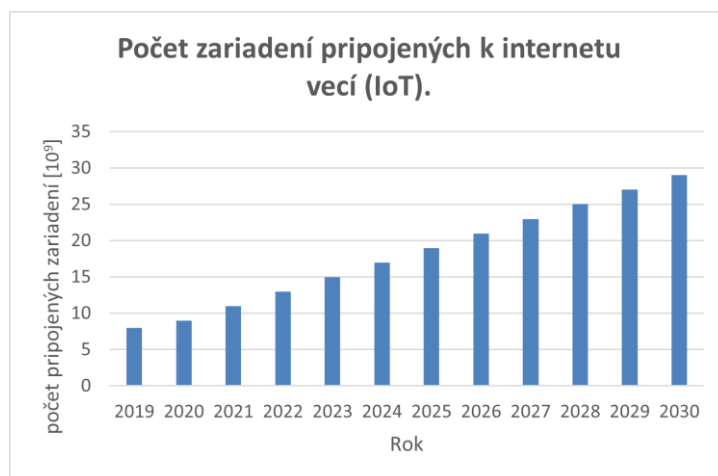
Štvrtá kapitola sa zaoberá monitorovaním pohybu v určenom priestore. V kapitole je opísaná implementácia tohto systému vrátane zapojenia hardvéru až po využitie služieb Google Drive a SMTP pre archiváciu fotografií a odosielanie upozornení pri narušení bezpečnosti.

V poslednej kapitole sa venujeme výsledkom implementácie komplexného IoT dochádzkového systému. Poukazujeme na potenciál tohto systému a rôzne výzvy, s ktorými sme sa stretli, a poskytujeme odporúčania na zlepšenie jeho efektivity.

1 INTERNET VECÍ

Internet vecí (IoT) začal ako vízia fyzických objektov, ktoré sú zabudované senzormi, softvérom a inými technológiami, ktoré sú prepojené a fungujú inteligentným spôsobom. Prvá zmienka o IoT bola publikovaná v roku 2002 [1]. Autor Schoenberger navrhol aplikáciu IoT v obchodoch a uviedol: „Obchody majú oči, teraz dostávajú mozgy. Bezdrôtové čipy budú sledovať všetko, čo nosíte a kupujete“ [1]. Víziou technológie IoT je prijímanie a vymieňanie dát v reálnom čase. Dáta sa analyzujú pomocou rôznych analyzačných metód. Inteligentné služby sa aplikujú v rôznych kontextoch, ako je sledovanie objektov, úspora energie a mnoho ďalších kontextov. Táto vízia sa v priebehu rokov rýchlo vyvíjala, kde bolo navrhnutých, testovaných mnoho technológií v rôznych prostrediach. V súčasnosti je možné dosiahnuť bezproblémovú komunikáciu medzi ľuďmi, procesmi a predmetmi vďaka schopnosti pripájať každodenné objekty k digitálnemu svetu. V jednoduchosti, fyzický svet komunikuje s digitálnym svetom a navzájom spolupracujú [2].

Do konca roku 2024 sa predpokladá, že do celosvetovej siete IoT, bude pripojených viac ako 17 miliárd zariadení. Na tento trend si postupne zvykáme na väčšiu rozmanitosť nositeľných zariadení a každodenných pripojených produktov. Podľa analýzy bude do roku 2030 pravdepodobne pripojených viac ako 30 miliárd zariadení IoT [3].



Obr. 1: Očakávaný nárast IoT technológie [3]

IoT motivuje podniky k transformácii na digitálne podniky vďaka ktorým sa vytvárajú nové obchodné modely, zvýšenie efektivity a možnosti vytvárania dodatočných zdrojov príjmov. Vzájomne prepojené prostredia zvýšia konkurencieschopnosť a uľahčia ľuďom každodenný život.

1.1 IoT architektúra a komponenty

Architektúra internetu vecí pozostáva z niekoľkých blokov. Na obr. 2 je znázornené, ako sú jednotlivé komponenty IoT navzájom prepojené a spolu tvoria škálovateľný a kompatibilný systém. Jednotlivé funkcie blokov sú vysvetlené nasledovne:



Obr. 2: IoT architektúra – jednotlivé bloky

Senzory a aktuátory

Senzory sú pripojené k fyzickým zariadeniam v sieti IoT. Senzory detegujú udalosti a zmeny v prostredí a túto informáciu sprostredkujú zariadeniam. Senzor môže byť aj prevodník, ktorý spracúva jednu formu energie na iný typ. Napríklad premena vibračnej energie na elektrickú.

Aktuátory sú zariadenia, ktoré vykonávajú opačnú činnosť ako snímače. Aktuátory sa používajú na premenu elektrickej energie na príslušajúcu fyzikálnu aktivitu (pohyb, tlak). V systéme IoT sú informácie zaznamenávané senzorom a následne poslané do riadiaceho centra, a na základe rozhodnutia sa výsledok pošle aktuátorovi.

Zariadenia

Zariadenia predstavujú fyzické objekty, ktoré majú schopnosť zbierať údaje zo senzorov a komunikujú s inými objektami. Týmto objektami môžu byť napríklad výrobné stroje, vozidlá, inteligentné domy, chladničky atď. Senzory nemusia byť vždy pripojené k týmto objektom.

Brány

Brány sa používajú na zabezpečenie prepojenia medzi cloudom a zariadeniami spojenými s IoT. Údaje vytvorené zariadeniami sa musia odosielať do cloudu a zase naopak cloud do vecí. Brány umožňujú predbežné filtrovanie údajov pred ich prenosom do cloudu. Cloud posiela riadiace príkazy do zariadení prostredníctvom brány. Tieto príkazy následne vykonávajú aktuátory.

Cloudové brány

Údaje pri komunikácii medzi bránami a cloudovým serverom musia byť komprimované a šifrované. Cloudová brána zaručuje komunikáciu a podporuje šifrovanie a kompresiu údajov. Tiež zabezpečuje kompatibilitu medzi rôznymi protokolmi podporovanými bránami.

Úložisko dát

Úložisko dát uchováva informácie tak, ako boli pôvodne generované zariadeniami, bez toho, aby ich menilo do iného formátu. Keď sa vyžaduje predbežné spracovanie a filtrovanie údajov, možno ho získať z úložiska dát. Okrem toho sú dátové úložiská zodpovedné aj za ukladanie dodatočných podrobností o senzoroch a zariadeniach, ako je umiestnenie nainštalovaných senzorov, ovládanie aplikácií a odosielanie príkazov jednotlivými zariadeniami.

Analýza údajov

Analýza údajov umožňuje využívať informácie uložené v databázach na identifikáciu súčasných trendov a hľadanie praktických riešení. Tieto dáta môžu odhaliť vzťahy a vzory, ktoré sú následne využívané na vytváranie užitočných algoritmov a kategorizačných aplikácií. V súvislosti s digitálnou transformáciou, strojové učenie poskytuje moderný nástroj na vytváranie efektívnejších a presnejších modelov. Tieto modely umožňujú vytváranie inteligentných systémov, schopných prispôbovať sa meniacim sa podmienkam prostredia na základe spracovaných údajov z analýzy.

Riadiace aplikácie

Riadiace aplikácie automaticky dávajú pokyny a upozornenia aktuátorom. Napr. v prípade inteligentného domu pri otváraní alebo zatváraní okien sú závislé na predpovedi počasia. Zariadenia v rôznych prostrediach môžu byť pripojené k systému IoT, aby boli nepretržite monitorované senzormi a v prípade situácií odrážajúcich riziko porúch je možné posielat' notifikačné správy technikom.

1.2 Aplikačné možnosti

V dnešnej dobe sa dáta stali kľúčovým zdrojom, ktorý umožňuje nové prístupy v oblasti technológií a digitalizácie. Inovácie založené na internetových technológiách, digitalizácii a perspektívach budúcnosti menia spôsob, akým chápeme aplikácie IoT. Tieto trendy neovplyvňujú iba širšiu koncepciu digitalizácie, ale tiež ponúkajú nové možnosti využitia dát a technológií pre aplikácie IoT.

V oblasti umelej inteligencie (AI) a v neurónových sieťach nastala zmena v spracovaní dát v zariadeniach IoT. Tieto pokroky robia zariadenia nielen jednoduchšími na používanie, ale aj cenovo dostupnejšími, čo umožňuje ich širšie využitie v domácnostiach [2].

Internet vecí (IoT) predstavuje revolúciu v spôsobe, akým interagujeme s technológiami a našim okolím. Doprava, inteligentné siete, inteligentné domy, zdravotná starostlivosť, priemysel, poľnohospodárstvo sú príklady základných koncepcií založených na IoT. Oblasť využitia IoT sú znázornené na obr. 3 [4].



Obr. 3: Oblasť využitia IoT

Inteligentná doprava

IoT predstavuje jednu z kľúčových úloh v inovačnom rozvoji dopravy a logistiky. Inteligentné dopravné systémy pomáhajú dopravným orgánom pri riešení strategických výziev, ako je nedostatočná infraštruktúra, cenové obmedzenia, zvyšujúce sa emisie a rastúce potreby zákazníkov [5]. Základnými komponentmi inteligentnej dopravy sú inteligentné a prepojené produkty. Ako sú napr. vozidlá, snímače a inteligentné prepojené miesta, ktoré spoluvytvárajú inteligentnú infraštruktúru. Inteligentná doprava zahŕňa celý rad technológií. Inteligentné semaforey, výrazne zrýchľujú premávku a znižujú riziko vzniku dopravnej zápch [6]. Ďalej automobily vybavené anténou, ktorá obojsmerne prijíma aj vysiela dáta, umožňuje vozidlu komunikovať so zariadeniami infraštruktúry.

Okrem zmieňovaných prvkoch by sa nemala prehliadnuť taktiež bezpečnosť na cestách. Prostredníctvom pokročilých senzoroch a kamier, sa dokážu identifikovať nebezpečenstvá a zabrániť k vzniku dopravnej nehody. Inteligentná doprava má potenciál znížiť emisie skleníkových plynov, prostredníctvom lepšieho plánovania trás a efektívnejšieho využívania paliva [4].

Inteligentné siete

Technológie IoT sa zaoberajú na úrovni výroby integráciou niekoľkých energetických zdrojov, ako sú ropa, plyn, uhlie, jadrová energia, vodná energia, solárna energia a obnoviteľné zdroje.

Inteligentná sieť je tvorená miliónmi komponentov - od ovládacích prvkov, cez počítače a elektrické vedenia, až po nové technológie a zariadenia, ktoré spolu tvoria dynamický a adaptívny systém schopný reagovať na meniace sa potreby a podmienky [7].

Inteligentné domy

Inteligentný dom je považovaný za jednu z najbežnejších aplikácií internetu vecí, kde domáce spotrebiče alebo zariadenia sa môžu monitorovať a ovládať na diaľku napr. cez smartfón. Dôležitou charakteristikou inteligentného domu je automatizácia. Inteligentná domácnosť môže využívať kombináciu bezdrôtovej a káblovej technológie, aby mohla efektívne fungovať. Inteligentná domácnosť predstavuje ovládanie kúrenia, klimatizácie,

zavlažovanie, osvetlenie, multimédia a rôzne iné procesy. Možnosti sú prakticky neobmedzené závisia od potreby prostredia a aktivít obyvateľov domu [8].

Zdravotná starostlivosť

Možnosti IoT v systémoch zdravotnej starostlivosti sa venuje čoraz viac výskumníkov a organizácií [9, 10]. Zdravotná starostlivosť sa rozšírila kvôli pandémie COVID-19 do oblasti IoT a otvorila nové možnosti v zdravotníctve. Pandémia viedla k rýchlemu prijatiu týchto technológií aby došlo k minimálnemu kontaktu ľudí.

Zariadenia s podporou internetu vecí umožňujú vzdialené monitorovanie hladiny kyslíku a cukru v krvi, EKG a ďalšie iné. IoT zariadenia zhromažďujú údaje o pacientoch pomocou senzorov, kamier a ďalších technológií. Nositeľné zariadenia ako inteligentné hodinky, náramky, umožňujú používateľom sledovať svoj zdravotný stav v reálnom čase. IoT je dôležitým nástrojom pre zdravotníckych pracovníkov na poskytovanie lepšej starostlivosti o pacientov [11, 12].

Priemysel

Priemysel 4.0 je skvelý príklad ktorý sa zavádza do priemyselných prostredí IoT. Koncept súvisí s modulárnou štruktúrou, ktorá využíva fyzické a virtuálne systémy monitorujúce priemyselné procesy, zamerané na neustále zlepšovanie rôznych ukazovateľov výkonnosti v rámci procesu. Dochádza k veľkému rozsahu pridávania senzorov, ktoré komunikujú cez internet, alebo medzi zariadeniami (M2M). V rámci IoT fyzické a virtuálne systémy komunikujú a spolupracujú v reálnom čase medzi sebou a ľuďmi. Firmy a podniky sa stavajú tzv. „smart“. Priemysel využíva technológie ako sú robotika, digitálne dvojčatá, rozšírená realita a mnoho ďalších technológií. Priemysel si vyžaduje vysoko kvalifikovaný personál a potrebu šandardizácie [13].

Inteligentné poľnohospodárstvo

Inteligentné poľnohospodárstvo tiež profituje z implementácie technológie založenej na IoT. Zariadenia IoT sa zameriavajú na monitorovanie zavlažovania, chemické ošetrovanie rastlín, hnojenie, monitorovanie kŕmenia, atď. Monitorovanie rastu plodín pomocou zariadení internetu vecí pomáha farmárom analyzovať riziká a zmeny na základe kvality, charakteristík rastlín, a environmentálnych faktorov. To umožňuje lepši výber semien a predpovedanie chorôb, čo umožňuje včasné opatrenia v intelligentnom

poľnohospodárstve. Využívanie dronov a senzorov s využitím umelej inteligencie vyžaduje úzku spoluprácu týchto častí pre presné a kvalitné poľnohospodárstvo. Centrálny modul spracováva údaje z týchto senzorov v reálnom čase. Táto možnosť umožňuje poľnohospodárom včasnú diagnostiku, čo v konečnom dôsledku umožňuje presnejšie a cielenejšie používanie prípravkov na ochranu rastlín. Aj keď poľnohospodárske systémy založené na IoT spotrebúvajú veľké množstvo energie, udržateľnosť ich nasadenia vyžaduje vyvážené zohľadnenie energetických a environmentálnych faktorov [14].

1.3 IoT konektivita

IoT konektivitu môžeme kategorizovať na základe technológie bezdrôtového pripojenia IoT, rozsahu pokrytia, spotrebu energie a rôznych typov technológií s rôznymi špecifikáciami. Pri konektivite sú dôležité aj technické výzvy existujúcich technológií v oblasti masívneho pripojenia k internetu vecí. Pri výbere vhodnej technológie pre IoT zariadenia je kľúčové zohľadniť technické prekážky súčasných pripojení a zvoliť riešenie, ktoré tieto výzvy najefektívnejšie adresuje.

Topológia

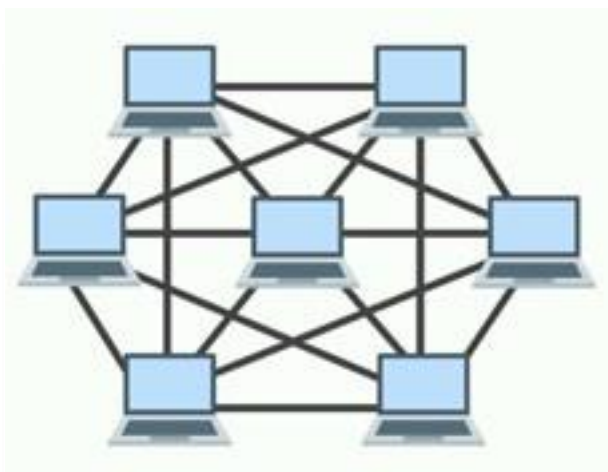
Spôsob, akým sú uzly v sieti usporiadané a navzájom prepojené, sa nazýva topológia. Dve populárne topológie používané v IoT sú hviezdicové a mesh topológie.

V prípade hviezdicovej topológie sú uzly v sieti pripojené k centrálnemu uzlu, ktorý sa používa ako vstupná brána [15]. Technológia Wi-Fi, BLE, ZigBee je príkladom hviezdicovej topológie, kde centrálny uzol je AP (prístupový bod) a všetky ostatné uzly sa nazývajú stanice. Uzly sa môžu pripojiť k inému uzlu prostredníctvom centrálného uzla.

V topológii mesh môže byť vstupnou bránou jeden alebo viacero uzlov. Topológia v ktorej sú všetky uzly navzájom prepojené.



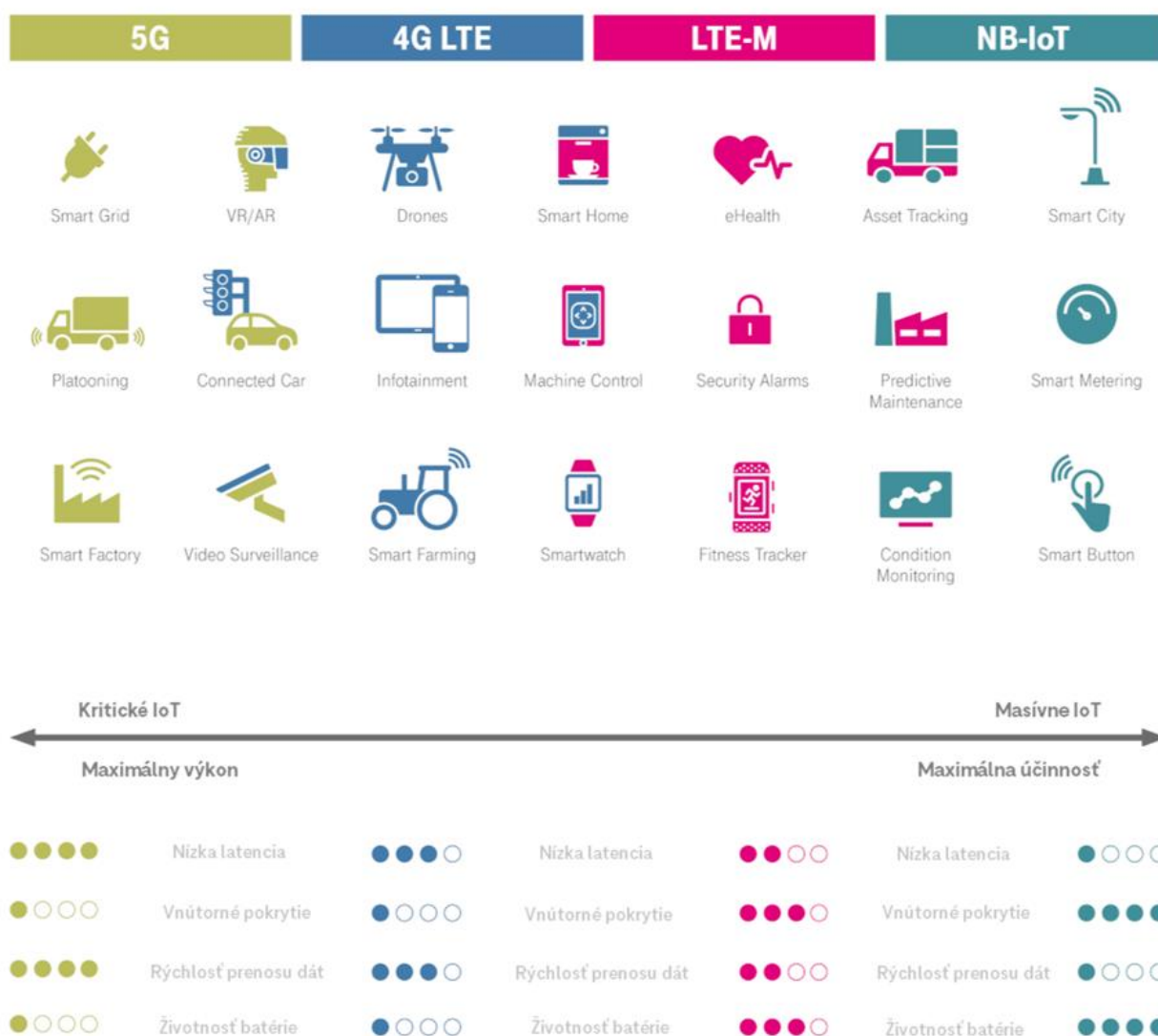
Obr. 4: Hviezdicová topológia [16]



Obr. 5: Mesh topológia [17]

Jednotlivý popis typov IoT technológií

V IoT sa komunikácia medzi zariadeniami/vecami uskutočňuje pomocou rádiových technológií, vrátane Bluetooth a Wi-Fi v sieťach LAN. V sieťach WAN sa používajú tradičné mobilné siete GSM (2G), UMTS (3G), LTE (4G), a 5G. Patria sem aj nové technológie, ktoré sú známe svojou nízkou spotrebou energie a pokrytím širokého územia LPWAN siete, Sigfox.



Obr. 6: Porovnanie rôznych typov IoT sietí a ich aplikačné možnosti [18]

LTE, 5G

LTE/LTE-Advance (LTE-A) ako štandardizovaná technológia 4. generácie (4G) je teraz úspešne nasadená po celom svete. LTE-A má nominálnu latenciu 15 ms cieľovú blokovú chybovosť (BLER) 10^{-1} [19]. V súčasnosti sa do nášho každodenného života postupne začleňujú rôzne kritické aplikácie, ktoré sa týkajú komunikácie a inteligentnej dopravy. Tieto aplikácie majú veľmi obmedzujúce požiadavky, pokiaľ ide o latenciu (1 ms alebo menej) a spoľahlivosť prenosu (BLER až 10^{-9}) [20].

Jednou z kľúčových úloh 5G je riešenie výziev nízkych oneskorení, ako aj ultravysokej spoľahlivosti prenosov. Hlavnou výhodou 5G oproti LTE je schopnosť poskytovať 100x vyššiu rýchlosť prenosu dát, 10x nižšiu latenciu a podporovať 100x viac pripojených zariadení. Je to vďaka využitiu rádiového rozhrania, ktoré zahŕňa oveľa vyššie frekvencie, ako sú milimetrové vlny (mmWave), a využívaniu pokročilejších rádiových technológií, napr. massive MIMO (mMIMO).

Štandard 5G tiež zahŕňa a stavia na súbore existujúcich štandardov zameraných konkrétne na podporu zariadení IoT s úzkou šírkou pásma, nízkou spotrebou energie. Aktuálne nasadené siete 5G sú postavené na existujúcich sieťach 4G, pričom využívajú technológie ako LTE for Machines (LTE-M) a Narrowband-IoT (NB-IoT). 5G teoreticky ponúka rýchlosti až 10 Gbit/s. V realite sa predpokladajú maximálne rýchlosti zvyčajne 100 – 200 Mbit/s. Najväčší vplyv 5G bude mať využitie technológií NB-IoT a LTE-M a ich následný vývoj v nadchádzajúcich vydaniach. Aplikácie, ktoré vyžadujú spoľahlivú a nízku latenciu komunikácie, môžu pravdepodobne čeliť pomalšiemu rozvoju [26]. Nízka latencia a ultravysoká spoľahlivosť sú dve protichodné požiadavky. Plné nasadenie 5G v oblasti internetu vecí sa zameria na súkromné areálové siete. Tie sú najrýchlejšie a najjednoduchšie na nasadenie. Prípady použitia zahŕňajú továrne, sklady, nemocnice a ďalšie iné areály.

LPWAN

LPWAN (Low Power Wide Area Network) môže byť implementované v ľubovoľnom frekvenčnom pásme LTE, súčasne s ostatnými službami LTE využívajúcimi podobnú šírku pásma. Poskytujú konektivitu pre zariadenia a aplikácie, ktoré vyžadujú nízku mobilitu a nízke rýchlosti a zriedkavý prenos dát, ako sú napríklad senzory. Technológie LPWAN vyplňajú priestor medzi mobilnými bunkovými a bezdrôtovými sieťami s

krátkym dosahom a sú určené na komunikáciu medzi zariadeniami. Zariadenia LPWAN majú dlhú životnosť batérie, pretože prenášajú len malé pakety údajov v zriedkavých intervaloch. Existuje množstvo LPWAN konkurenčných technológií, ktoré poskytujú rôzne úrovne pokrytia a kapacitu.

Nelicencované siete LPWAN:

- **LoRa**

Technológia LoRa sa zameriava na dvojsmerný prenos údajov, čo ju robí ideálnou voľbou pre prijímanie a odosielanie správ. V závislosti od faktora šírenia a šírky pásma kanála sa prenosová rýchlosť môže pohybovať medzi 50 b/s a 300 kb/s. LoRa má štandardizovaný komunikačný protokol založený s názvom LoRaWAN. LoRaWAN je organizovaný v topológii hviezdy, kde zariadenia brány prenášajú správy medzi koncovými zariadeniami a centrálnym sieťovým serverom [21]. LoRaWAN definuje tri typy zariadení (trieda A, B a C). Trieda A je trieda zariadení LoRaWAN s najnižšou spotrebou energie. Triedy B sú navrhnuté pre aplikácie s dodatočnými požiadavkami na downlink prenos. Triedy C majú kontinuálne prijímacie sloty, a teda vždy počúvajú kanál okrem prípadov, keď potrebujú vyselať. Napriek týmto triedam všetky zariadenia sú kompatibilné s triedou A [21].

- **SigFox**

Je ďalším dominantným nelicencovaným riešením LPWAN. SigFox navrhuje použiť ultra úzkopásmovú (UNB) technológiu so šírkou pásma len 100 Hz pre prenos s veľmi krátkym užitočným zaťažením. Pomocou technológií UNB umožňuje Sigfox zariadeniam nižšiu spotrebu energie a podporuje širšie pokrytie v porovnaní s LoRa za cenu nižšej dátovej rýchlosti. Sigfox podporuje obojsmernú technológiu ale so značnou asymetriou spojenia. Downlink prenos môže byť spustený len po uplink prenose. Nevýhodou sigfoxu je obmedzený počet uplinkovej správy a maximálna dĺžka užitočného zaťaženia pre každú uplinkovú správu je tiež obmedzená. LoRaWAN je považovaný za flexibilnejší a otvorenejší konkurent.

Licencované siete LPWAN:

Sa vzťahujú na technológie LPWAN využívajúce licencované zdroje spektra. Sú štandardizované podľa 3GPP. Pre licencované LPWAN sú LTE-M a NB-IoT dva najslubnejšie štandardy, ktoré boli zavedené v roku 2016 [22].

- **LTE-M**

Je možné považovať za zjednodušenú verziu LTE určenú pre aplikácie IoT s nízkou cenou zariadenia a nízkou spotrebou energie. LTE-M je plne kompatibilný s existujúcimi bunkovými sieťami. LTE-M ponúka rýchlosť prenosu dát 1 Mbit/s pre 3GPP vydanie 13, ktorá sa zvyšuje na 4 Mbit/s pre vydanie 14, väčšiu mobilitu a hlasové možnosti cez sieť [23]. V 3GPP Rel-14 a Rel-15 boli navrhnuté nové funkcie na zvýšenie výkonu LTE-M z hľadiska rýchlosti prenosu dát, latencie, určovania polohy a hlasového pokrytia. Na zníženie nákladov a zložitosti hardvéru sa používa šírka pásma 1,4 MHz a zvyčajne podporuje jeden reťazec prijímacej antény a polovičné duplexné operácie. Povolené sú ale aj plne duplexné prevádzky. LTE-M spotrebuje však viac energie, pretože poskytuje vyššie prenosové rýchlosti a implementuje plno hodnotnejší protokol v porovnaní s NB-IoT.

- **NB-IoT**

V porovnaní s LTE-M je NB-IoT systém postavený na existujúcej funkcionalite LTE s jediným úzkym pásmom 200 kHz s nízkou zložitou základného pásma, ktorého cieľom je podpora širšieho pokrytia, nižšie náklady na zariadenie, dlhšia výdrž batérie, a vyššia hustota spojenia. NB-IoT je tiež kompatibilný s existujúcimi sieťami LTE, ktoré môžu využívať existujúci sieťový hardvér a znižovať náklady na nasadenie. NB-IoT podporuje iba polovičné duplexné operácie. NB-IoT rozširuje pokrytie a hlboko preniká do budov a menej dostupných oblastí vďaka úzkej šírke pásma a nízkej rýchlosti prenosu. Pomocou NB-IoT dokážeme prepojiť množstvo zariadení na relatívne veľkom území. V závislosti od pokrytia NB-IoT toleruje latenciu, ktorá môže dosiahnuť sekundy zatiaľ čo v LTE-M je nutná v desiatkach milisekúnd [24].

Technológie krátkeho dosahu

Bezdrôtové technológie krátkeho dosahu pre aplikácie IoT sa používajú na podporu konektivity v rámci malej oblasti pokrytia. Existuje množstvo technológií krátkeho dosahu s rôznymi funkciami a výkonom pre dané aplikačné požiadavky.

- **Wi-Fi**

Wi-Fi ponúka nízku spotrebu energie a nízke náklady v porovnaní s bunkovou sieťou. Wi-Fi funguje v nelicencovanom spektre, čo má za následok aj nižšie náklady na prenos dát. Väčšina sietí Wi-Fi dnes funguje v pásme ISM na 2,4 GHz a 5 GHz. Keďže v pásme 5 GHz je k dispozícii viac kanálov, je možné dosiahnuť vyššie rýchlosti prenosu dát. Existuje niekoľko rôznych štandardov Wi-Fi optimalizovaných pre aplikácie IoT. V roku 2017 bol predstavený IEEE 802.11ah na podporu internetu vecí s rozšíreným pokrytím a požiadavkami na nízku spotrebu energie. Funguje v nelicencovaných pásmach pod 1 GHz a jeho šírka pásma je zvyčajne iba 1 MHz alebo 2 MHz. V porovnaní s vysokorýchlostnými generáciami cieľom 802.11ah je poskytnúť konektivitu tisíckam zariadení s pokrytím až 1 km. Sú vytvorené aj ďalšie iné štandardy ako napríklad 802.11p je štandard pre komunikáciu medzi vozidlami [25]. Štandard 802.11s definuje sieť Wi-Fi mesh. Za správnych podmienok zvyšuje dosah siete vďaka presmerovaniu cez viacero skokov a poskytuje väčšiu šírku pásma a lepšiu výdrž batérie vďaka nižšiemu výkonu prenosov spôsobenému kratšími skokmi medzi susednými uzlami. Siete mesh umožňujú rýchle nasadenie s lacnejším spätným prenosom a uľahčujú poskytovanie pokrytia v ťažko dostupných oblastiach [26].

- **Bluetooth**

Bluetooth funguje v nelicencovanom pásme (ISM) na frekvencii 2,4 GHz. Dosah sa pohybuje od 1 m do 100 m v závislosti od triedy použitého rádia. Rýchlosť prenosu dát sa pohybuje od 1 Mb/s až 3Mbps. Čím nižšie sú prenosové rýchlosti, tým dlhšie sú dosahy. Klasické rozhranie Bluetooth pre IoT zariadenia je nepraktický vzhľadom na tie, ktoré si vyžadujú prenosy s nízkou spotrebou energie. Na tento účel bol zavedený Bluetooth Low Energy (BLE) špeciálne pre zariadenia IoT s nízkou spotrebou. Vo verzii Bluetooth 5.1 bola vylepšená funkcia vyhľadávania smeru BLE, aby sa lepšie pochopil smer signálu a dosiahla lepšia presnosť lokalizácie [27]. Na základe rozsiahlych sietí zariadení IoT sa vytvorili siete BLE mesh [17]. Topológia BLE mesh funguje na princípe riadeného smerovania dát na preposielanie správ z jedného zariadenia na druhé [28].

2 NAVRH HARDVÉROVÉHO RIEŠENIA S VYUŽITÍM BIOMETRICKÝCH METÓD PRE MONITOROVACÍ SYSTÉM

V našej práci sa dôkladne zameriavame navrhovaním a implementáciou dochádzkového systému, pričom využívame biometrické metódy na presné zaznamenávanie príchodov a odchodov zamestnancov. Hlavným cieľom je vyvinúť systém, ktorý efektívne dokáže monitorovať dochádzku zamestnancov prostredníctvom detekcie tváre alebo odtlačkov prstov. V rámci tejto práce predstavíme komplexnú architektúru, ktorá zahŕňa hardvérové a softvérové komponenty, ako sú kamery a senzory odtlačkov prstov. Naším úsilím je vytvoriť robustný, spoľahlivý systém ktorý bude efektívny v reálnych podmienkach prevádzky.

ESP32 PSRAM Timer Camera X

Timer Kamera X je kamerový modul založený na ESP32, integrovaný s čipom ESP32 a 8M-PSRAM. Kamera (OV3660) má 3 miliónov pixelov schopná fotografovať s rozlíšením 2048 x 1536, vstavanou 140mAh batériou a LED indikátorom stavu s ultra nízkou spotrebou energie. Modul podporuje Wi-Fi prenos obrazu a ladenie USB portu. Výstup spodného portu GROVE (HY2.0-4P) je možné pripojiť k ďalším perifériám. Napájanie je zabezpečené prostredníctvom USB-C napätia 3,3V. Timer Kamera X poskytuje flexibilitu vo voľbe programovacej platformy, vrátane ESP-IDF, Arduino a UIFlow. V tomto prípade sme si zvolili platformu Arduino, ktorá ponúka vhodné prostredie pre vývoj a nahrávanie kódu na Timer Kamera X. Arduino, umožňuje efektívne využívať všetky funkcie a vlastnosti kamerového modulu X.



Obr. 7: ESP32 PSRAM Timer Camera X [29]

Senzor odtlačku prsta AS608

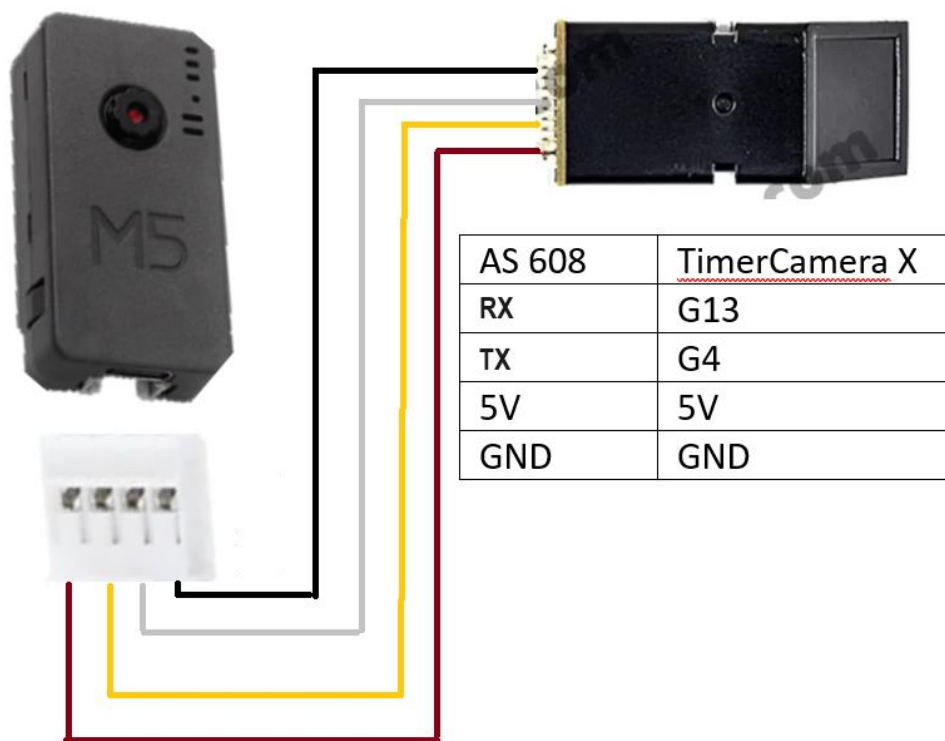
Optický senzor odtlačkov prstov AS608, pracuje s nízkym rozlíšením a zbiera obraz koncovkej časti prsta. Tieto obrazy sa následne spracovávajú a transformujú na polia identifikátorov, ktoré slúžia na jedinečnú identifikáciu každého odtlačku prsta. Senzor AS608 má kapacitu uložiť až 128 jedinečných odtlačkov prstov a je plne kompatibilný s platformou Arduino. Pomocou poskytnutých informácií o registrovaných odtlačkoch prstov je senzor schopný overiť a odmietnuť priložené odtlačky. Komunikácia so snímačom prebieha cez UART sériovú komunikáciu, čo umožňuje jednoduchú integráciu s Arduino, a to vďaka knižnici ADAFRUIT. Algoritmus odtlačkov prstov, ktorý je integrovaný v senzore, umožňuje rýchle a spoľahlivé spracovanie odtlačkov prstov a porovnávanie s uloženými vzormi.



Obr. 8: Senzor AS608 [30]

2.1.1 Hardvérové zapojenie dochádzkového systému.

Pre napájanie kamery využívame USB-C kde je nutné minimálne napätie 5V. Pre pripojenie senzoru odtlačkov prsta AS608 využívame konektor GROVE (HY2.0-4P), ktorý je na spodnej časti kamery. Pre správne pripojenie senzora bolo nutné správne pripojiť príslušné piny senzora s GROVE konektorom. Medzi sensorom a kamerou sú potrebné dva piny - RX (receive) a TX (transmit). Pin RX senzora je pripojený k pinu G13 na Timer Kamere X, ktorý slúži na prijímanie dát, zatiaľ čo pin TX senzora je pripojený k pinu G4 na Timer Kamere X a slúži na vysielanie dát ako je vidieť na obr. č.9.

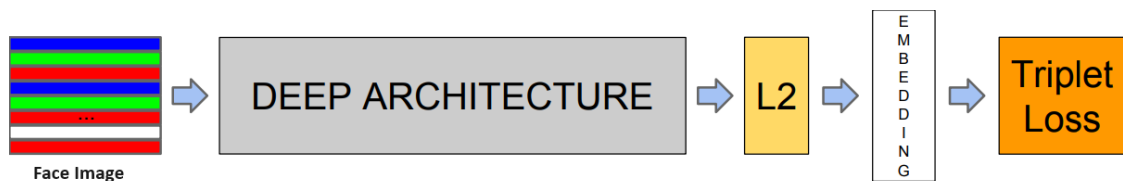


Obr. 9: Hardvérové zapojenie kamery X a senzoru odtlačku prsta

2.1.2 FaceNet

FaceNet je jedným z najvýznamnejších prelomov v technológii rozpoznávania tváre, ktorý prispieva k širokému využívaniu. FaceNet je systém založený na neurónových sieťach, ktorý využíva algoritmy hlbokého učenia na rozpoznávanie tváre. Systém bol vyvinutý spoločnosťou, Google v roku 2015. FaceNet využíva konvolučnú neurónovú sieť (CNN) na mapovanie tváre do euklidovského priestoru, kde priamo porovnáva podobnosť tvárí [31].

FaceNet využíva hlbokú neurónovú sieť, ktorá sa učí a extrahuje rôzne črty tváre. Tieto vlastnosti sú potom mapované do 128-rozmerného priestoru, kde sú tváre patriace tej istej osobe reprezentované blízko seba a ďaleko od tvarí iných osôb. Architektúra FaceNetu je zložená z nasledujúcich častí:



Obr. 10: Architektúra modelu Facenet [31]

A. Hlboká neurónová sieť

FaceNet využíva vo svojej architektúre komplexné učenie. Pôvodne FaceNet používal Inception Network ako svoju chrbticovú architektúru. Základným konceptom Inception je použitie 1X1 filtrov na redukcii rozmerov. Ako príklad, konvertovanie 256x256x3 RGB obrazu na 256x256x1. V súčasnosti je možné použiť množstvo chrbticových sietí namiesto Inception Network.

B. Normalizácia

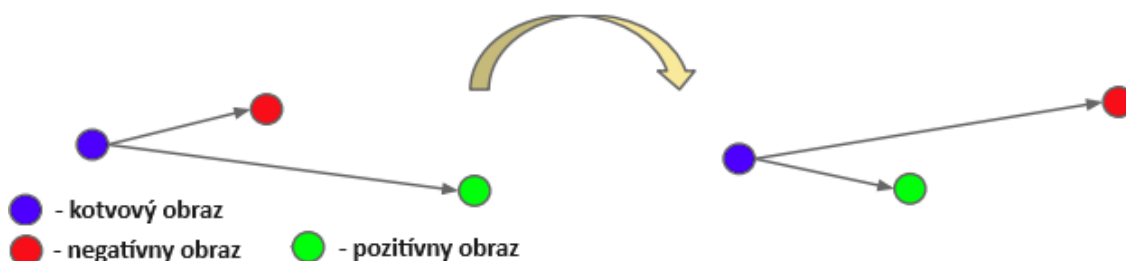
Tieto modely hlbokého učenia poskytujú vloženie obrazu s normalizáciou L2 známej aj ako euklidovská norma. Tento proces zabezpečuje, že každý vektor má dĺžku 1 vo vektorovom priestore. Čím sa uľahčuje porovnávanie a klasifikácia tvárí pomocou jednoduchších matematických operácií.

C. Vkládanie

Na vkladanie sa dá pozerat' ako na "zhrnutie" identity. Vkladanie sa vypočíta a zmapuje v príslušnom priestore prvkov. Použitie takejto menšej reprezentácie (v porovnaní s originálnym obrazom) je rozhodujúce pre efektívne riešenie úlohy rozpoznávania tváre. Vkladanie umožňuje efektívne a spoľahlivé porovnanie tvári napriek variabilitám v osvetlení, póze, alebo výrazu tváre.

D. Trojitá strata

Táto funkcia je kľúčová k trénovaniu modelu FaceNet. Myšlienka použitia trojitej straty je, že pomáha modelu presadiť rozpätie medzi tvármi rôznych identít. Funkcia porovnáva vzdialenosť medzi obrazom kotvy a pozitívnym obrazom tej istej osoby so vzdialenosťou medzi obrazom kotvy a negatívnym obrazom inej osoby. Cieľom je minimalizovať vzdialenosť medzi obrazom kotvy a pozitívnym obrazom a zároveň maximalizovať vzdialenosť medzi obrazom kotvy a negatívnym obrazom. Výber trojice (troch obrazov, ktoré sa majú zadať ako vstup do funkcie) pre funkciu trojitej straty je rozhodujúci pre efektívnosť tréningu. Náročnejšie trojice na učenie, môžu byť užitočné na zlepšenie odolnosti siete voči zmenám osvetlenia, pózy a výrazu. Výber trojíc je dôležitým aspektom tréningu architektúry FaceNet a vyžaduje vyváženie požadovaného výkonu s dostupnými zdrojmi.



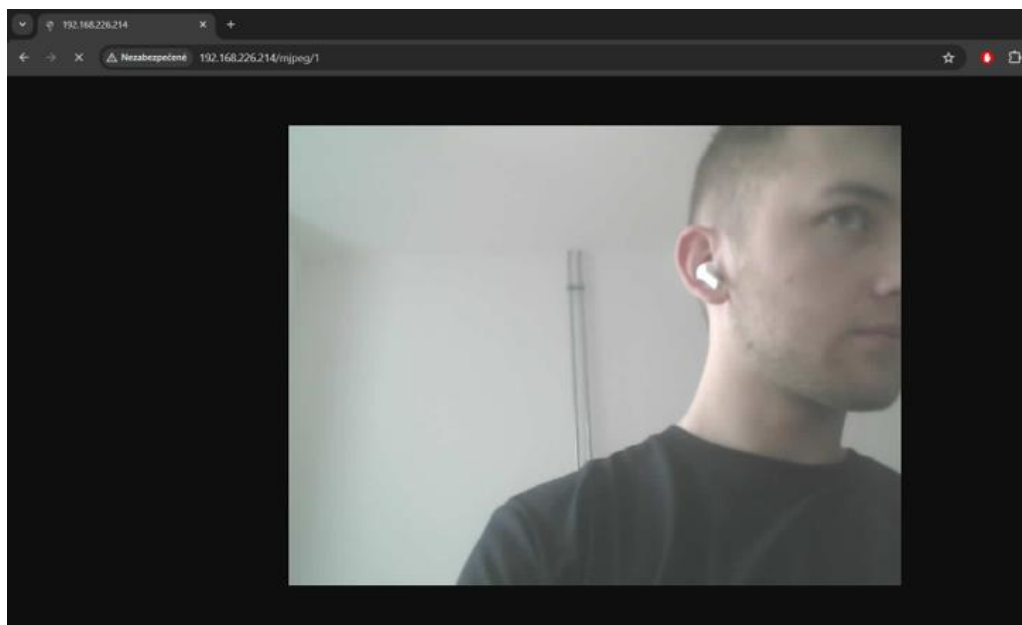
Obr. 11: Trojitá strata a učenie [31]

FaceNet dosiahol na súbore údajov o tvárach z YouTube presnosť 95,12 % so štandardnou chybou 0,39 pri použití prvých 100 snímok. Výsledky modelu FaceNet ukazujú, že model je invariantný voči zakrývaniu časti tváre, póze, osvetleniu a dokonca aj veku [31].

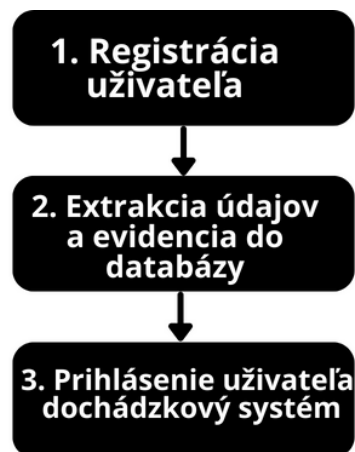
3 SOFTVÉROVÁ REALIZÁCIA MONITOROVACIEHO SYSTÉMU

Na vytvorenie komplexného softvéru pre správu kamery a senzoru odtlačku prsta využívame platformu Arduino v jazyku C++. Táto platforma poskytuje širokú škálu možností konfigurácie a ovládania, vrátane nastavenia rozlíšenia obrazu, kvality JPEG a ďalších mnohých nastavení. Bezdrôtové pripojenie realizujeme pomocou Wi-Fi pripojenia, ktoré umožňuje streamovať obraz v reálnom čase vo formáte MJPEG, čím vytvárame integrované IoT riešenie. Náš kód implementuje možnosť generovania IP/URL adresy v lokálnej sieti, čo umožňuje sledovať živý obraz z kamery v reálnom čase. Táto funkcionálna podporuje súčasné pripojenie 10 klientov. Vytvorili sme RTOS tasky pre efektívne spracovanie obrazových dát a ich odosielanie klientom. Tasky sa starajú o získavanie snímok z kamery a ich odosielanie klientom cez webový server. To umožňuje plynulý tok obrazových dát a poskytuje užívateľom živý obrazový stream z kamery.

V rámci implementácie odtlačku prsta využívame knižnicu Adafruit, ktorá umožňuje získavať a spracovávať odtlačky prsta, aby sme ich v prípade potreby mohli registrovať a následne ukladať. Vytvorený kód používa metódy pre prácu s HTTP protokolom na odosielanie informácií (identifikátorov odtlačkov prstov) na server, čo umožňuje ďalšie spracovanie a riadenie systému.



Obr. 12: MJPEG streamu s rozlíšením 800x600 vo webovom prehliadači

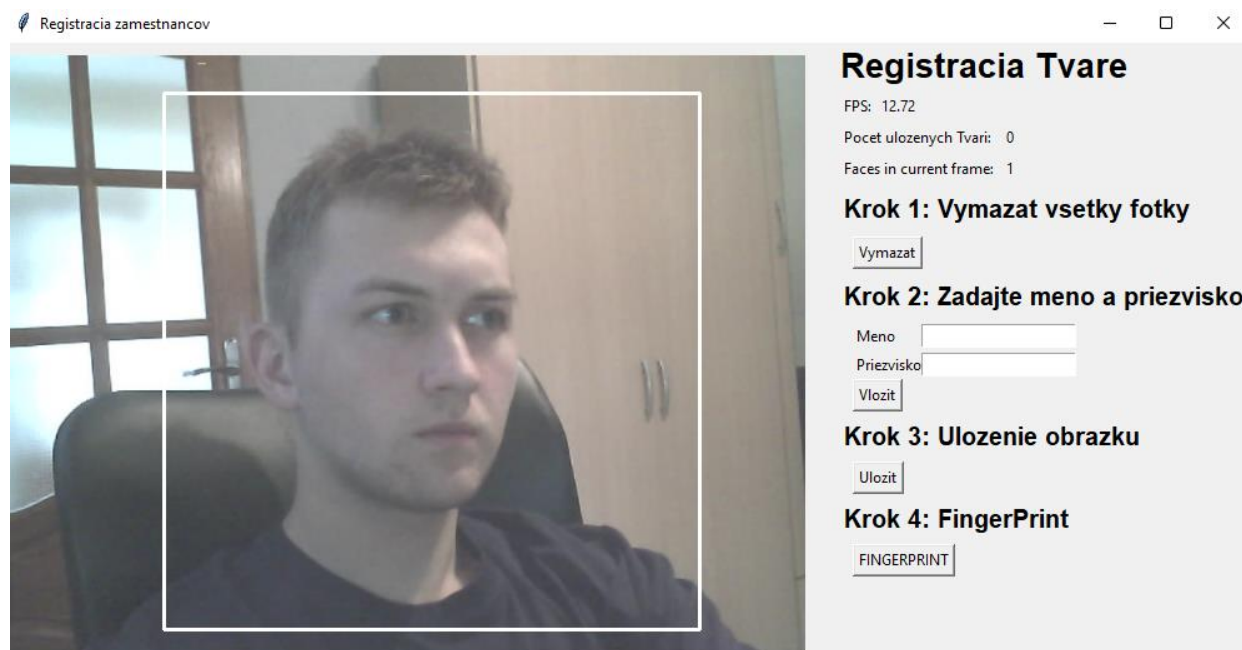


Obr. 13: Bloková schéma softvérovej realizácie dochádzkového systému

Tieto kroky sú základnými stavebnými blokmi pri vytváraní softvérovej implementácie dochádzkového systému. Ich dodržiavanie zabezpečuje účinnú a spoľahlivú prevádzku systému, ktorý prispieva k efektívnemu riadeniu dochádzky zamestnancov.

3.1.1 Registrácia užívateľa

Pre registráciu zamestnancov používame platformu Python. Aplikácia získava obraz v reálnom čase z IP/URL adresy pomocou vytvoreného kódu v platforme Arduino. Proces registrácie je rozdelený do niekoľkých krokov, ktoré sú znázornené na obr.14.



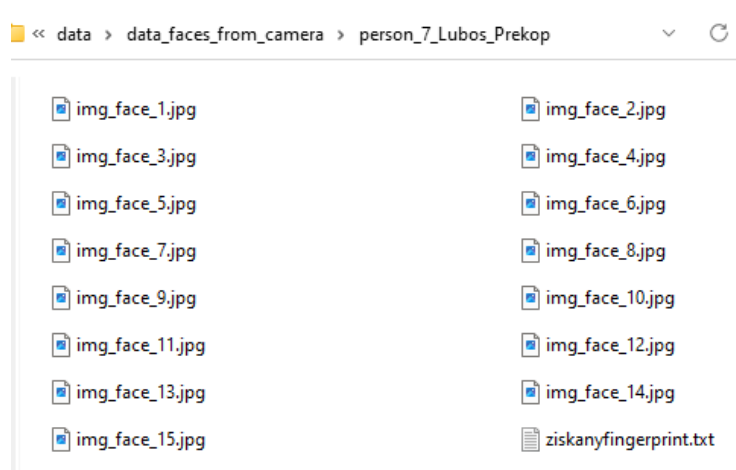
Obr. 14: Aplikácia pre registráciu zamestnanca

1. Vymazanie fotografií

Prvý krok registrácie umožňuje správcovi systému flexibilne rozhodnúť, či chce udržať alebo odstrániť existujúce fotografie zamestnancov. Tento krok slúži na možnosť vymazať všetky existujúce fotografie zamestnancov, ktorí už boli zaregistrovaní. Uvedená funkcionality pre používateľa nie je povinná a fotky môžu zostať zachované v prípade, aj keď sú už registrované v databáze. Niekedy je nutné vymazať existujúce fotografie z databázy, aby sa predišlo možným bezpečnostným rizikám spojeným s údajmi zamestnancov.

2. Zadanie mena a priezviska

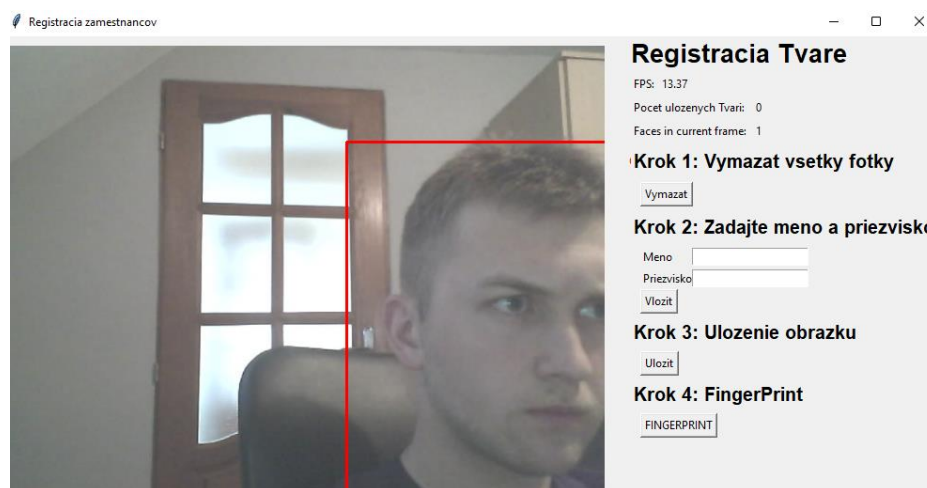
Používateľ zadáva meno a priezvisko, čím sa vytvorí priečinok pre konkrétneho zamestnanca. Priečinok slúži ako jedinečný identifikátor pre následné spracovanie údajov.



Obr. 15: Priečinok zamestnanca po registrácii

3. Fotografie zamestnanca

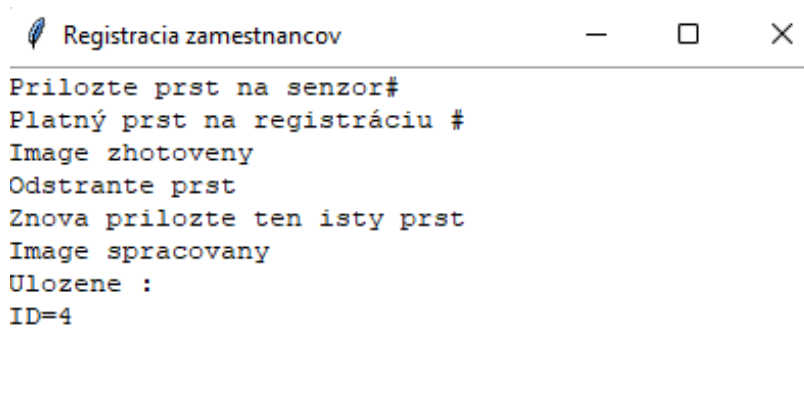
Po zadaní osobných údajov nasleduje snímanie tváre zamestnanca. Pre optimálnu detekciu dochádzkového systému sa odporúča nasnímať viacero fotografií zamestnanca. Biely obdĺžnik na obrazovke signalizuje, že je zamestnanec v optimálnej vzdialenosti pre kvalitnú detekciu tváre. Červený obdĺžnik znamená, že sa musí priblížiť alebo vzdialiť, aby bola dosiahnutá optimálna vzdialenosť. Ak sa táto podmienka nesplní, snímanie tváre nie je možné. Sú nasnímané iba správne zarovnané tváre, čo prispieva k presnosti a spoľahlivosti registrácie. V našom prípade štvorcový obrázok obsahujúci iba tvár osoby je užitočný na zníženie rozptylu pri trénovaní.



Obr. 16: Neoptimálne umiestnenie tváre – červený obdĺžnik

4. Odtlačok prsta

Štvrtý a posledný krok zahŕňa registráciu odtlačkov prstov. Po stlačení príslušného tlačidla „fingerprint“ žiada od zamestnanca priložiť prst na snímač odtlačkov. Po správnom zachytení požaduje opätovné priloženie prsta. Úspešné porovnanie a získanie zhody odtlačkov vytvára jedinečné ID odtlačku prsta, ktoré je uložené v priečinku zamestnanca.



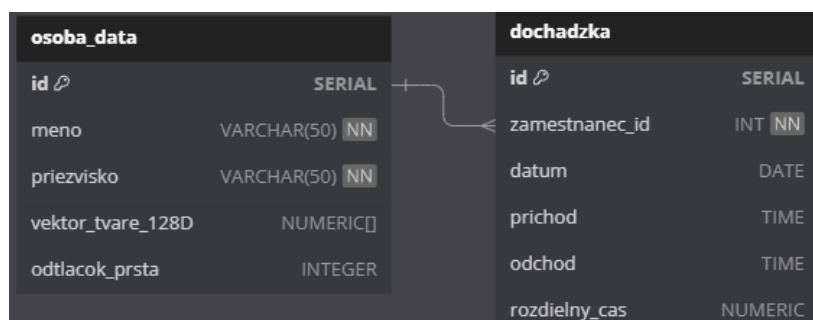
Obr. 17: Proces registrácie odtlačku prsta

Webový framework Flask vytvára rozhranie medzi Arduino a Pythonom a umožňuje nám vytvoriť server, ktorý prijíma a spracováva požiadavky. Toto rozhranie slúži ako API (Application Programming Interface), čo znamená, že umožňuje komunikáciu a interakciu medzi rôznymi časťami softvéru. V tomto prípade aplikácia v Pythone pomocou HTTP požiadaviek získava údaje z Arduino, ako sú informácie a identifikátory odtlačkov prstov, na účely registrácie. Takto vytvorené API poskytuje jednoduchý a spoľahlivý spôsob integrácie rôznych častí systému a umožňuje nám efektívne fungovať ako jednotný celok.

3.1.2 Extrakcia údajov a evidencia do databázy

Po úspešnej registrácii zamestnanca je nutné vykonať ďalší krok a to je vytvorenie záznamu v databáze pre zamestnanca. Tento krok sme implementovali v Pythone, kde sa spracúvajú fotografie tváre a identifikátory odtlačkov prstov, ktoré boli získané počas registrácie. V našej implementácii aplikujeme už predtrénovaný model poskytnutý knižnicou Dlib [32]. Tento model je natrénovaný na veľkom množstve dát a je schopný efektívne generovať 128D vektory tváre, čo nám umožňuje rýchlo a spoľahlivo identifikovať tváre a vytvárať ich reprezentácie v podobe vektorov. Na spracovanie fotografií používame detektor tváre na identifikáciu tváre na fotografiách. Potom sa použije model landmarkov, aby sa získali dôležité body tváre, ako sú polohy očí, nosa a úst, konkrétne 68 bodov. Nakoniec sa použije predtrénovaný model na získanie 128D vektorov tváre, ktoré sú reprezentáciou tváre v podobe vektorov. Ak existuje viacero fotografií vytvorených v priečinku, spraví sa stredná hodnota vektora, ktorá sa považuje za kvalitnú reprezentáciu 128D vektora tváre. Tento vektor následne používame na identifikáciu a záznam zamestnanca v databáze. Ďalej spracovávame záznam odtlačku prsta, ktorý bol vytvorený a uložený počas registrácie. Informácie záznamu sú použité na identifikáciu zamestnanca v databáze. Zamestnanec si môže zvoliť jednu z metód identifikácie - buď odtlačok prsta, vektor tváre alebo oboje.

Na vytvorenie databázy sme si zvolili objektovo-relačný databázový systém PostgreSQL. V PostgreSQL databáze sú vytvorené dve tabuľky: „osoba_data“ a „dochadzka“. Tabuľka osoba_data ukladá informácie o jednotlivých zamestnancoch, zatiaľ čo tabuľka dochadzka slúži na evidenciu dochádzky zamestnancov. Táto štruktúra umožňuje efektívny prístup k údajom a zabezpečuje integritu dát. Dochádzkový systém ukladá záznamy o dochádzke zamestnanca, vrátane dátumu, príchodu odchodu a časových rozdielov. Pri práci s databázou využívame knižnicu Psycopg2 na pripojenie.

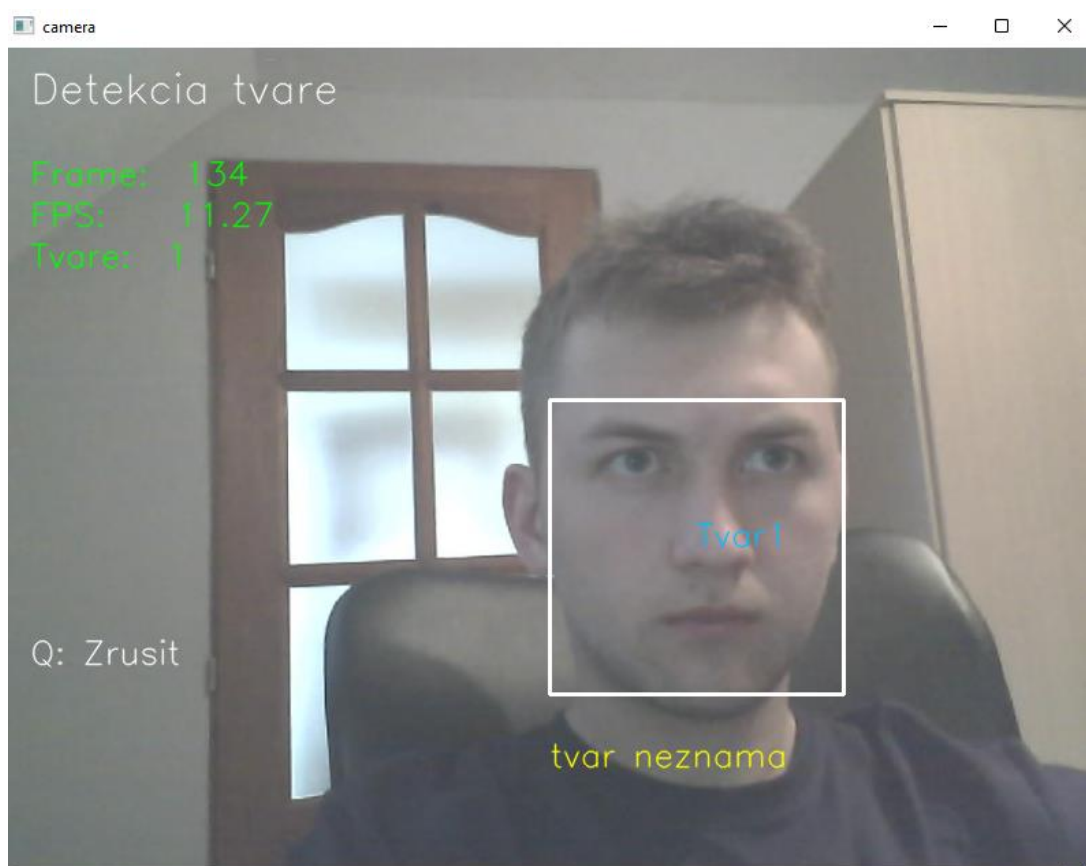


Obr. 18: Konceptuálna schéma dochádzkového systému

3.1.3 Prihlásenie užívateľa do dochádzkového systému

V reálnom čase spracovávame obraz kamery v jazyku Python a pripájame sa na databázu pomocou knižnice psycopg2. V našom vytvorenom kóde sme implementovali proces na porovnávanie tváre s databázou. Pre každú rozpoznatú tvár v reálnom čase porovnáваме s tvármi (vektormi) uloženými v databáze. Výsledné euklidovské vzdialenosti sú porovnávané s prahovou hodnotou 0,4. Ak je minimálna vzdialenosť nižšia ako táto hodnota, tvár považujeme za zhodnú a priradí sa jej identifikátor zamestnanca (ID). Týmto spôsobom sa umožňuje zamestnancovi prihlásiť do dochádzkového systému.

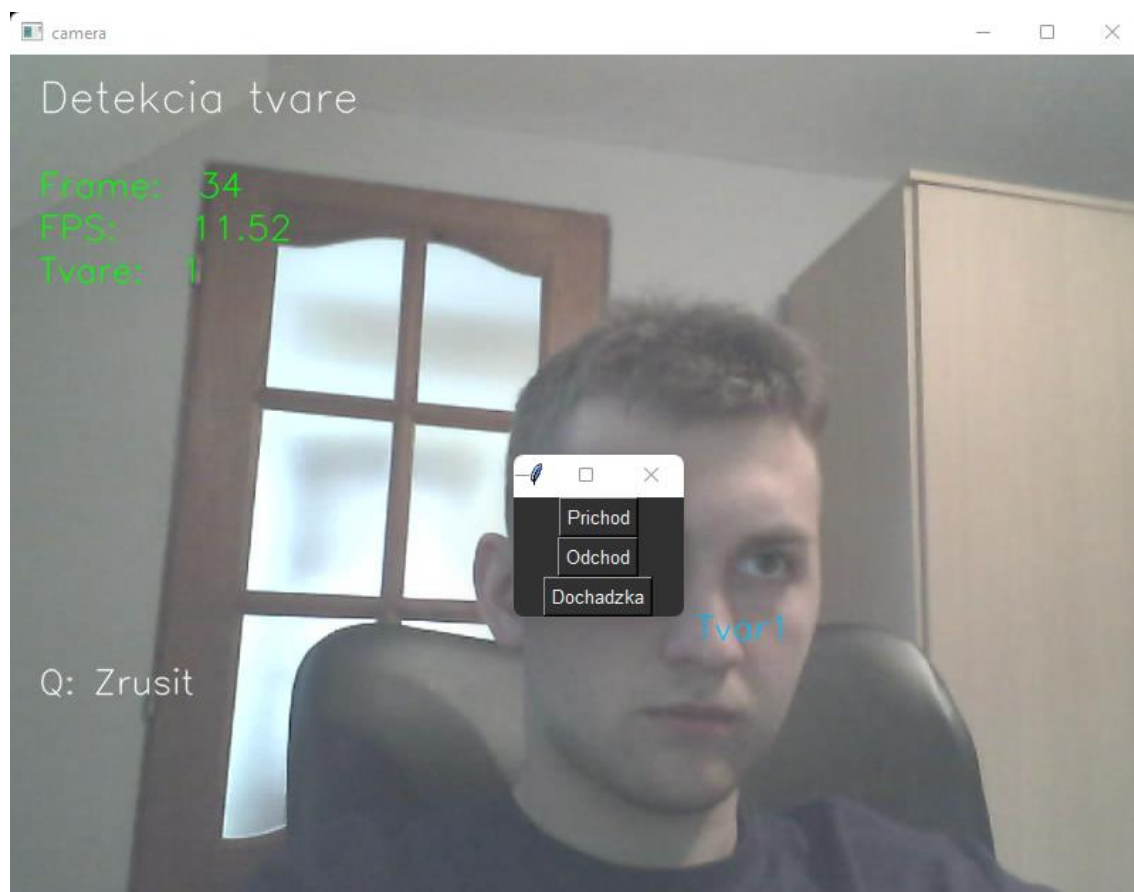
Pre metódu odtlačku prsta, zamestnanec v reálnom čase priloží prst na snímač odtlačkov prstov. Úspešné prihlásenie v porovnaní s odtlačkami v databáze nastane, kedy senzor porovná aktuálne zosnímaný odtlačok prstu so uloženými odtlačkami v pamäti a pomocou HTTP protokolu pošle ID zamestnanca s prahovou hodnotou ktorá musí byť vyššia ako hodnota 70. Ak je táto podmienka splnená a v databáze existuje príslušné ID odtlačku, umožňuje zamestnancovi úspešné prihlásenie do dochádzkového systému.



Obr. 19: Neúspešné prihlásenie do systému

Pri detekcii tváre, ak systém nedokáže rozpoznať tvár, aplikácia upozorní užívateľa pod obdĺžnikom, že uvedená tvár sa nenachádza v databáze obr.19. Tento prípad nastáva, keď užívateľovi systém deteguje tvár, ale minimálna vzdialenosť medzi jeho tvárou a tvármi v databáze je väčšia ako prahová hodnota 0.4. Toto upozornenie môže zamestnanca viesť k tomu, aby skúsil iný uhol alebo postoj, aby systém lepšie identifikoval jeho tvár a umožnil mu úspešné prihlásenie. Užívateľ sa neprihlási do systému v prípade ak jeho tvár nie je registrovaná v databáze.

Po úspešnom prihlásení sa zobrazí zamestnancovi nové okno, kde má možnosť si vybrať príchod, odchod alebo zobrazenie dochádzky, ako je možné vidieť na obr. 20. Dochádzkový systém využíva časový rozdiel medzi príchodom a odchodom pre efektívne sledovanie dochádzky zamestnanca s prihliadnutím na prípadné prestávky. Pri výpočte časového rozdielu sa implementovalo zaokrúhľovanie na polhodinové intervaly.

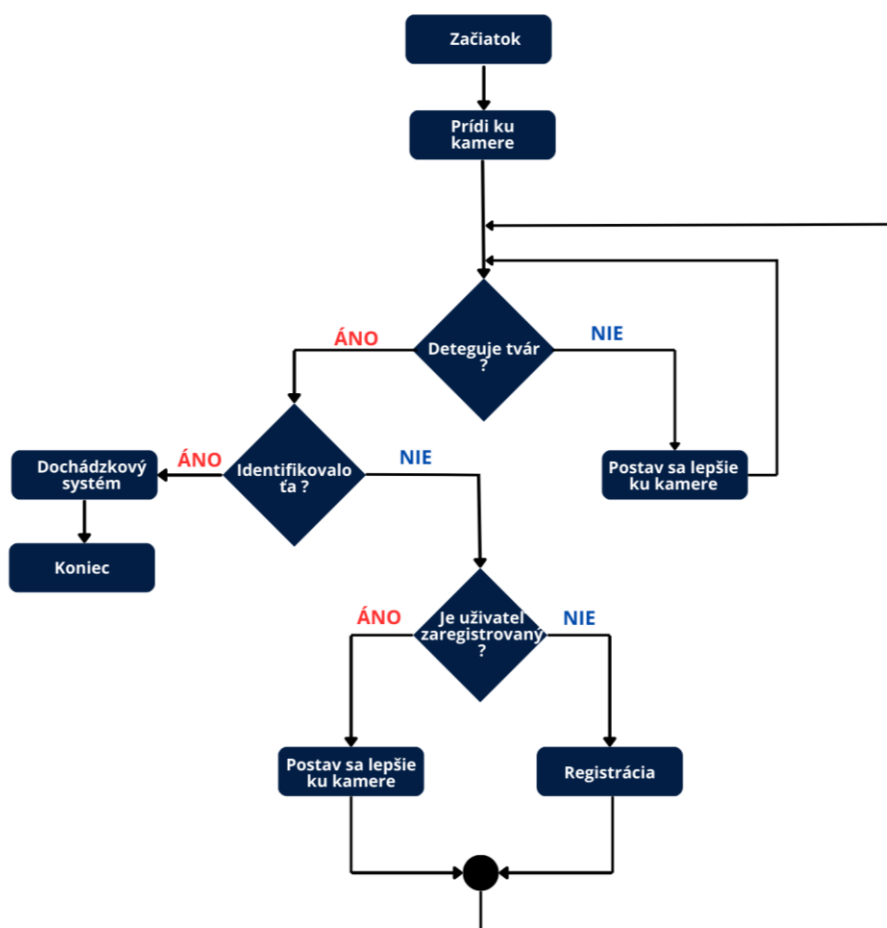


Obr. 20: Úspešné prihlásenie zamestnanca do dochádzkového systému

		Príchod	Odchod	Dochádzka
	Datum	Cas prichodu	Cas odchodu	Pocet hodin
	2024-03-09	19:52:01.020017	21:21:57.483262	1.0
	2024-03-22	21:01:33.004795	22:17:42.140417	1.0
	2024-03-23	12:50:56.543651	12:51:07.947743	0.0
	2024-03-23	12:51:34.529082	15:07:20.220068	2.0
	2024-03-23	15:07:27.089322	21:42:05.125302	6.0
	2024-03-24	12:52:35.685701	18:09:40.812897	5.0
	2024-03-26	08:36:19.702253	21:10:34.162290	12.0
	2024-03-27	10:03:07.512342	20:45:03.616318	10.0
	2024-03-28	09:27:08.076988	20:53:36.962599	10.5
	2024-03-30	16:46:40.015794	20:40:50.217149	3.5
	2024-03-31	10:19:52.905616	20:45:22.197367	9.5
Celkový odpracovaný čas za March: 60.5 hours				

Obr. 21: Zobrazenie dochádzky zamestnanca

Po prihlásení do systému má zamestnanec možnosť pozrieť svoju dochádzku v rámci aktuálneho mesiaca. Spodná časť tabuľky zobrazuje celkový počet odpracovaných hodín za celý mesiac, čo poskytuje zamestnancovi jasný prehľad o jeho pracovnom výkone počas daného obdobia.

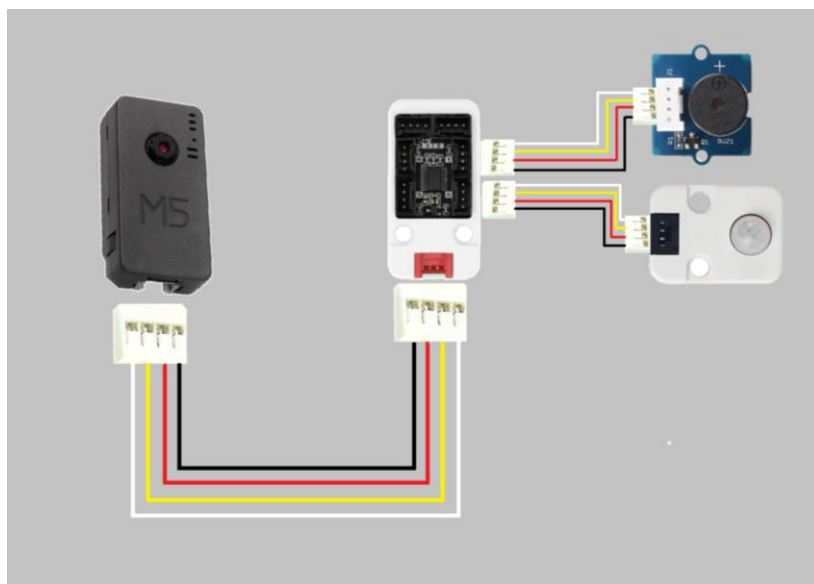


Obr. 22: Vývojový diagram dochádzkového systému pre detekciu tváre

Vývojový diagram dochádzkového systému kompaktne zobrazuje všetky hlavné body predstavené vyššie. Ide o dynamický cyklický proces, ktorý neustále monitoruje prostredie a snaží sa detegovať tváre a identifikovať užívateľov pri ich príchode. Úspešná identifikácia umožňuje užívateľovi prihlásenie do systému, no v prípade neúspešnej detekcie sa systém snaží upozorniť užívateľa na lepšie postavenie pre zachytenie celej tváre. Pri neúspešnej identifikácii užívateľovi je odporúčané meniť polohu pre rôzne uhly detekcie. Ak užívateľ nie je zaznamenaný v databáze, nebude mu umožnené prihlásenie do systému. Je nutný proces registrácie, pri ktorom sa zachytia snímky tváre a následne sú uložené do databázy pre budúce identifikácie.

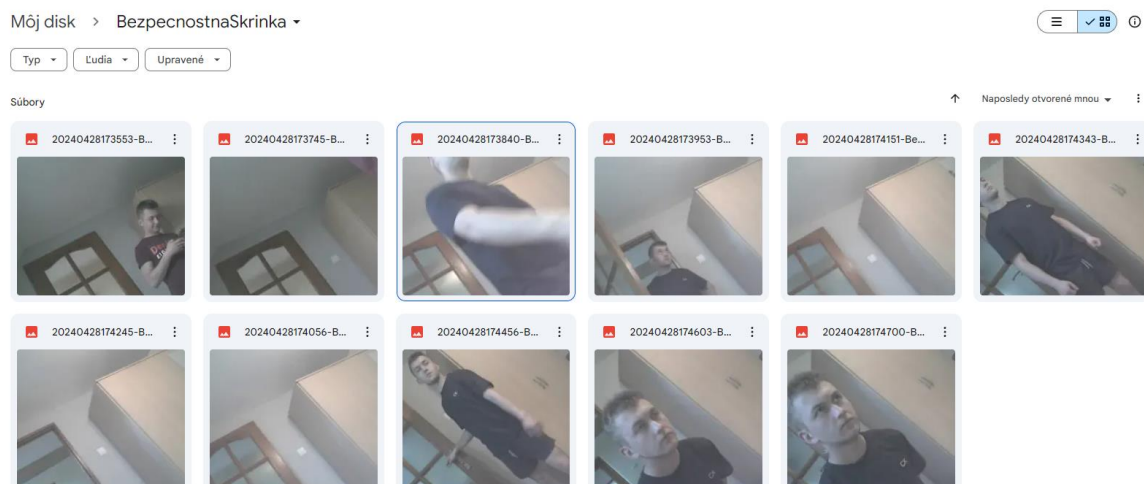
4 MONITOROVANIE POHYBU V PRIESTORE POMOCOU IOT BEZPEČNOSTNÉHO SYSTÉMU

Rozhodli sme sa implementovať IoT bezpečnostný systém, ktorý monitoruje pohyby v určenom priestore. Pre tento systém sme zvolili Timer Kamera X, ktorá vyžaduje minimálne napätie 5V a USB-C. HUB používame na prepojenie pohybového senzora a bzučiaka. Kamera X sa pripája k HUBu cez konektor GROVE, ktorý je integrovaný v HUBe. HUB má až 6 portov, z toho využívame porty 0 a 1. Pohybový senzor sa pripája na port 0 a bzučiak na port 1, oba pomocou konektora GROVE, ako je znázornené na obr. 23.



Obr. 23: Hardvérové zapojenie IoT bezpečnostného systému

Implementácia bezpečnostného systému je založená na programovaní v platforme Arduino, čo nám umožňuje efektívne spracovávať udalosti. ESP32 riadi celý systém a zabezpečuje integráciu všetkých komponentov. Pohybový senzor zachytí pohyb, spustí sa bzučiak a Timer Kamera X zachytí fotografiu. Táto fotografia je následne odoslaná na Google Drive, kde je uložená pre ďalšie použitie alebo analýzu. Na tento účel sme vytvorili skript v službe Google Apps Script, ktorý nám umožňuje prijímať HTTP požiadavky a spracovávať ich. Keď systém zachytí pohyb a vykoná fotografiu, obrázok je odoslaný ako dátový reťazec pomocou HTTP POST požiadavky. Script následne spracuje prijaté dáta, uloží obrázok do špecifikovaného priečinka na Google Drive. Tento systém nám umožňuje efektívne archivovať zachytené snímky a poskytuje nám možnosť sledovať zachytené udalosti.



Obr. 24: Zachytené fotografie v Google Drive

Okrem toho sme implementovali aj odosielanie upozornení prostredníctvom mailu. Aby sme mohli používať Gmail pre odosielanie e-mailov, museli sme povoliť prístup menej zabezpečeným aplikáciám vo svojom účte Gmail. Následne sme vygenerovali heslo pre aplikáciu, ktoré sme použili na autentifikáciu pri pripájaní k serveru SMTP. Naša aplikácia obsahuje kód, ktorý používa knižnicu "WiFiClientSecure" a obsahuje aj detaily o Gmail SMTP serveri a autentifikačné údaje. Po zachytení udalosti systém vytvorí mail obsahujúci informácie o miestnosti a čase zachytenia fotografie. Tento email je odoslaný na určenú emailovú adresu. Tento prístup nám umožňuje informovať účastníkov systému o detegovaných udalostiach prostredníctvom emailových notifikácií. Napríklad pracovníci bezpečnostných služieb dostávajú tieto správy a môžu okamžite zareagovať. Tento mechanizmus zvyšuje efektivitu a rýchlosť reakcie na potenciálne rizikové situácie.



Obr. 25: Upozornenie prostredníctvom mailu

5 VÝSLEDKY PRÁCE A DISKUSIA

Pri hodnotení rýchlosti detekcie tváre sme identifikovali niekoľko kritických faktorov, ktoré ovplyvňujú úspešnosť tohto procesu. Jedným z najdôležitejších faktorov je rozlíšenie obrazu z kamery, ktoré má priamy vplyv na kvalitu zachytených snímok a presnosť identifikácie tváre. Nižšie rozlíšenie môže viesť k nedostatočne jasným a detailným obrazom, čo znižuje schopnosť identifikovať tvár.

Tabuľka 1: Vplyv rozlíšenia obrazu na čas detekcie a FPS

Rozlíšenie	Priemerný čas [s]	FPS
320x240	6	35
640x480	4.3	17
800x600	3.6	12
1280x720	10.4	6
1920x1080	17	3

Je zrejmé, že vyššie rozlíšenie obrazu má za následok dlhší čas detekcie a nižší počet snímok za sekundu (FPS). Je to dôsledok zvýšenej zložitosti a počtu pixelov, ktoré je potrebné spracovať pri vyššom rozlíšení. Naopak, nižšie rozlíšenia umožňujú rýchlejšiu detekciu a vyššie FPS, ale sú obmedzené v čistote obrazu a detailoch. Rozlíšenie obrazu 800x600 považujeme za najviac ideálnu možnosť, s ohľadom na rýchlosť detekcie a kvalitu zobrazenia.

Dôležitým aspektom je aj kvalita registrácie tváre. Kvalita zachytených snímok tváre priamo súvisí s úspešnosťou detekcie. Pri registrácii tváre je potrebné zabezpečiť, aby boli snímky tváre zachytené vo vhodných podmienkach a z rôznych uhlov. Nasnímanie z viacerých uhlov môže výrazne zvýšiť úspešnosť následnej detekcie.

Rôzne svetelné podmienky navyše výrazne ovplyvňujú schopnosť systému rozpoznať tvár. Pri nedostatočnom osvetlení môže dôjsť k zhoršeniu kvality obrazu a následne k chybám pri detekcii. Podobne aj príliš jasné svetelné podmienky môžu spôsobiť odchýlky.

Napriek tomu, že FaceNet sa považuje za robustný a dobre pretrénovaný model natrénovaný na tisíckach fotografií, stále nemôžeme úplne zaručiť presnosť detekcie v závislosti od rôznych prostredí, uhlov, odchýlky vo vzhľade človeka. V našom systéme používame prahovú hodnotu na určenie podobnosti medzi tvármi. Čím je táto prahová hodnota nižšia, tým presnejšie musia byť snímky tváre, aby boli považované za podobné. Aj drobné rozdiely vo vzhľade tváre môžu mať výrazný dopad na výsledok detekcie. Tieto

rozdiely sa týkajú rôznych aspektov tváre, ako sú napríklad tvar nosa, tvar očí, pozícia pier, odtieň pleti a ďalšie detaily. To zvyšuje náročnosť procesu detekcie, pretože systém musí byť schopný identifikovať tváre aj v prípade, že sú od seba len mierne odlišné.

Tabuľka 2: Testovanie detekcie pri rôznej prahovej hodnote

Prah. hodnota	Rozlíšenie	Priemerný čas [s]
0.1	800x600	-
0.2	800x600	-
0.3	800x600	32
0.4	800x600	3.6
0.8	800x600	1

Počas nášho experimentu sme vykonali testy s rozlíšením 800x600 a rôznymi prahovými hodnotami, ktoré určujú vzdialenosť v euklidovskom priestore medzi tvármi. Experiment sme realizovali na 15 osobách, pričom nie všetky osoby mali zaregistrované nasnímané tváre na rovnakom mieste. Na základe nameraných údajov sme dospeli k nasledujúcim záverom:

- Pri prahových hodnotách 0.1 a 0.2 sme zaznamenali, že detekcia tváří nie je aplikovateľná, čo poukazuje vysokú náročnosť na presnosť a podobnosť tváří.
- Pri prahovej hodnote 0.3 sme zistili, že priemerný čas detekcie bol 32 sekúnd, pričom sme museli experimentovať s rôznymi uhlovými pohľadmi, aby sme dosiahli úspešný výsledok.
- Pri prahovej hodnote 0.4 sme zistili, že priemerný čas detekcie bol 3.6 sekundy, čo sme považovali za optimálnu hodnotu, kde sa dosahuje dobrá rovnováha medzi rýchlosťou a presnosťou detekcie.
- Pri prahovej hodnote 0.8 sme zaznamenali najkratší čas detekcie, 1 sekundu, avšak s rizikom narušenia bezpečnosti a s možnosťou identifikácie veľmi podobných tváří, ktoré môžu byť takmer identické.

Tieto výsledky poukazujú na dôležitosť voľby správnej prahovej hodnoty pri detekcii tváří, kde je potrebné zvážiť rovnováhu medzi rýchlosťou, presnosťou a bezpečnosťou systému.

Okrem toho sme pri našej práci zistili, že aplikovanie procesu detekcie tváre na každý snímok by viedlo k zníženiu efektivity a rýchlosti celej aplikácie. Preto sme zvolili metódu reklasifikácie snímok, ktorá aplikuje proces detekcie iba na každý desiaty snímok. Táto metóda nám umožňuje dosiahnuť rovnakú úroveň presnosti detekcie, pričom zachováva schopnosť spracovať obraz v reálnom čase.

Pre kvalitnejšiu detekciu sme zaviedli v našom systéme aj senzor odtlačkov prstov, ktorý poskytuje ďalšiu možnosť prihlásenia a zabezpečenia pre používateľov. Vzhľadom na to, že nie všetky prsty sú rovnaké, zohľadňujeme aj kvalitu a dôležitosť jednotlivých prstov pri registrácii a detekcii. Napríklad, pri identifikácii sa zvyčajne preferuje palec, pretože je najväčší a má väčšiu mieru detailu, čo umožňuje lepšiu detekciu a porovnanie s uloženými odtlačkami prstov. Zohľadnenie výberu správneho prsta a dôkladná registrácia odtlačkov prstov sú kľúčové pre zabezpečenie spoľahlivej a efektívnej funkcionality tejto časti aplikácie. Vďaka tejto kombinácii opatrení dosahujeme vyššiu úroveň bezpečnosti a presnosti v identifikácii, a overovaní zamestnancov. Je podstatné, aby odtlačky prstov neboli znečistené, čo môže ovplyvniť kvalitu registrácie a následne aj proces reálnej detekcie.

Pri identifikácii sa najprv overuje zhoda medzi identifikátorom extrahovaným z odtlačku prsta a identifikátorom uloženým v našej databáze. Tento proces je riadený prahovou hodnotou, ktorá určuje minimálnu hodnotu porovnania, ktorá musí byť dosiahnutá, aby sa identifikácia považovala za úspešnú.

Keďže proces identifikácie môže byť ovplyvnený rôznymi faktormi, ako sú napríklad kvalita odtlačku prsta alebo podmienky prostredia, zahrnuli sme aj kontrolu kvality porovnania. Keď sa dosiahne zhoda a porovnanie prekročí stanovenú prahovú hodnotu, používateľ je úspešne prihlásený do dochádzkového systému. Po niekoľkých testovaniach sme sa snažili nájsť ideálnu hodnotu prahovej hodnoty, ktorú sme stanovili na 70.

Na dosiahnutie prihlásenia do aplikácie je potrebné, aby bola spustená na zariadení, kde sa zobrazuje aktuálny záznam obrazu. Tento záznam slúži ako vizuálny sprievodca pre zamestnanca, aby sa mohol správne postaviť pri detekcii tváre alebo pri použití odtlačku prsta. Po úspešnom prihlásení zamestnanec má možnosť jednoducho vybrať príchod, odchod alebo zobrazit' svoju dochádzku. Tento spôsob interakcie zabezpečuje jednoduché a efektívne používanie aplikácie zamestnancom a minimalizuje riziko chýb v procese sledovania dochádzky.

ZÁVER

Cieľom našej bakalárskej práce bolo navrhnúť a implementovať monitorovací systém s využitím IoT technológií, ktorý zahŕňa dochádzkový systém využívajúci biometrické metódy na zaznamenávanie príchodov a odchodov zamestnancov. Systém sa zameriava na využitie technológie internetu vecí na zlepšenie efektívnosti a bezpečnosti v pracovnom prostredí. Skúmali sme technológie IoT a ich aplikácie v rôznych oblastiach života, s dôrazom na komunikačné technológie umožňujúce spoľahlivú a efektívnu výmenu údajov medzi zariadeniami v IoT sieti.

Detailne sme predstavili architektúru systému a proces implementácie softvéru na správu kamery ESP32 Timer Camera X a senzora odtlačku prsta AS608. Tieto kroky viedli k vytvoreniu komplexného dochádzkového systému, ktorý umožňuje jednoduché prihlásenie zamestnancov pomocou biometrických údajov.

Venovali sme sa aj monitorovaniu pohybu v určenom priestore a architektúry systému vrátane zapojenia hardvéru a implementácie služieb Google Drive a SMTP na archiváciu fotografií a odosielanie upozornení pri narušení bezpečnosti.

V poslednej časti sme zhodnotili naše výsledky implementácie nášho IoT dochádzkového systému, kde poukazujeme na jeho potenciál a výzvy. Navrhli sme niekoľko odporúčaní pre optimalizáciu a zlepšenie efektivity pre použitie v praxi.

Práca na tomto projekte bola veľmi komplexná a identifikovali sme množstvo potenciálnych vylepšení, ktoré by tento systém výrazne zdokonalili. Jedným z týchto vylepšení je vytvorenie výpočtového servera, ktorý by centralizoval spracovanie údajov a výpočty. Vytvorené API, cez ktoré by koncové zariadenia komunikovali a získavali potrebné informácie. Týmto spôsobom by sme eliminovaním priameho pripájania aplikácií na databázu zvýšili bezpečnosť systému a udržateľnosť databázových operácií.

Veríme, že náš IoT monitorovací systém predstavuje hodnotný nástroj pre podniky a organizácie, ktoré sa zaoberajú riadením pracovnej dochádzky a zabezpečením pracovného prostredia. Jeho schopnosť zaznamenávať príchody a odchody zamestnancov pomocou biometrických údajov a sledovať pohyb v určených priestoroch môže výrazne prispieť k zlepšeniu efektivity a bezpečnosti v pracovnom prostredí. Vďaka využitiu IoT technológií môže byť tento systém ďaleko flexibilnejší a schopný prispôbiť sa meniacim sa potrebám a požiadavkám organizácií.

ZOZNAM POUŽITEJ LITERATÚRY

- [1] The internet of things. *Forbes* [online]. [cit. 2024-02-26]. Dostupné na: <https://www.forbes.com/global/2002/0318/092.html>.
- [2] *What is the Internet of Things (IoT)?* [online]. [cit. 2024-02-26]. Dostupné na: <https://www.oracle.com/internet-of-things/what-is-iot/>.
- [3] IoT connected devices worldwide 2019-2030. *Statista* [online]. [cit. 2024-02-26]. Dostupné na: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>.
- [4] KHANNA, Abhishek a Sanmeet KAUR. Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. *Wireless Personal Communications* [online]. 2020, vol. 114, p. 1687–1762. ISSN 1572-834X.
- [5] LEVINA, Anastasia I., Alissa S. DUBGORN a Oksana Yu. ILIASHENKO. Internet of Things within the Service Architecture of Intelligent Transport Systems, European Conference on Electrical Engineering and Computer Science (EECS) [online]. 2017, p. 351–355. ISBN 978-1-5386-2085-4.
- [6] *HNonline.sk - Čo to je inteligentná doprava?* [online] [cit. 2024-02-26]. Dostupné na: <https://hnonline.sk/focus/ekonomika/2023036-co-to-je-inteligentna-doprava>.
- [7] SHAHINZADEH, Hossein, Jalal MORADI, Gevork B. GHAREHPETIAN, Hamed NAFISI a Mehrdad ABEDI. IoT Architecture for Smart Grids. 2019 International Conference on Protection and Automation of Power System (IPAPS) [online]. 2019, p. 22–30. ISBN 978-1-7281-1505-4.
- [8] Čo je inteligentný dom. SMART HOME SYSTÉMY [online]. [cit. 2024-02-26]. Dostupné na: <https://www.homesystem.sk/inteligentny-dom.html>.
- [9] SUNDMAEKER, Harald, Patrick GUILLEMIN, Peter FRIESS a Sylvie WOELFFLÉ. Vision and Challenges for Realizing the Internet of Things [online]. 2010, p. 52. ISBN 978-92-79-15088-3.
- [10] BUI, Nicola a Michele ZORZI. Health care applications: A solution based on the Internet of Things. ACM International Conference Proceeding Series [online]. 2011, vol. 1, p. 1-5. ISBN 78-1-4503-0913-4.
- [11] YIN, Yuehong, Yan ZENG, Xing CHEN a Yuanjie FAN. The internet of things in healthcare: An overview, *Journal of Industrial Information Integration* [online]. 2016, vol. 1, p. 3-13. ISSN 2452-414X.
- [12] IoT in Healthcare: applications, benefits & Challenges. *Peerbits* [online]. [cit. 2024-02-26]. Dostupné na: <https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html>.

- [13] Základné prvky Industry 4.0, Digitalizácia, Smart Factory. *Industry 4.0* [online]. [cit. 2024-02-26]. Dostupné na: <https://industry4.sk/o-industry-4-0/principy/>.
- [14] KHAN, Nawab, Ram L. RAY, Ghulam Raza SARGANI, Muhammad IHTISHAM, Muhammad KHAYYAM a Sohaib ISMAIL. Current Progress and Future Prospects of Agriculture Technology: Gateway to Sustainable Agriculture. *Sustainability* [online]. 2021, vol. 13(9), p. 1-31. ISSN 2071-1050.
- [15] MEHRAVARI, N. Performance and protocol improvements for very high speed optical fiber local area networks using a passive star topology. *Journal of Lightwave Technology*. 1990, vol. 8, no. 4, p. 520–530. ISSN 0733-8724.
- [16] BANDARA, Tanushi. Tree Topology And Mesh Topology. *Medium* [online]. [cit. 2024-02-27]. Dostupné na: <https://blog.bugzero.io/tree-topology-and-mesh-topology-f73f6b720ef3>.
- [17] Mesh Model. *Bluetooth® Technology Website* [online]. [cit. 2024-02-29]. Dostupné na: <https://www.bluetooth.com/specifications/specs/mesh-model-1-0-1/>.
- [18] IoT konektivita - Poskytujeme špičkovú bezdrôtovú komunikáciu pre pripojenie vašich zariadení na internet. Získajte kontrolu nad svojimi zariadeniami vďaka NB-IoT alebo M2M Universal. - Telekom [online]. [cit. 2024-03-01]. Dostupné na: <https://www.telekom.sk/biznis/iot-konektivita>.
- [19] *Getting to 5G: Comparing 4G and 5G System Requirements* - Qorvo [online]. [vid. 2024-02-29]. Dostupné na: <https://www.qorvo.com/design-hub/blog/https://www.qorvo.com/design-hub/blog/getting-to-5g-comparing-4g-and-5g-system-requirements>.
- [20] POPOVSKI, Petar. Ultra-Reliable Communication in 5G Wireless Systems. 1st International Conference on 5G for Ubiquitous Connectivity [online]. 2014, p. 146-151. ISBN 978-1-6319-0055-6.
- [21] IKPEHAI, Augustine, Bamidele ADEBISI, Khaled RABIE, Kelvin ANOH, Ruth ANDE, Mohammad HAMMOUDEH, Haris GACANIN a Uche MBANASO. Low-Power Wide Area Network Technologies for Internet-of-Things: A Comparative Review. (*IEEE Internet of Things Journal*) [online]. 2019, vol. 6, no. 2, p. 2225-2240. ISSN 2327-4662
- [22] STERNHOFF, Johan, LTE-M vs NB-IoT – A Guide Exploring the Differences between LTE-M and NB-IoT. *Telenor IoT* [online]. [cit. 2024-02-29]. Dostupné na: <https://iot.telenor.com/iot-insights/lte-m-vs-nb-iot-guide-differences/>.

- [23] Specification # 22.368 [online]. [cit. 2024-02-03]. Dostupné na: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=645>.
- [24] PH.D, Anna Ukovich. NB-IoT Explained: What Is It, and How Does It Work? *Telit Cinterion* [online]. [cit. 2024-02-29]. Dostupné na: <https://www.telit.com/blog/nb-iot-new-cellular-standard-means-business/>.
- [25] DING, Jie, Mahyar NEMATİ, Chathurika RANAWEERA a Jinho CHOI. IoT Connectivity Technologies and Applications: A Survey. *IEEE Access* [online]. 2020, vol. 8, p. 67646-67673. ISSN 2169-3536.
- [26] CHERUVU, Sunil, Anil KUMAR, Ned SMITH a Wheeler DAVID. Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment. *Apress* [online], 2020, p. 370-395. ISBN 978-1-4842-2895-1.
- [27] WOOLLEY, Martin. Bluetooth Core Specification, Bluetooth® Technology [online], [cit. 2024-02-29]. Dostupné na: https://www.bluetooth.com/wp-content/uploads/Files/Specification/1901_Feature_Overview_Brief_FINAL.pdf.
- [28] DARROUDI, Seyed Mahdi a Carles GOMEZ. Bluetooth Low Energy Mesh Networks: A Survey. *Sensors* [online]. 2017, vol. 17, p. 1-17. ISSN 1424-8220.
- [29] *m5-docs* [online]. [cit. 2024-03-03]. Dostupné na: https://docs.m5stack.com/en/unit/timercam_x?ref=langship.
- [30] Arduino Optical Fingerprint Sensor (AS608). *Maker Portal* [online]. [cit. 2024-03-03]. Dostupné na: <https://makersportal.com/blog/2019/6/9/arduino-optical-fingerprint-sensor-as608>.
- [31] F. Schroff, D. Kalenichenko and J. Philbin. FaceNet: A unified embedding for face recognition and clustering. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) [online]. 2015, p. 815-823. ISBN 978-1-4673-6964-0
- [32] KING, Davis E. *davisking/dlib-models* [online]. C++. [cit. 2024-03-26]. Dostupné na: <https://github.com/davisking/dlib-models>.

ČESTNÉ VYHLÁSENIE

Vyhlasujem, že som zadanú bakalársku prácu vypracoval samostatne, pod odborným vedením vedúceho bakalárskej práce Jarinová Darina, Ing. PhD. a používal som len literatúru uvedenú v práci.

V Žiline dňa 5. mája 2024

Luboš Prekop.

PRÍLOHOVÁ ČASŤ

ZOZNAM PRÍLOH

Príloha A: Obsah priloženého CD	I
Príloha B: Monitoring_IoT_System_GitHub	II

PRÍLOHA A: OBSAH PRILOŽENÉHO USB

Na priloženom USB sa nachádza priečinok s názvom Lubos_Prekop v ktorom sa nachádzajú:

- Priečinok Esp32_fingerprint_ARDUINO obsahuje esp32_fingerprint.ino skript, potrebné knižnice a ďalšie súbory, ktoré sú potrebné pre správne fungovanie skriptu. Okrem toho obsahuje aj instruction.txt, ktorý poskytuje podrobné inštrukcie na nastavenie a použitie skriptu.
- Priečinok monitoring_environment_ARDUINO, ktorý obsahuje skript monitoring_environment.ino, potrebné knižnice a ďalšie súbory, ktoré sú potrebné pre správne fungovanie skriptu. Okrem toho obsahuje aj instruction.txt, ktorý poskytuje podrobné inštrukcie na nastavenie a použitie skriptu.
- Priečinok DELETEDFINGER, ktorý obsahuje skript DELETEDFINGER.ino, ktorý je nutný prípade vymazania ID odtlačkov prstov z pamäte AS608 a textový súbor instruction.txt, ktorý poskytuje podrobné inštrukcie na nastavenie a použitie skriptu. Subor Delete_fingerprint_GUI.py skript na jednoduché odstránenie ID používateľa z databázy a odstránenie ID odtlačku prsta z pamäte AS608 vďaka jednoduchému GUI rozhraniu.
- Priečinok facedetection_PYTHON, ktorý obsahuje python skripty:
 - Registration.py, skript na registráciu používateľa (snímky tvári, odtlačky prsta)
 - Extraction_into_database.py, skript na spracovanie a evidenciu používateľa do databázy.
 - Real_time_attendance_system.py, skript na prihlásenie používateľov v reálnom čase do dochádzkového systému.
 - Instruction.txt, textový súbor pre ktorý poskytuje podrobné inštrukcie na nastavenie a použitie komplexného dochádzkového systému.
- Instructions.txt textový súbor sú zahrnuté pokyny o spustení IoT monitorovacieho systému a ďalšie podrobnosti o jeho použití.
- Bakalárska práca vo formáte MS WORD (Lubos_Prekop.docx)

PRÍLOHA B: MONITORING_IOT_SYSTEM_GITHUB

https://github.com/Lubos229/MONITORING_IOT_SYSTEM. Tento odkaz vedie k elektronickej verzii všetkých súborov, ktoré sú obsiahnuté na priloženom USB. Vďaka tejto forme je možné pristupovať k vytvoreným skriptom a stiahnuť ich prostredníctvom internetu. Na tomto mieste sú dostupné inštrukcie vytvorené v slovenskej aj anglickej verzii.