ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA ELEKTROTECHNICKÁ

KATEDRA MIKROELEKTRONIKY

MODEL ZABEZPEČOVACÍHO SYSTÉMU ŘÍZENÝ KONTROLÉREM S VYUŽITÍM V IOT

SECURITY SYSTÉM CONTROLLED BY A CONTROLLER WITH USE IN IOT

DIPLOMOVÁ PRÁCE

JAKUB DRBOHLAV

Studijní program: Inteligentní budovy

Vedoucí diplomové práce: prof. Ing. Miroslav Husák, CSc.

Praha 2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Drbohlav** Jméno: **Jakub** Osobní číslo: **474621**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra měření**

Studijní program: **Inteligentní budovy**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Zabezpečovacího systému řízený kontrolérem s využitím v IoT

Název diplomové práce anglicky:

Security System Controlled by a Controller with Use in IoT

Pokyny pro vypracování:

1. Proveďte rešerši současného stavu řešení elektronických zabezpečení (EZS) rodinných domů z hlediska zpracování a ukládání dat, používaných senzorů a aktuátorů a IoT aplikací.
2. Navrhněte a realizujte jednoduchý model IoT systému pro řízení a zpracování dat elektronického zabezpečení rodinného domu řízeného vhodným typem kontroléru, např. Raspberry Pi. V návrhu použijte vybrané typy zabezpečovacích senzorů (typicky magnetický kontaktní, senzor tříštění skla, PIR/mikrovlnný senzor pohybu, vstup z IP kamery pro rozpoznání objektu apod.) a vhodné akční výstupy (typicky akustický, vhodný komunikační standard pro odesílání dat, např. na mobilní telefon).
3. Zjistěte parametry navrženého systému a porovnejte s parametry komerčních systémů. Proveďte ekonomickou úvahu pro výrobu navrženého systému.

Seznam doporučené literatury:

1. Raspberry Pi Documentation. https://www.raspberrypi.com/documentation/computers/.
2. MQTT -univerzální protokol pro cloudové a IoT aplikace. HW Group. https://www.hw-group.com/cs/podpora/mqtt-univerzalni-protokol-pro-cloudove-a-iot-aplikace#:~:text=Protokol%2C%20určený%20především%20pro%20senzorové,je%20optimální%20pro%20IoT%20aplikac
3. Co je MQTT a k čemu slouží ve IoT? Popis protokolu MQTT. ipc2U. https://ipc2u.cz/blogs/news/mqtt-protokol
4. IoT Device Development. Arm MBED [online]. c2022, https://www.mbed.com/en/

Jméno a pracoviště vedoucí(ho) diplomové práce:

prof. Ing. Miroslav Husák, CSc. katedra mikroelektroniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **15.02.2024** Termín odevzdání diplomové práce: **24.05.2024**

Platnost zadání diplomové práce: **21.09.2025**

prof. Ing. Miroslav Husák, CSc. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Mgr. Petr Páta, Ph.D. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

. | Datum převzetí zadání

Podpis studenta

Anotace

Cílem diplomové práce je zhotovení funkčního modelu elektronického zabezpečovacího systému pro byt či dům. V práci jsou popsány vybrané komerčně dostupné produkty a vhodné komunikační protokoly. Model je realizován s využitím minipočítače Raspberry Pi jako ústředny celého systému a USB analyzátoru packetů pro zajištění komunikace s bezdrátovými senzory. Kontrolér využívá ke komunikaci s jednotlivými prvky protokoly Zigbee a wifi. Model navrženého systému zajišťuje, kromě základních funkcí, také pořízení a zpracování obrazového záznamu pomocí IP kamery. Obsluha zabezpečovacího systému je realizována prostřednictvím webového rozhraní a součástí systému je volba zasílání příslušných notifikací pomocí emailu a SMS zprávy prostřednictvím GSM modulu a vložené SIM karty.

Annotation

The goal of this Diploma thesis is creation of a functional model of electronical security system for homes. This thesis contains a description of select few comercially available products and usable comunication protocols. Model is made using mini computer Raspberry Pi as a central unit of the system and USB packet sniffer which allows a comunication with wireless sensors. The resulting controller and system uses Zigbee and Wifi protocols for comunication with other devices. This model also offers a posibility of recording and processing of images in case of intrusion in the secured area. Manipulation of the system is possible using built-in web interface and receiving notifications is prepared using emails or SMS messages through GSM module and prepaid SIM card.

Klíčová slova

model zabezpečovacího systému, Raspberry Pi, Zigbee protokol, IoT, bezdrátové senzory, IP kamera

Keywords

security system model, Raspberry Pi, zigbee protocol, IoT, wireless sensors, IP cam

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V praze dne ……

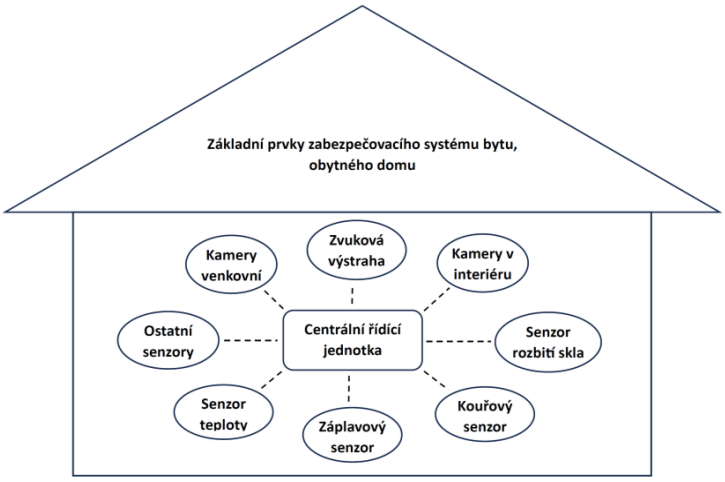
Obsah

Seznam obrázku

Seznam tabulek

Úvod

V dnešním, rychle se rozvíjejícím a technologiemi naplněném světě je zajištění bezpečnosti našich domovů stále větší a větší starostí. Současný rychlý rozvoj elektroniky vede k tvorbě mnoha více či méně sofistikovaných systémů zabezpečení našich objektů. Různé společnosti tyto systémy vyvíjí se zaměřením například na přímé zabránění k nedovolenému vniknutí do objektu, k detekování nestandardních situací, hrozeb a k odhalování bezpečnostních rizik. Tyto systémy by měly uživatelům domovů poskytnout především pocit pohody a bezpečí. Typicky se tyto systémy skládají z několika částí, jednak celý systém zahrnuje centrální řídicí jednotku s některým z mnoha typů mikrokontrolérů a menší či větší počet různých senzorů pohybu, teploty, kontaktních senzorů, kamerových senzorů apod. Komunikace centrální jednotky a všech senzorů je v současné době realizována převážně některým z bezdrátových systémů prostřednictvím wifi, ZigBee, Z-Wave, atp. Výchozí konfigurace může být uživatelem dále rozšiřována instalací dalších senzorů dle aktuálních požadavků. Centrální jednotka na základě aplikačního software snímá a vyhodnocuje signály ze všech senzorů a následně aktivuje příslušné akční prvky systému, notifikace email, SMS, zvukové sirény atd. Na Obrázek 1 je vidět jednoduchý diagram pro představu, jak takový systém může vypadat.



Obrázek 1 diagram pro znázornění zabezpečovacího systému bytu

Integrace bezdrátových technologií dále umožňuje rozšiřovat tyto systémy a zajišťovat tak jednoduchost instalace s bezproblémovou komunikací mezi jednotlivými prvky.

Z velkého množství mikrokontrolérů a minipočítačů je ve velké oblibě populární minipočítač Raspberry Pi, cenově dostupný a všestranný počítač o velikosti kreditní karty, a to především pro oblast DIY projektů, ale je oblíben i mezi profesionály díky svému potenciálu využití a množství realizovaných aplikací. Vzhledem ke konektivitě, kterou nabízí, a k jednoduchosti implementace, je Raspberry Pi jedním z vhodných prostředků pro realizaci řídicí centrály v bezdrátovém systému s využitím různých senzorů a akčních prvků. To nám umožňuje vytvořit cenově dostupné a na míru šité systémy podle potřeb majitele domu a jeho obyvatel.

Tato práce má za cíl zmapovat možnosti implementace zabezpečení domu pomocí bezdrátového systému a řídicí centrály realizované pomocí minipočítače Raspberry Pi. V následujících kapitolách jsou popsány různé bezdrátové sítě, které se v dnešní době k těmto účelům využívají, jsou zmíněny jejich výhody a nevýhody s popisem vhodných protokolů. Zároveň jsou pro daný protokol popsané příklady komerčně dostupných řídicích centrál příslušných systémů na současném trhu. Na základě analýzy jednotlivých systémů je dále popsán a navržen model systému, který bude zahrnovat 5 ks vstupních zařízení, 1 ks výstupního prvku a možnosti pro nastavení zasílání notifikací danému uživateli (email, notifikace v mobilu nebo alarm). Nedílnou součástí je ukládání získaných dat do databáze pro případné další zpracování.

1 Elektronické zabezpečovací systémy a jejich současný stav

Obecně si zabezpečovací systémy v obytných budovách kladou za cíl chránit jak osoby obývající daný objekt, tak i majetek, který se zde nachází. Konkrétně mohou chránit například před neoprávněným vniknutím dalších osob, před požárem, při porušení vodovodního potrubí apod. a posílat notifikace na uživatele objektu, případně na bezpečnostní agenturu.

1.1 Zabezpečení bytu, domu

Jednou z vlastností instalovaného zabezpečovacího systému v bytě nebo rodinném domě je samotný efekt viditelných prvků, například různých kamer. Už to samo o sobě slouží jako prevence a výstraha pro nezvané hosty tím, že mohou odradit ty, jenž měli v úmyslu nějakým způsobem poškodit hlídaný objekt nebo jeho majitele. Jako nejjednodušší a také nejlevnější slouží pro tyto účely různé atrapy bezpečnostních kamer, kdy s minimální investicí můžeme předejít několikanásobně vyšším škodám.

Vhodně navržený systém dokáže včas detekovat bezpečnostní rizika jako například možnost vzniku požáru, poškození interiéru tekoucí vodou nebo okamžitě zaznamená rozbití okna v případě násilného vniknutí do střeženého objektu. Majitele také může varovat v případě jeho nepřítomnosti na zapomenuté otevřené okno či dveře.

V takovém případě, kdy systém detekuje jakýkoliv problém v objektu, by měl být schopen zaslat majiteli nebo oprávněné osobě notifikaci ve formě e-mailové nebo SMS zprávy nebo upozornit okolí. K tomu může sloužit například aktivace sirény alarmu, který je součástí celého systému. Už tato zvuková výstraha může v některých případech zabránit v pokračování trestné činnosti a vetřelce od dalšího postupu odradit.

Instalovaný zabezpečovací systém pracuje s velkým množstvím různých dat ať již interních systémových, tak především dat ze všech senzorů, kamer a vyhodnocených anomálií. Proto musí být schopen tato data zaznamenat a ukládat

na definované místo podle volby uživatele. K tomuto účelu je možné využít ukládání do databáze spolu s kamerovými záznamy jednak na lokální datové úložiště nebo lépe na cloudové úložiště. Lokálně ukládaná data mohou být při případném incidentu poškozena nebo zcizena. Tato data je možné případně poskytnout při vyšetřování vzniklé události, a tímto způsobem zvýšit šance na případné odškodnění. Zároveň některé pojišťovny v případě uzavírání pojistných smluv zohledňují instalaci zabezpečovacích systémů.

Zabezpečovací systémy se převážně skládají z řídicí jednotky, centrály, která v prvé řadě zpracovává signály ze všech senzorů, vyhodnocuje je na základě interního programu, aktivuje výstupy a zároveň zprostředkovává komunikaci uživatele se systémem. Další nedílnou součástí systému jsou senzory odpovídající zadaným požadavkům, které monitorují celý objekt a poskytují systému vstupní data pro vyhodnocení aktuální situace v objektu. Poslední částí systému jsou akční prvky, nebo výstupní zařízení, která dokáží aktivovat příslušný výstup, vyslat signál nebo upozornit okolí například zvukem sirény.

1.1.1 Centrální prvek, řídicí jednotka

Jedná se o hlavní součást systému, dá se říci i „mozek“, protože zajišťuje funkčnost samotného systému jako celku a poskytuje uživateli možnost daný systém optimalizovat, aby mohl následně samostatně vyhodnocovat aktuální situaci. Řídicí jednotky mají často i vlastní interní paměť, která umožňuje ukládání uživatelského nastavení a zároveň také aktuálně naměřených dat.

Zajišťuje komunikaci instalovaného systému s okolím prostřednictvím daného komunikačního protokolu ať už bezdrátově nebo po kabelu, umožňuje připojit i další periferie, a tak rozšířit funkčnost celého systému.

Komunikace uživatele s instalovaným systémem může probíhat následujícími způsoby:

- Webové rozhraní a aplikace – uživatel pomocí mobilního telefonu či počítače dokáže ovládat systém po internetu nebo v rámci lokální sítě
- GSM modul – umožňuje ovládání a upozornění pomocí mobilního telefonu, například pomocí hovoru či SMS zprávy, v případě, kdy není k dispozici internetové připojení

- Klávesnice – umožňuje například zadat přístupový kód k zámku
- Vzdálený přístup k příkazové řádce systému, například SSH
- Komunikátor využívající IR záření či RF technologie

1.1.2 Vstupní zařízení

Aby mohl zabezpečovací systém spolehlivě plnit zamýšlenou funkci dle našich představ, potřebuje odpovídající vstupní data, signály. K tomu slouží různé senzory, které jsou připojené k řídicí jednotce a buď v pravidelných intervalech, nebo v případě změny stavu, posílají potřebná data.

Mezi základní vstupní zařízení pro zabezpečení bytových prostor patří:

- Detektory pohybu
    - Detekují přítomnost, pohyb osob v zorném poli pohybového senzoru, v domácím prostředí se nejčastěji využívají senzory typu PIR (Passive Infra-Red) detektory, k dalším patří např. IR, dále mikrovlnné a ultrazvukové detektory
- Mechanické kontakty
    - Magnetický senzor se skládá ze dvou částí, magnetu a mechanického kontaktu, který je již léta znám, někdy od 30. let minulého století, jako jazýčkový kontakt. Díky své jednoduchosti a snadné implementaci se stále používá. Ve stavu pohotovosti se do řídicí jednotky posílá stav log 0 a v případě aktivace se stav změní na log 1
    - Tyto senzory se nejčastěji využívají pro detekci otevření oken a dveří
- Detektor rozbití, tříštění skla
    - Převážně slouží k detekci vniknutí do střeženého objektu oknem, dveřmi jejich poškozením, rozbitím
    - Existují dva hlavní způsoby detekování rozbití skla
        - Prvním je senzor vibrací, který obsahuje akcelerometr a měří intenzitu vibrací, popř. změnu polohy, naklonění
        - Druhý způsob zahrnuje analýzu zvuku snímaného mikrofonem při tříštění skla

- Kamera
    - Neodmyslitelným zařízením jsou kamery, velmi často kombinované se senzorem pohybu. Slouží k monitorování prostorů uvnitř budov, popř. monitorují okolí domu. V případě detekování pohybu automaticky aktivují záznam videa na interní paměťovou kartu nebo na nějaké datové úložiště. Některé kamery dokáží vyhodnotit změny ve snímaném obraze a po překročení uživatelsky nastavené úrovně zaznamenaných změn aktivují alarm.

1.1.3 Výstupní zařízení

Výstupní zařízení umožňují systému ovlivňovat hlídané prostředí na základě uživatelova příkazu nebo automaticky dle vyhodnocených dat.

K tomu mohou sloužit zařízení jako např. reproduktory, alarmy nebo světla. V modelu bude použitý alarm, který má vestavěné LED diody pro světelné upozornění v případě spuštění.

1.2 Systémy senzorů, akčních prvků a komunikační protokoly

Existuje mnoho systémů a protokolů, na kterých dané systémy fungují. Mnohé z nich jsou komerčně dostupné a umožňují integraci dalších IoT prvků v obytných prostorech. Bohužel jsou často drahé a možnost zasáhnout do některých nastavení je omezená, a tak je uživatel limitován daným systémem.

V takovém případě se nabízí možnost vývoje a tvorby vlastního zabezpečovacího systému. Zde je ale zapotřebí brát na vědomí, že takovou možnost lze využít pouze v případě, kdy je uživatel obeznámen s programováním v některém z používaných jazyků, např. Pythonu, a rozumí logice. Dále jsou potřeba i znalosti např. minipočítače Raspberry Pi a systému Raspbian (systém založený na OS Debian) nebo některého z mnoha dalších kontrolérů. Samozřejmě je nutné být obeznámen s potřebným komunikačním protokolem, aby byla zajištěna funkčnost celého systému.

Nejčastěji používanými známými protokoly pro bezdrátovou komunikaci v podobných systémech jsou Z-Wave, Zigbee a Wi-Fi protokoly.

1.2.1 Z-Wave

Z-Wave je bezdrátový komunikační protokol navržený primárně pro automatizaci v domácnosti a funguje na frekvenci pod 1 GHz, okolo 900 MHz, čímž odpadá rušení ze strany sítí wifi. Propojení jednotlivých prvků v síti je pomocí topologie „mesh“, tím je možné přeposílat data přes jednotlivé senzory, dokud se data nedostanou k požadovanému cíli. Maximální množství prvků v jedné síti Z-Wave je 232. [27]

Velkou výhodou zmíněného protokolu je úspora energie. To je důležité hlavně pro bezdrátové senzory, které jsou primárně napájené bateriemi. Další výhodou je způsob, kterým jednotlivé prvky komunikují. A dalším kladem je i přísná certifikace Z-Wave zařízení ze strany Z-Wave Alliance, která je vyžadována u všech zařízení, která tento protokol používají. Díky tomu jsou všechna zařízení v této síti mezi sebou kompatibilní i když jsou od různých výrobců. [28]

Existuje však i pár nevýhod a hlavní z nich je přenosová rychlost, která maximálně dosahuje rychlosti 100 kb/s. Tím je nutnost omezit množství posílaných dat na minimum. Další nevýhodou je množství a cena dostupných zařízení, která protokol Z-Wave využívají například oproti protokolu Zigbee.

1.2.2 ZigBee

Podobně jako v případě Z-Wave byl tento protokol navržen pro zapojení bezdrátových zařízení a k automatizaci domácností a sběru dat ze sítě senzorů. Dalším cílem Zigbee bylo nabídnout bezdrátové připojení za nižší cenu. Komunikace probíhá jak na frekvenci 2,4 GHz, tak i na frekvencích 900 MHz v USA a 868 MHz v EU. Využití frekvencí 2,4 GHz s sebou nese i nevýhodu, že se komunikace může navzájem rušit se sítěmi Wifi a Bluetooth. Na druhou stranu velkými výhodami oproti Z-Wave jsou vyšší přenosová rychlost, která dosahuje až 250 kb/s, a podpora sítě až o 65 tisících různých zařízení. [4]

I tento protokol je vhodný pro využití hlavně u bezdrátových senzorů díky své energetické úspornosti. V tomto ohledu je v některých případech Zigbee i úspornější v porovnání se Z-Wave.

Zařízení s tímto komunikačním protokolem jsou cenově méně nákladná a je jich k dispozici více než v případě protokolu Z-Wave, jedním z důvodu a zároveň

i problémem je absence striktní certifikace. To má za důsledek stav, kdy každý výrobce si může implementaci protokolu lehce pozměnit, a ačkoliv sítě ZigBee podporují velké množství zařízení připojených najednou, tak je nutné zkontrolovat, aby jednotlivá zařízení byla mezi sebou kompatibilní.

1.2.3 Wifi

Wifi sítě jsou v dnešní době velmi rozšířené a většina mobilních zařízení je podporuje. Nespornou výhodou je rychlost přenosu, kdy Wifi sítě využívající frekvence 2,4 GHz v ideálním prostředí mohou dosahovat rychlostí až 450–600 Mb/s. Bohužel Wifi sítí je natolik, že se navzájem ruší, a tak je komunikace na větší vzdálenosti, především v hustě obydlených oblastech, často nestabilní.

Zároveň jsou zařízení využívající tento způsob komunikace náročnější, co se spotřeby energie týče, proto není tento protokol vhodný pro zařízení napájená pomocí baterií. Pro svou rychlost se však hodí například pro ovládání systému, tedy pro umožnění připojení uživatele k systému, nebo pro přenos obrazových informací z jednotlivých kamer integrovaných v daném systému.

1.3 Dostupná řešení na trhu

Vybral jsem několik příkladů dostupných systémů, které si může uživatel nainstalovat do svého bytu nebo zaplatit za jejich instalaci certifikovanými pracovníky.

1.3.1 Fibaro

Fibaro umožňuje uživatelům realizovat síť senzorů pomocí komunikačních protokolů Z-Wave, Wifi, ethernet a nově u verze Home Center 3 také Zigbee. Řídicí jednotka je dostupná ve dvou verzích, Home center 3 a Home Center 3 Lite. Obě verze fungují i offline pouze s lokální sítí s tím, že bez přístupu k internetu není k dispozici vzdálené ovládání, některé integrace s aplikacemi třetích stran a cloudové služby, avšak běžné ovládání a automatizace, která pracuje pouze s daným systémem, není nijak ovlivněna.

Mezi těmito verzemi jsou poměrně velké rozdíly jak v hardwaru, tak i softwaru. Home Center 3 podporuje Zigbee a neomezený počet scén, které umožňuji přednastavení různých prvků v systému a následně mezi těmito scénami je možné přepínat. Tato verze také umožňuje připojení až 230 zařízení. [6] [11]

Na druhou stranu Lite verze nepodporuje prozatím ZigBee periférie, maximální počet scén je omezen na 20 a k této jednotce lze připojit pouze 40 senzorů. Rozdíl je také v nákladech na pořízení, cena řídicí jednotky Home Center 3 se pohybuje okolo 10 000 – 13 000 Kč, zatímco verze Lite je výrazně levnější a uživatele přijde na cca 2 000 – 4 000 Kč. [6] [11]

Velkou výhodou obou těchto řídicích jednotek jsou tzv. lua scény umožňující uživatelům, kteří umí programovat, vytvářet skripty a scény v jazyce lua. Pro tvorbu jednoduchých scén je také možné využívat předdefinované příkazy a jejich jednoduché řazení.

1.3.2 iGET

Další možností je systém značky iGET. Ta nabízí několik různých variant, které lze použít pro vytvoření zabezpečovacího systému. Všechny jejich systémy podporují zařízení a senzory značek iGET, Philips Hue, Tuya apod. Nejlevnější variantou je iGET HOME Gateway GW1, jedná se o bránu, která umožňuje připojení kromě iGet senzorů i Zigbee zařízení do mobilní aplikace. V aplikaci je poté možné zobrazit aktuální stav jednotlivých senzorů, manuálně ovládat jednotlivá zařízení nebo nastavovat automatické akce. Náklady na tuto bránu se pohybují okolo 700 Kč. [8]

Dalším podobným produktem této značky je iGET HOME Gateway GW6, tento produkt je výkonnější, jeho součástí je i dotykový LCD displej a zároveň podporuje protokol Bluetooth 4.2. Cena se pohybuje okolo 3 600 Kč. [9]

Nakonec sem patří také iGET HOME x5. Jedná se o alarm, který je schopen fungovat samostatně nebo je opět možné ho přidat do mobilní aplikace. Součástí produktu je centrála s dotykovým displejem, PIR senzor pohybu, dva bezdrátové magnetické kontaktní senzory a dva dálkové ovladače k alarmu. Nevýhodou je, že tento systém je možné rozšířit pouze o zařízení značky iGET řady SECURITY Pxx, kde „xx“ značí číslo produktu. [10]

Všechny tři systémy k funkci potřebují připojení k internetu, kde ukládají data na cloudové úložiště a následně je poskytují skrze mobilní aplikaci uživateli. Výjimkou u této značky jsou kamerové systémy, kde iGET poskytuje zařízení, které funguje jako lokální úložiště.

1.3.3 Homey Pro

Homey Pro od společnosti Athom je všestranný systém, který byl navržen pro podporu velkého množství různých zařízení. Hlavní výhodou tohoto systému je podpora několika různých protokolů, čímž zaručuje kompatibilitu s různými výrobci i dalšími systémy. Podporuje protokoly ZigBee, Z-Wave, Bluetooth i Wifi. Podporuje také i méně známé protokoly Matter a Thread. Cena za Homey Pro se pohybuje okolo 400 USD. [5] [6]

Nevýhodou tohoto systému je absence ethernetového portu, tudíž bez dokoupení USB adaptéru může být připojení přes wifi při slabém signálu nestabilní. Avšak to nemá žádný vliv na funkci, jelikož Homey Pro je schopné fungovat i bez přístupu k internetu pouze s lokální sítí díky internímu úložišti. [5] [6]

Nabízí se zde i levnější varianta Homey Bridge, která stojí oproti verzi Pro pouhých 70 USD. Avšak tato varianta poskytuje pouze možnost propojení senzorů a aplikace. Nepodporuje nejnovější protokoly Matter a Thread a zároveň chybí podpora psaní vlastních skriptů a užití komunitních aplikací. Další nevýhodou je omezené množství zařízení. Pokud uživatel chce zapojit více jak 5 zařízení k systému Homey, musí platit předplatné ve výši 3 USD. Další velkou nevýhodou je potřeba internetového připojení k funkci zařízení, jelikož všechna data, jejich zpracování a automatizace akcí se provádí na vzdáleném serveru. [6]

1.3.4 Jablotron

Pro porovnání je tu uvedena i česká firma Jablotron. Ta nabízí velmi robustní zabezpečovací systémy, jak drátové, tak i bezdrátové. Tyto systémy však nelze koupit přímo jako koncový uživatel a musí je instalovat pracovník s certifikací.

Firma Jablotron má k dispozici startovní sady, které lze dle potřeby rozšiřovat dalšími zařízeními. [7]

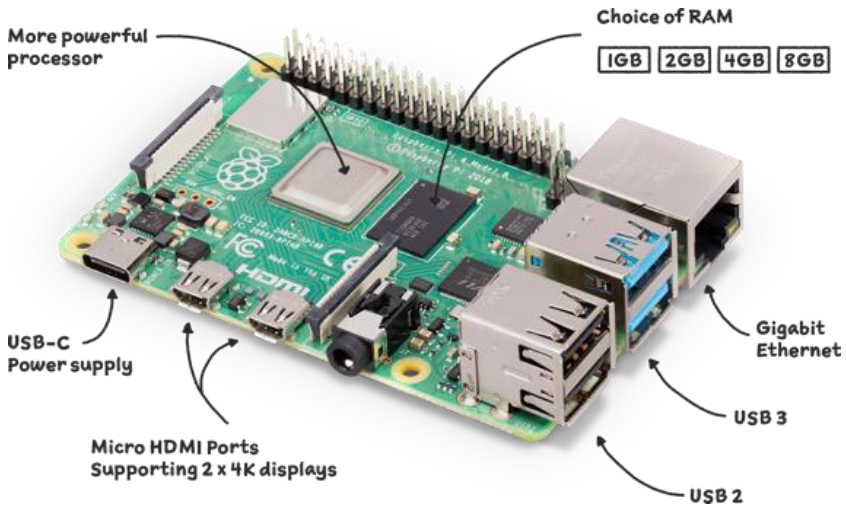
Avšak s kvalitou a spolehlivostí stoupá i cena a nejlevnější sada pro malý byt, včetně montáže, se pohybuje okolo 24 000 Kč. Tato sada obsahuje centrálu s LAN, GSM a rádiovým modulem, 1 magnetický detektor kontaktu, 1 PIR detektor pohybu, bezdrátovou sirénu a přístupový modul s klávesnicí a čtečkou RFID. [7]

Jablotron alarmy mají i interní úložiště realizované pomocí micro SD karty. Díky tomu jsou schopny ukládat veškeré události a data lokálně a nejsou závislé na internetovém připojení. Internetové připojení se používá převážně pro vzdálený přístup a monitorování. [12]

Systém v základní verzi nepodporuje žádné bezdrátové protokoly, které se běžně používají. Avšak pro verze systému Jablotron 100+ existuje zařízení Jablotron SmartHub, které umožňuje propojit alarm Jablotron spolu se systémy jako je IFTTT (IF This Then That) nebo Home assistant. [13]

1.4 Systém s centrálou realizovanou za použití Raspberry Pi

Tato práce se zabývá tvorbou centrály právě pomocí minipočítače Raspberry Pi. Jak takový minipočítač vypadá je vidět na Obrázek 2.S ohledem na cenu a dostupnost jednotlivých zařízení a senzorů bude v práci zajištěna konektivita po síti Zigbee pomocí USB analyzátorů packetů fungujícím na Zigbee síti. Lze však připojit i jiná zařízení, jelikož Raspberry Pi disponuje možností připojení na lokální síť pomocí kabelu a wifi nebo připojení dalších periférií pomocí protokolu Bluetooth. Připojení k síti umožňuje použití IP kamery a sběru obrazových dat bez jakýchkoliv dalších hardwarových požadavků.



Obrázek 2 Raspberry Pi 4 [14]

Toto řešení s sebou přináší mnoho výhod při tvorbě zabezpečovacího systému, ale má i své nevýhody.

Mezi výhody patří:

- Cena
    - Raspberry Pi je malý, cenově dostupný a plnohodnotný počítač, cena se pohybuje okolo 1 200 – 1 400 Kč pro verzi 4 a 1 600 – 2 200 Kč pro novější a výkonnější verzi 5.
- Systém šitý na míru
    - Na Raspberry Pi běží plnohodnotný systém Raspbian, který je postavený na linuxové distribuci Debian. Tím umožňuje uživateli vytvořit systém dle svých přání a zároveň použít tento minipočítač i k jiným úkonům než jen zabezpečovací systém. Raspberry Pi lze použít i pro vytvoření lokálního úložiště, tudíž umožňuje data ukládat pouze lokálně bez potřeby internetového připojení.
- Rozsáhlá a velmi aktivní komunita
- Konektivita
    - Podpora Bluetooth a wifi protokolů již v základu, ale zároveň možnost rozšířit způsoby připojení např. pomocí USB zařízení pro zprovoznění dalších protokolů jako například Zigbee pomocí USB analyzátoru packetů CC2531 nebo CC2652P nebo Z-Wave.

Na druhou stranu mezi nevýhody patří například:

- Nutné technické znalosti
    - Uživatel nebo tvůrce takového systému musí počítat s tím, že se mohou vyskytnou problémy, které musí vyřešit. K tomu je často zapotřebí umět programovat v jazyce, ve kterém je systém psán, a rozumět elektronice a komunikaci mezi senzory, centrálou a softwarem samotným. V případě absence těchto dovedností může být pro běžného uživatele obtížné spravovat daný systém bez podrobného manuálu a návodů.
- Absence servisu a podpory
    - Pokud je systém tzv. DIY (Do It Yourself – Udělej si sám), pravděpodobně nebude k dispozici oficiální podpora. V tom případě musí uživatel problémy řešit sám nebo se obrátit na komunitu okolo Raspberry Pi projektů.

Pro správný chod systému a možnou analýzu naměřených dat je nutné definovat i odpovídající úložiště, kam může centrála přistupovat a ukládat data a aktivitu zaznamenanou senzory. K tomu může sloužit například databáze. Ale vzhledem k tomu, že jediné úložiště, které Raspberry Pi v základu poskytuje, je micro SD karta, je vhodné do systému zahrnout i externí disk. Důvodem je kapacita a rychlost, kdy například při používání IP kamery může poměrně rychle ubývat místo pro data, tudíž by se tato data musela mazat a přepisovat, a tím by se SD kartě zkracovala životnost. Kromě integrování externího disku je možné využít i síťové úložiště NAS, kam by se data ukládala, spolu s databází, která by běžela na jiném zařízení v síti. Je dobré ale myslet na to, aby všechny tyto komunikace probíhaly pouze po lokální síti, aby výsledný systém nebyl závislý na internetovém připojení, a tak i zranitelný.

2 Model zabezpečovacího systému

Předmětem této práce je návrh zabezpečovacího systému a realizace funkčního modelu. Systém musí být schopen komunikovat se všemi připojenými senzory a akčními prvky, musí umět spolehlivě uložit data do databáze pro pozdější použití. Dále musí správně vyhodnotit vstupní data a posoudit situaci v hlídaném objektu. Následně musí, vhodnou a spolehlivou formou komunikace, poslat upozornění uživateli v případě, že nastala nějaká nestandardní situace, například rozbití okna, pohyb v bytě atd. Komunikace centrální jednotky a jednotlivých senzorů bude realizována pomocí protokolu ZigBee.

2.1 HW Komponenty

Řídicí jednotku zabezpečovacího systému tvoří minipočítač Raspberry Pi, konkrétně verze 4 B s pamětí RAM o velikosti 4 GB. Vzhledem k tomu, že Raspberry Pi samotné neumí komunikovat a zprostředkovávat komunikaci v síti ZigBee, je ve finální verzi modelu použitý externí analyzátor packetů SONOFF Zigbee 3.0 USB Dongle Plus, který funguje na čipu CC2652P od firmy Texas Instruments.

Pro celistvost systému je potřeba připojit i samotné senzory a akční prvky. Realizovaný model bude obsahovat celkem 7 vstupních zařízení a 1 výstupní. Pro ilustraci, jak takové senzory vypadají, je možné na Obrázek 3 vidět jednotlivé senzory, které byly vybrány pro realizaci modelu zabezpečovacího systému.

Obrázek 3 Vybrané senzory pro model zabezpečovacího systému, zleva Aqara vibration sensor, Magnetický kontaktní senzor SNZB-04, PIR senzor SNZB-03 [32][33][34]

Systém je také možné rozšířit o další typy ZigBee zařízení, popř. naprogramovat vlastní. Avšak každý typ musí být ručně definován v souboru „devices.py“. Hlavním důvodem jsou odchylky v implementacích ZigBee protokolu u různých výrobců.

V souboru je vytvořena obecná třída pro senzor se všemi potřebným funkcemi, ze které další konkrétní typy senzorů mohou dědit a tím je jejich definice mnohem jednodušší. Důležité je hlavně definovat název, model, výrobce a formát, ve kterém zařízení vrací data.

2.1.1 Analyzátory packetů

CC2531

CC2561 je tvořen mikrokontrolérem, RF vysílačem a přijímačem. Je vhodný pro aplikace využívající standard IEEE 802.15.4, ZigBee a RF4CE, a právě z tohoto důvodu a díky své cenové dostupnosti byl použitý pro první verzi modelu. Dalšími výhodami je rozhraní USB pro připojení k PC a Raspberry Pi a možnost přehrávání firmwaru pomoci CC debugeru nebo GPIO pinů na Raspberry Pi. Pro představu, jak takové zařízení vypadá, je zde Obrázek 4. Na obrázku jsou také vidět jednotlivé piny na pravé straně desky s plošnými spoji, které se používají pro propojení s Raspberry Pi v případě nahrávání nového firmwaru. [15]

Obrázek 4 USB analyzátor packetů s CC2531 [29]

Bohužel se jedná o starší verzi a podpora novějšího standardu ZigBee verze 3 je omezená. Při testování beta verze firmwaru, která údajně podporuje verzi 3, se choval přijímač nestabilně a neustále zamrzal (v průměru 2x denně). Proto lze říci, že spolehlivě podporuje pouze ZigBee do verze 1.2. To v tomto případě není tak velký problém, protože ZigBee 3 je zpětně kompatibilní.

SONOFF Zigbee 3.0 USB Dongle Plus (ZBDongle-P)

V konečné verzi modelu je však nakonec použitý novější přijímač, a to sice SONOFF ZigBee 3.0 USB Dongle Plus, který je postaven na čipu CC2652P od firmy Texas Instruments. Tato změna s sebou přinesla několik výhod:

- Nativní podpora verze ZigBee 3 bez nutnosti beta verze firmwaru
    - To zajistilo značné zlepšení stability, kde systém přestal zamrzat a nebylo ho z tohoto důvodu již nadále potřeba restartovat
- Možnost přehrání firmwaru přímo přes USB
    - Není nutné propojit debugovací piny s GPIO piny Raspberry Pi. Tato možnost je vhodná zejména z toho důvodu, že oficiální verze firmwaru, se kterým je zařízení dodáváno, má jisté limity, které omezují výkon zařízení.
- Vyšší úroveň signálu
    - Novější přijímač obsahuje externí anténu, jak lze vidět na Obrázek 5, která zajišťuje lepší pokrytí signálem, na rozdíl od integrované antény na PCB u přijímače s CC2531.
- Stabilita a spolehlivost

Obrázek 5 Sonoff Zigbee 3.0 USB Dongle Plus [30]

Obecně je novější varianta i vhodnější pro realizaci rozsáhlejších sítí, na rozdíl od CC2531, které bylo schopné podporovat síť pouze o velikosti cca 20 zařízení. Tento model v základní verzi s původním firmwarem dokáže napřímo připojit až 21

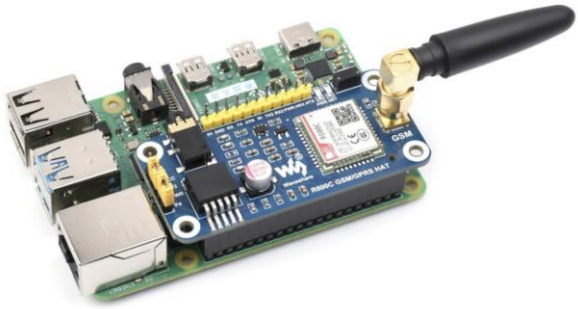
zařízení s možností propojení v síti až 40 připojených zařízení. To lze pomocí nové verze firmwaru navýšit na 50 přímých připojení a až 200 zařízení v celé síti. [16]

2.1.2 GSM Modul

Další součástí je GSM modul Waveshare R800C GSM/GPRS Hat. Ten umožňuje připojení SIM karty a následnou komunikaci po sítích 2G, 3G a LTE.

Pro ovládání modulu se používá sériová komunikace přes GPIO piny. K dispozici je zasílání a přijímání SMS zpráv i hovorů.

Na Obrázek 6 je vidět jak Raspberry Pi, tak i GSM modul, který je díky nasazení na všechny piny poměrně kompaktní a pevně usazený, díky tomu nehrozí riziko nechtěného odpojení v případě, že by zařízení nebylo schopné posílat notifikace pomoci SMS zpráv.



Obrázek 6 GSM Modul nasazený na Raspberry Pi [35]

2.1.3 Magnetický kontaktní detektor

Tento senzor je tvořen dvěma částmi. Základní část senzoru obsahuje vysílač a zprostředkovává komunikaci s koordinátorem v ZigBee síti a zároveň dokáže detekovat přítomnost magnetu ve své blízkosti. Magnet je v tomto případě druhou částí senzoru.

Základní klidový stav senzoru je z důvodu úspory energie režim spánku. Pouze pokud se druhá část s magnetem vzdálí nebo přiblíží, tak se senzor probudí a vyšle informace o změně stavu do řídicí jednotky. Nejčastěji se tyto senzory používají pro detekci otevírání a zavírání dveří nebo oken.

V této práci je konkrétně použit senzor od společnosti SONOFF s označením SNZB-04.

2.1.4 Detektor pohybu

Dalším prvkem modelu systému je senzor detekující pohyb. Pro realizaci byl vybrán SONOFF SNZB-03, který je typu PIR (passive infra-red). Ten dokáže spolehlivě detekovat pohyb lidi a zvířat v monitorovaném prostoru.

Z funkčního hlediska se jedná o měření množství dopadajícího infračerveného záření na citlivý povrch senzoru. V klidovém stavu, kdy v zorném poli nedochází k žádnému pohybu, je přijímané IR záření senzorem téměř konstantní. V případě, kdy do snímaného prostoru vstoupí člověk či zvíře tak senzor zaznamená změnu v detekovaném množství infračerveného záření, probudí se a vyšle záznam o změně stavu do řídicí jednotky.

Pokud po krátký, definovaný časový interval neproběhne další změna, senzor opět pošle zprávu, že nedochází k detekci pohybu, a přejde do úsporného režimu spánku.

Nevýhodou PIR senzoru je, že nerozpozná, zda se v prostoru pohybuje člověk nebo zvíře. K zajištění tohoto požadavku je nutné kombinovat původní způsob detekce například s informacemi z kamerového záznamu. Dále není vhodné směrovat zorné pole senzoru na prostor s okny či radiátory. V tom případě se může stát, že senzor nahlásí „pohyb“ jen při změně teploty v případě, kdy se začne topit, větrat nebo dojde k osvitu okna slunečním zářením. Pro takové případy je vhodné kombinovat PIR senzor s jinými typy detektorů, jako například mikrovlnnými.

2.1.5 Detektor rozbití skla

Detekce tříštění skla se nejčastěji realizuje senzory, které dokáží snímat vibrace a vyhodnocovat svou polohu, nebo zaznamenávat a vyhodnocovat zvuk, který tříštění skla produkuje.

Senzory, které snímají vibrace, obsahují akcelerometr a v momentě, kdy dojde k naklonění, vibracím nebo pohybu senzoru, dokáží vzruch zaznamenat, číselně

vyjádřit sílu vzruchu nebo povahu (vibrace, pád, naklonění) a poslat informaci řídicí jednotce.

Oba dva způsoby však mají své klady a zápory. Mezi ty největší zápory patří falešné vyhodnocení tříštění skla. Z toho důvodu je vhodné tato data kombinovat a sledovat dané místo více senzory, tím je možné samotné vyhodnocení monitorování maximálně zpřesnit.

Senzor vibraci

V modelu zabezpečovacího systému je použitý senzor vibrací Aqara od společnosti Xiaomi, který umožňuje nastavení pracovní citlivosti. Tím lze do určité míry ovlivnit přesnost vyhodnocení, aby nebylo detekováno tříštění skla například při otevírání a zavírání oken nebo prosklených dveří.

V momentě, kdy senzor zaznamená vibrace, začne sledovat jejich intenzitu a 5 minut po uklidnění stavu nahlásí sílu největšího zaznamenaného otřesu. Také nahlásí povahu pohybu, zda se jedná o vibrace, pád nebo naklonění.

Tento senzor je také příkladem, jak se implementace ZigBee protokolu mohou lišit u různých výrobců. Pro spárování je nutné provést aktivaci senzoru, tedy podržení resetovacího tlačítka, i několikrát za sebou, dokud se senzor správně nenahlásí koordinátoru a nedojde k validní integraci do stávající sítě.

Senzor pro vyhodnocování hluku a klasifikaci zvuku

Senzor vibrací občas nestačí a například při bouchnutí okna při průvanu dokáže nahlásit takový záznam o vibracích, že je stav detekován jako rozbití okna. Pro tento případ je v modelu realizovaného systému použitý také senzor, který monitoruje hladinu ruchu v okolním prostoru a dokáže klasifikovat různé zvuky, včetně krátkého cinknutí a tříštění skla.

Tyto senzory však nejsou oproti senzorům vibrací tolik dostupné, z toho důvodu jsem pro jeho výrobu využil faktu, že řídicí jednotku tvoří Raspberry Pi a funkci tohoto senzoru jsem realizoval sám.

Ke zhotovení posloužil obyčejný mikrofon s dostatečným frekvenčním rozsahem. Je možné použít i směrový mikrofon, který by cíleně mířil na okna, která je nutné zabezpečit. Pro ilustraci funkce senzoru v modelu je však použitý obyčejný

všesměrový mikrofon Audio-Technica ATR4697-USB, který je připojen k Raspberry Pi pomocí rozhraní USB. Z hlediska funkce není možné sledovat pouze určité jednotlivé frekvence, jelikož zvuk generovaný rozbitím skla závisí na mnoha faktorech: materiál, tloušťka, charakter úderu a síla, která zapříčinila rozbití.

Jedna varianta pro zhotovení senzoru je sledování různých frekvenčních pásem, ve kterých se rozbití a cinkání skla pohybuje. Jakmile dojde k dostatečně hlasitému ruchu v tomto pásmu, dojde k vyhodnocení, zda-li se jedná o zvuk tvořený rozbitím skla.

V modelu zabezpečovacího systému jsem však zvolil jiné řešení. Detekce probíhá tak, že Raspberry Pi kontinuálně snímá zvuk okolí a opakovaně vytváří a ukládá krátkou zvukovou nahrávku v bezztrátovém formátu. Následně tento soubor otevře v dalším vlákně provede analýzu obsahu.

K analýze se používá strojové učení. Google ve své volně dostupné knihovně Mediapipe, kromě zpracování obrazové informace, poměrně nově implementoval klasifikaci zvuků v příslušné audionahrávce nebo datovém proudu. Pro tento účel využívá hlubokou neuronovou síť YAMNet. Dostupný model je naučen na datasetu AudioSet, a tak umožňuje pomocí naučených vzorů rozpoznat až 632 různých zvuků, mezi které patří i tříštění skla, manipulace se skleněnými předměty a vzájemné cinkání skleněných předmětů o sebe. [17] [18]

Vlákno, které zajišťuje funkci samotného senzoru, zpracovává záznam o velikosti 50 snímků. Každou nahrávku po uložení otevře, spustí nad ní klasifikaci, která vrátí seznam detekovaných zvuků a skóre vyjadřující pravdivost detekce. Seznam následně profiltruje a vybere pouze zvuky týkající se tříštění skla, a následně, dle předem nastavené prahové hodnoty, vyhodnotí, zda k tříštění opravdu došlo, nebo ne. Pokud je detekce pozitivní, předá ji k dalšímu zpracování řídicím systémem.

2.1.6 Zvukový Alarm

Jediným výstupním prvkem v modelu zabezpečovacího systému je siréna, která se na vyžádání nebo automaticky v případě zaznamenaného narušení monitorovaného prostoru či jiného problému spustí a upozorní tak okolí na detekovaný problém. Pro realizaci byla použita siréna R7051 od společností Woox.

Obrázek 7 Siréna WOOX R7051

Siréna komunikuje bezdrátově a používá protokol ZigBee. Kromě zvuku má i zabudované LED diody, pro které lze navolit intenzitu jasu a rychlost blikání, nebo v případě potřeby je možné LED diody zcela vypnout. Na Obrázek 7 je vidět reproduktor uprostřed sirény, LED diody jsou rozmístěny po zbytku celé plochy ze stejné strany. Pro zajištění funkce je nutné sirénu připojit k napájení pomocí odpovídajícího napájecího zdroje a kabelu s micro usb konektorem. Pro případ výpadku elektrické energie má vestavěnou baterii, která vydrží cca 1 den provozu. Napájení po kabelu je nutné, protože zařízení nemůže nikdy přejít do režimu spánku a musí být neustále připraveno v pohotovosti, aby mohlo kdykoliv přijímat povely k aktivaci alarmu. Samotný úkon hlasité reprodukce zvuku a blikání světel je také energeticky náročnější oproti činnosti senzorů.

2.1.7 IP Kamera

Posledním vstupním zařízením je IP kamera. Na rozdíl od ostatních připojených zařízení využívá připojení po síti LAN a nikoliv ZigBee. Důvodem je větší objem dat, které by nebylo možné přes ZigBee posílat. Na trhu je mnoho dostupných kamer, mnoho z nich však poskytuje video záběr pouze prostřednictvím aplikace výrobce. Pro potřeby této práce je nutné vybrat kameru, která poskytuje i samotný datový proud videa po síti, například pomocí protokolu RTMP, RTSP nebo ONVIF.

Pro realizaci popsaného zabezpečovacího systému jsem vybral kameru Tapo c200 od společnosti TP-Link. Hlavními důvody jsou pořizovací cena a schopnost kamery poskytnout přenos pomocí zmíněného protokolu RTSP ve dvou různých kvalitách, a to full-HD (1080p) a SD (360p). Jedinou nevýhodou je, že se kamera

musí prvotně nastavit s připojením na internet, ale poté funguje bez problému na lokální síti i bez přístupu k internetu.

Dále kamera disponuje možností nočního vidění s pomocí infračervených LED diod pro dodatečné osvětlení monitorovaného prostoru. Jedná se také o tzv. PT kameru. To znamená, že má motorizovaný pohyb v osách X a Y, tedy pohyby ve vodorovné a vertikální ose. To umožňuje systému a uživateli vzdáleně upravovat oblast monitorovaného prostoru pro záznam videa.

Kamera umožňuje také nahrávání do cloudového úložiště od firmy TP-Link. Tato funkce není ale pro funkci celého systému nutná, jelikož se nahrávky ukládají lokálně přímo z datového proudu přes RTSP.

Zpracováni obrazu

Připojení kamery k systému umožňuje obrazový záznam dále zpracovávat a rozšířit tak funkčnost celého systému. Záznam se nemusí jen ukládat, ale je možné i detekovat objekty, které se v záběru nachází. Tim lze třeba vyhodnotit, jestli byl vzruch na PIR senzoru způsoben člověkem, domácím mazlíčkem nebo je to jen falešně pozitivní zpráva.

Tento proces je však výpočetně náročný, hlavně pro zařízení jako je Raspberry Pi, které má poměrně omezený výpočetní výkon, proto není vhodný pro verzi 3 a starší, jelikož je zapotřebí, aby detekce běžela dostatečně rychle a s dostatečnou přesností v reálném čase.

Detekce běží kontinuálně, tedy v momentě, kdy se zpracuje jeden snímek, pošle systém zpracovaný snímek s vyznačenými detekovanými objekty do webového rozhraní a vezme se nový aktuální snímek z kamery a zpracuje ho. Tento způsob ovšem zanedbá veškeré snímky, které proběhly během zpracovávání, kvůli tomu sníží detekce snímkovou frekvenci videa, které uživatel vidí. Z toho důvodu má uživatel možnost detekci vypnout v nastavení systému.

V systému je implementováno několik různých druhů frameworků a modelů, které lze pro detekci použít. Díky tomu má uživatel možnost odladit a otestovat nový model v různých formátech, pokud má k dispozici vhodný dataset. Dataset je sbírka dat, ve které jsou uložené údaje o detekovaných objektech.

Faster R-CNN

Jedná se o populární způsob detekce. Průběh zpracování se skládá ze dvou fází, generování potenciálních bounding boxů okolo objektů zájmu a v druhé fázi probíhá klasifikace jednotlivých boxů a přiřazuje se jim pravděpodobnost toho, o jaký objekt se jedná. Modely tohoto typu jsou známé pro svoji přesnost, ale je to možné jen na úkor rychlosti, a proto nejsou moc vhodné pro aplikace, které fungují v reálném čase.

SSD – Single Shot Multibox Detection

V tomto přístupu se kombinují obě fáze do jedné, tedy detekce bounding boxů i klasifikace probíhají zároveň. Tento způsob je efektivnější a stále dostatečně přesný, takže je vhodnější pro aplikaci v této práci.

YOLOv8 – You Only Look Once version 8

Jedná se, podobně jako v případě SSD, o jedno fázový detektor. YOLOv8 je známé pro svoji rychlost a jednoduchost užití. Princip detekcí u tohoto frameworku je v tom, že se obraz rozdělí do mřížky a poté se detekce pustí na každou buňku v mřížce zvlášť. Nakonec proběhne NMS („non maximum suppresion“), to eliminuje překrývající se detekce a vrátí uživateli seznam detekcí.

Výhodou použití YOLOv8 je poměrně snadný proces ladění nového modelu a možný export do dalších formátů. V systému je možné použít jak základní „.pt“ PyTorch formát, tak i „.onnx“, který je optimalizovaný pro běh na CPU.

TensorFlow Lite

Nakonec jsou zde modely ve formátu TensorFlow Lite. Ty jsou odlehčenou verzí TensorFlow a jsou optimalizovány pro použití na mobilních zařízeních a zařízeních s omezeným výkonem, kam spadá i Raspberry Pi. SSD i YOLOv8 modely lze exportovat do formátu TensorFlow Lite.

Důležitou součástí je možnost kvantizace modelu. Kvantizace je proces, který za malého snížení přesnosti dokáže výrazně snížit velikost modelu a zrychlit proces detekce. To je možné snížením přesnosti čísel, které reprezentují parametry uvnitř modelu. Standardně jsou všechny parametry ve formátu typu s plovoucí řádovou čárkou o velikosti 32 bitů, tento proces je ale schopný je převést na velikost o 16

bitech nebo dokonce do celých čísel o velikosti 8 bitů. Díky tomu je možné dosáhnout vysoké snímkové frekvence s detekcí i na zařízeních jako je Raspberry Pi.

Tabulka 1 Porovnání různých modelů pro detekci objektů spuštěných na Raspberry Pi

Doba trvání detekce v 1 snímků z kamery			
Formát modelu	Max [ms]	Min [ms]	Průměr [ms]
Faster R-CNN	4415,46	1137,74	2045,63
SSD	2019,45	587,21	977,92
YOLOv8n (.pt)	2703,05	847,26	1365,16
YOLOv8n (.onnx)	2344,13	780,58	1366,40
TensorFlow Lite	227,48	140,02	153,64

Z Tabulka 1**Chyba! Nenalezen zdroj odkazů.** je patrné, že pro použití v aplikaci, kde je důležitý živý záznam z kamery, je vhodný pouze formát TensorFlow Lite díky svým optimalizacím.
U všech formátů je patrné, že některé detekce trvají mnohem déle. Důvodem je téměř konstantní vytížení CPU na 100 % jeho výkonu.

AI Akcelerátor, Google Coral USB Accelerator

Pro zlepšení a zrychlení detekce existuje tzv. AI akcelerátor, např. Coral USB Accelerator od společnosti Google. Zařízení obsahuje procesor Edge TPU, který umožňuje efektivní provádění operací spojených se strojovým učením. Dokáže provádět až 4 bilióny operací za sekundu (4 tera-operations) s maximální spotřebou energie 2 W. K Raspberry Pi ho lze připojit pomocí USB 3.0 rozhraní. [19]

Nespornou výhodou přesunutí zpracování záznamu na toto zařízení je uvolnění CPU samotného Raspberry Pi, kdy není vytížené na maximum a je tak možné ho používat i pro jiné procesy.

Pro využití je nutné do systému stáhnout knihovnu libedgetpu1, která je dostupná ve dvou verzích, „-std“ a „-max“. Verze „max“ dokáže procesor v USB akcelerátoru přetaktovat, a tak dosáhnout vyššího výkonu, ale zároveň se zvýší produkce

odpadního tepla, proto je nutné zkontrolovat, aby se při dlouhodobém užívání zařízení nepřehřívalo. [20]

Aby bylo možné modely pro detekci spustit na procesoru Edge TPU, musí být vyexportovány do speciálního formátu. To ze zmíněných formátů podporuje pouze TensorFlow Lite.

Pro ukázku jsem vybral několik různých modelů ve formátu pro Edge TPU, které jsou dostupné na webových stránkách coral.ai. Všechny modely jsou testované na datasetu COCO, který umožňuje detekci až 90 různých objektů. Vybrané modely pro otestování výkonu jsou SSD MobileNet V1, SSD MobileNet V2, SSDLite MobileDet, EfficientDet-Lite0 a EfficientDet-Lite1. [21]

Tabulka 2 Porovnání různých modelů pro detekci objektů na Edge TPU

Porovnání různých modelů pro detekci spuštěných na Edge TPU							
Model	Velikost vstupu [px]	libedgetpu1-std [ms]			libedgetpu1-max [ms]		
		Max	Min	Avg	Max	Min	Avg
MobileNet V1	640x640	828,38	470,52	528,17	545,63	429,08	479,72
MobileNet V2	300x300	58,03	21,20	24,72	46,46	18,16	20,73
MobileDet	320x320	49,93	25,47	28,04	52,07	23,07	26,25
EfficientDet -Lite0	320x320	143,70	94,40	110,36	133,48	88,70	102,46
EfficientDet -Lite1	384x384	203,69	134,66	160,89	181,05	127,26	147,60

Z dat v Tabulka 2 je patrné, že s nejmenším modelem SSD MobileNet V2 lze dosáhnout i detekci téměř 50 snímků za vteřinu. RTSP stream z kamery poskytuje 15 snímků za vteřinu. Při použití nejrychlejšího modelu je tedy dostatečná rezerva výkonu a je možné použít přesnější modely, jako například MobileDet.

2.2 Komunikace mezi Raspberry Pi a ostatními prvky systému

Jak již bylo řečeno, jednotlivé senzory i minipočítač Raspberry Pi jsou připojené do sítě ZigBee. Raspberry Pi funguje jako koordinátor sítě a následnou komunikaci převádí ze ZigBee protokolu do MQTT pomocí softwaru Zigbee2MQTT. Zprávy ze senzorů a o stavu sítě přeposílá dál a zároveň přijímá externí příkazy, které například umožňují párování dalších senzorů, přejmenování zařízení v síti nebo zapnutí alarmu.

2.2.1 MQTT – Message Queue Telemetry Transport

Jedná se o komunikační protokol, který je navržen tak, aby byl lehký a jednoduchý. Umožňuje výměnu dat mezi jednotlivými zařízeními skrze tzv. brokera. Využívá se převážně v oblasti IoT právě díky jednoduchosti implementace a možnosti přeposílání malých i velkých zpráv, a to v rozpětí od 2 bytů do 256 megabytů. [24] [25]

Mezi výhody MQTT patří:

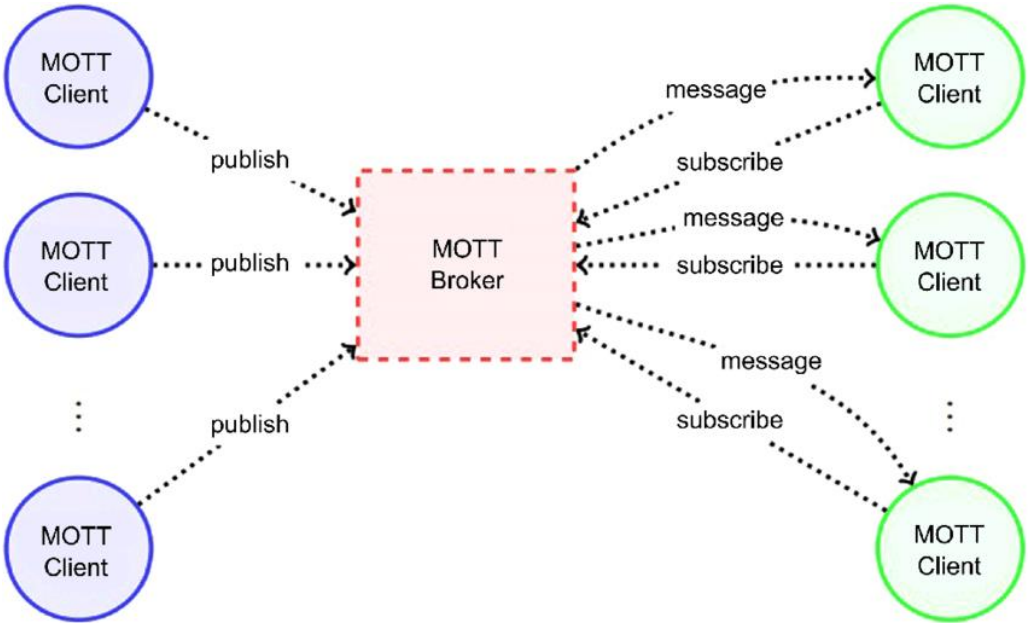
- Lehkost a jednoduchost
    - K implementaci není potřeba velký výpočetní výkon a ani příliš mnoho paměti, proto se hodí i pro malé mikrokontroléry a do sítí, kde je velmi omezená rychlost přenosu [24] [25]
- Rozšiřitelnost
    - MQTT je implementováno tak, aby co nejméně zatěžovalo zařízení, na kterém pracuje. Také umožňuje efektivně kategorizovat a rozeznávat jednotlivé zprávy a díky tomu lze k síti připojit mnoho různých zařízení a zprostředkovávat komunikaci i ve velkých sítích
- Spolehlivost
    - Tento protokol je také vhodný pro sítě, kde je omezená šířka dostupného pásma a velká latence. Díky vestavěné funkci QoS (Quality of Service) umožňuje nastavit každé zprávě její důležitost a podle toho ji i vyhodnocovat [24] [25]:
        - „QoS 0“ – odpovídá zprávě, kde odesílatel nedostane žádnou zpětnou vazbu

        - „QoS 1“ – zaručuje, že zpráva, kterou odesílatel poslal, došla příjemci alespoň jednou. Odesílatel zprávu odesílá opakovaně dokud nedostane zpět potvrzení o příjetí.
        - „QoS 2“ – v tomto případě se zajistí, aby zpráva, kterou odesílatel poslal, došla příjemci právě jednou a prošlo tak jenom jedno zpracování dané zprávy na straně příjemce. To je zaručeno procesem, kdy se pošlou 4 různé zprávy:
            - Publish – nese obsah
            - Pubrec – potvrzení o přijetí příjemcem
            - Pubrel – potvrzení o uvolnění zprávy u odesílatele
            - Pubcomp – potvrzení o zpracování příjemcem
- Bezpečnost
    - MQTT umožňuje mít naprosto otevřené sítě, kde nedochází k jakékoliv autentizaci jednotlivých členů sítě, ale zároveň umožňuje nastavit nutnost přihlášení všech uživatel a šifrování veškeré komunikace.
- Podpora
    - V dnešní době již existuje podpora tohoto protokolu v mnoha jazycích a je již vytvořeno mnoho knihoven, které je možné použít pro usnadnění implementace

Princip MQTT

MQTT funguje na principu odesílatele a odběratele. Každá zpráva obsahuje tzv. téma, které slouží k identifikaci a adresaci. Odesílatel a odběratel nejsou k sobě připojení napřímo, ale přes brokera, který je centrálním a nezbytným článkem sítě. Ten zaručuje přijetí zpráv a odeslání tam, kam zprávy patří. Vztahy mezi jednotlivými členy MQTT sítě lze vidět na

Obrázek 8. [24] [25]



Obrázek 8 Diagram znázorňující MQTT síť [31]

MQTT zprávy

Zprávy mohou být velmi krátké, jelikož samotná hlavička má pouze 8 bitů. Zbytek zprávy je tvořen daty.

Součástí dat je i téma. Témata mohou být jednoúrovňová nebo víceúrovňová a jednotlivé úrovně se od sebe oddělují pomocí znaku lomítka („/“). Příklady takových témat:

- Zigbee2mqtt/bridge/logging
- Zigbee2mqtt/Okno

Velkou výhodou pro filtrování zpráv jsou zástupné znaky „#“ a „+“, které umožňují vybrat zprávy s různými tématy v různých úrovních.

- „#“ je víceúrovňový, umožňuje tedy přijímat zprávy se všemi tématy v dané úrovni, a i všech dalších úrovních pod ní. Příklad:
  - „zigbee2mqtt/#“ umožňuje přijímat zprávy s tématem „zigbee2mqtt/okno“ i „zigbee2mqtt/bridge/logging“
- „+“ je naopak jednoúrovňový:
  - „zigbee2mqtt/+“ umožňuje přijímat zprávy s tématem „zigbee2mqtt/okno“, ale nikoli „zigbee2mqtt/bridge/logging“, jelikož téma má 3 úrovně

MQTT klient

Každý klient v síti má možnost fungovat jako odesílatel i jako odběratel. V případě, kdy chce klient odebírat zprávy od brokera, musí nahlásit seznam témat, která ho zajímají.

MQTT broker

Broker je koordinátor, který zprostředkovává komunikaci mezi všemi klienty v síti, včetně přeposílání zpráv klientům podle témat, ke kterým se přihlásily. Kromě toho slouží broker zároveň k:

- Autorizaci a ověřování MQTT klientů je-li tak síť nastavena
- Přeposílání zpráv do jiných systémů pro další zpracování
- Stará se o nedoručené zprávy a spojení s klienty
- Ukládá zprávy, které byly označené jako „persistent“ a přeposílá je všem zařízením, které se nově připojí a začnou odebírat téma, které zahrnuje právě tyto zprávy

2.2.2 Zigbee2MQTT

Jelikož se může stát, že řídicí centrály a senzory od různých výrobců nejsou kompatibilní, tak existuje open source software jako Zigbee2MQTT. Díky němu lze například k Raspberry Pi připojit jakékoliv již podporované zařízení, nebo pokud není ještě podporované, tak je možné zařízení v Zigbee2MQTT ručně nastavit a poté standardně používat.

Jedná se o aplikaci, která se chová jako brána pro síť ZigBee a používá externí přijímače jako koordinátora v síti. Díky tomu je schopný udržovat a tvořit síť senzorů.

Jednou z výhod je to, že aplikace je open source a existuje kolem ní velká komunita, která může v případě nesnází zastupovat do jisté míry i oficiální podporu, která by byla k dispozici v případě jiných řešení.

Zigbee2MQTT také podporuje velké množství různých senzorů a dalších zařízení od různých výrobců. Aktuálně podporuje přes 3580 zařízení od 430 různých výrobců a pokud uživatel narazí na zařízení, které není v danou chvíli podporováno,

může využít volně dostupného návodu na webových stránkách, aby podporu sám přidal. [22] [23]

Hlavní funkcí je obousměrné přeposílání informací mezi ZigBee sítí a MQTT sítí. Jednotlivá zařízení se ve většině případech párují naprosto totožně jak to uvádí výrobce, není tedy zapotřebí žádných složitých kroků. Pokud tomu tak však není, lze návod pro další postup najít popsaný v dokumentaci Zigbee2MQTT.

Jakmile se zařízení spáruje, systém o tom dostane zprávu a zobrazí ho ve webovém rozhraní, kde je možné s ním dále pracovat.

2.3 Požadavky na systém

Pro zprovoznění a spuštění systému je zapotřebí mít nainstalovaný nejnovější systém Raspbian. Je také nutné nainstalovat starší verzi pythonu, než se kterou se v základu systém zprovozní, a to sice 3.9. Tento krok je nezbytný, jelikož některé knihovny, které systém využívá, nejsou aktualizované pro novější verzi pythonu.

Dále se musí zapnout sériová komunikace přes piny GPIO pro připojení GSM modulu, který je na Raspberry Pi nasazený a umožňuje komunikaci při absenci internetového připojení.

Aby systém mohl správně přijímat zprávy ze ZigBee sítě a komunikovat s jednotlivými senzory, je nutné nejprve zajistit, aby v lokální síti byl k dispozici a správně nakonfigurován MQTT broker. K tomu lze využít software s názvem Mosquito, který lze také nainstalovat na Raspberry Pi. Nakonec se musí zapojit analyzátor packetů pro síť ZigBee, nahrát správný firmware, aby zařízení fungovalo jako koordinátor sítě, a nainstalovat software Zigbee2MQTT, který překládá komunikaci ze ZigBee sítě do MQTT sítě.

Aby bylo možné systém spustit, musí se také zajistit, aby byly v systému nebo virtuálním prostředí nainstalovány následující knihovny pro jazyk Python:

- ultralytics - 8.2.2
- flask - 3.0.0
- tflite - 2.10.0
- tflite-runtime - 2.7.0
- pytapo - 3.3.18
- mediapipe - 0.10.9
- pyaudio - 0.2.14
- paho-mqtt - 1.6.1

Jednotlivé knihovny jsou uvedeny i s verzí, se kterou byl systém testován. Při použití jiných verzí není zaručena funkčnost.

2.4 Funkce systému

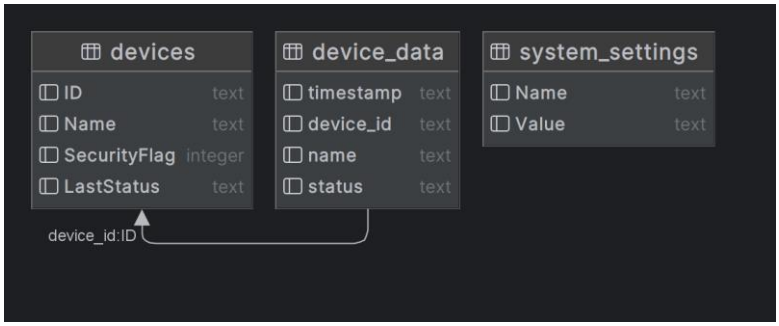
Většina systému je naprogramována v jazyce Python. Celý program běží ve 5 různých vláknech:

- Database handler – hlavní zprostředkovatel komunikace s databází, načítá nastavení při spuštění a ukládá nová data v případě, pokud jsou k dispozici
- Device handler – stará se o načítání jednotlivých senzorů do samostatných objektů, zajišťuje aktuální seznam referencí k aktivním senzorům a zajišťuje jejich obsluhu
- Communication handler – umožňuje komunikaci systému s uživatelem nezávisle na ostatních vláknech a předávání dat ze senzorů do systému
    - Umožňuje zasílat zprávy do MQTT sítě a odebírá téma „zigbee2mqtt/#“, čímž zajišťuje zachycení všech událostí v síti ZigBee a ovládání akčních prvků
- Logic handler – zpracovává a vyhodnocuje data a stav ve hlídaném objektu, následně může vyzvat systém ke spuštění alarmu či odeslání notifikace
- Frame processor – čte data z datového proudu poskytovaného kamerou a v případě zapnutí detekce zároveň provádí detekci objektů v obraze

Veškerá komunikace mezi vlákny probíhá pomocí předem definovaných zpráv, které nesou potřebná data a jsou ukládány se do front. Výhodou front je, že operace vložení a odebrání zprávy je atomická, tudíž nehrozí, že nastane souběh („race condition“) pří práci se sdílenými prostředky.

2.4.1 Ukládání dat

Pro zhotovení modelu zabezpečovacího systému je zvolena sqlite databáze, která se ukládá na samotnou SD kartu. Je však možné jednoduše změnit v kódu cestu k databázi na jakékoliv externí úložiště. Pro snímky pořízené kamerou je taktéž definována v kódu cesta, kam by se měly ukládat. Veškeré data je tak možné mít pouze na lokálních zařízení a není z tohoto důvodu nutné internetové připojení a při správném nastavení přístupů k datům je tak zajištěna i větší míra bezpečnosti.



Obrázek 9 Diagram databáze

Databáze, jak naznačuje diagram na Obrázek 9 Diagram databáze, obsahuje 3 tabulky:

- device_data
  - Zde jsou uložena veškerá data s referencí na jednotlivá zařízení, odkud pocházejí. Reference je tvořena jménem, které uživatel danému zařízení nastavil, tak i pomocí fyzické adresy, která je neměnná.
  - Dalšími sloupci jsou „status“ pro uložení hodnoty hlášené senzorem a „timestamp“ pro uložení časové značky, která označuje čas vložení dat do databáze.
- devices
  - Obsahuje seznam všech senzorů a akčních prvků připojených k systému.

    - Tato tabulka je tvořena sloupci „Device ID“, „Name“ a „LastStatus“, kdy první dva slouží k identifikaci zařízení a poslední sloupec je poslední naměřená hodnota pro případ, kdy se systém restartuje, aby bylo možné navázat na předchozí stav.
- system_settings
    - Obsahuje pouze dva sloupce, „name“ a „value“.
    - Do této tabulky se ukládají nastavení uživatele.

Systém je díky této databází v případě výpadku schopný navázat na stav, ve kterém byl před výpadkem, a zároveň uchovat veškerá nastavení, která uživatel provedl.

2.4.2 Komunikace systému s uživatelem

Dění v systému je možné sledovat přes terminál pomocí SSH, avšak to je pro normálního uživatele nepraktické řešení. Proto je zde i možnost zasílání notifikací uživateli v případě změny stavu.

Pro upozornění jsou zde zvoleny dva způsoby. Prvním je email, který umožňuje poslat podrobnou zprávu v podobě delšího textu a popř. připojit i malý soubor, například fotografii z kamery. Email je zvolen z důvodu přístupnosti. Zprávy lze zobrazit bez problému jak na mobilu, tak na počítači a není k tomu potřeba instalovat další aplikaci. Je také možné jednoduše v programu definovat i znění zprávy. Velkou nevýhodou je však nutné připojení k internetu.

Z toho důvodu je tu druhá možnost, a to sice SMS zpráva pomocí GSM modulu. V modulu je vložena SIM karta, která umožňuje poslat uživateli zprávu v momentě, kdy dojde k narušení prostor. Zde může být nevýhodou zpoplatnění komunikace, kdy v případě předplacených karet a absence tarifu, který by umožnil zaslání SMS zpráv zdarma, se může tento způsob notifikace prodražit. Proto systém zasílá SMS zprávy pouze pokud vyhodnotí situaci jako kritickou.

Webové rozhraní

Pro ovládání a zobrazení dat je zabezpečovací systém vybaven webovým rozhraním, které je naprogramováno pomocí webového frameworku Flask a jazyků Python, html, css a javascript. K rozhraní je v základu možné přistupovat pouze

z lokální sítě. Pro přístup zvenčí je možné využít „port forwarding“ na routeru, pokud má uživatel k dispozici veřejnou IP adresu, a tak zpřístupnit webové rozhraní odkudkoliv. Další možností je například přístup přes VPN do lokální sítě.

Úvodní stránka – Dashboard

Po připojení k rozhraní uživatele přivítá úvodní obrazovka, které nabízí celkový přehled o situaci. Zde je webové rozhraní velkou výhodou, jelikož umožňuje přehledně zobrazit velké množství dat. Ukázku úvodní stránky lze vidět na Obrázek 10.

Prvním prvkem v tzv. Dashboardu je kamerový záběr na levé straně. Jelikož kamera, kterou jsem použil pro zhotovení modelu, má motorizované pohyby švenkování a naklonění („pan“ a „tilt“), tak jsou pod kamerovým záběrem i tlačítka, která umožňují pohybovat s kamerou. Jedno stisknutí otočí kameru v daném směru o 5 stupňů. To umožňuje uživateli na dálku prohlížet celý prostor, ve kterém se kamera nachází, bez manuální manipulace.

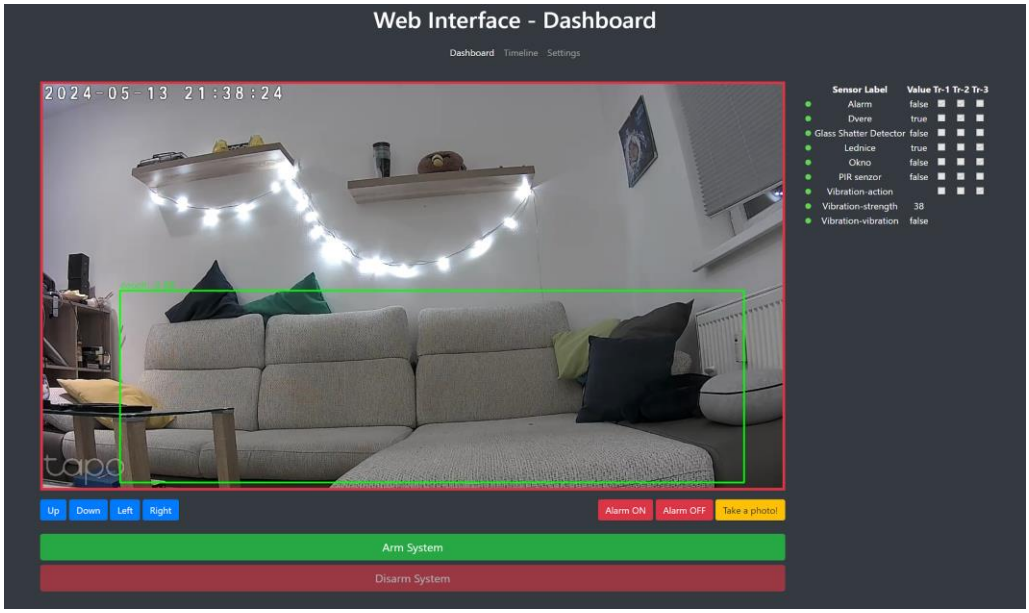
Vedle ovládání pohybu kamery jsou i tlačítka pro uložení aktuálního snímku z kamery na disk a pro manuální ovládání alarmu, aby uživatel mohl alarm kdykoliv zapnout či ztišit dle uvážení.

Napravo od záběru je dynamicky vygenerovaná tabulka všech senzorů. Webové rozhraní zobrazí pouze senzory, které jsou aktivní. Tabulku tvoří několik sloupců. Prvním je název, pod kterým se senzor identifikuje. Ten je možné změnit v nastavení zabezpečovacího systému. V případě spárování nového senzoru s modelem zde bude napsané ID, které je tvořeno z fyzické adresy senzoru.

Druhým sloupcem je aktuální stav, kdy například u magnetického senzoru kontaktu je hodnota „True“, když je senzor i magnet u sebe, a „False“ v případě rozpojení.

Nakonec jsou v tabulce sloupce označeny jako „TR-x“, kde x je číslo. V každém sloupci má každý senzor právě jedno zaškrtávací políčko, které je v Dashboardu uzamčené. Jednotlivé sloupce představují tzv. spouště, které se používají k vyhodnocení toho, kdy automaticky spustit alarm a zaslat upozornění skrze SMS uživateli.

Posledním a nejdůležitějším prvkem úvodní stránky jsou velká tlačítka „Arm system“ a „Disarm system“. Pomocí těchto tlačítek může uživatel přepínat mezi ozbrojeným a neozbrojeným stavem, kdy v ozbrojeném stavu dokáže systém reagovat automaticky a zasílat upozornění uživateli. V opačném případě systém není schopen sám reagovat na vzniklé situace, a tak nemůže ani např. spustit automaticky alarm. Tato funkce je zde přítomna, aby mohl uživatel během pobytu doma zabezpečení vypnout, a tak nerušeně pobývat v daných prostorech.



Obrázek 10 Ukázka Dashboardu se zapnutou detekcí objektů (detekována pohovka)

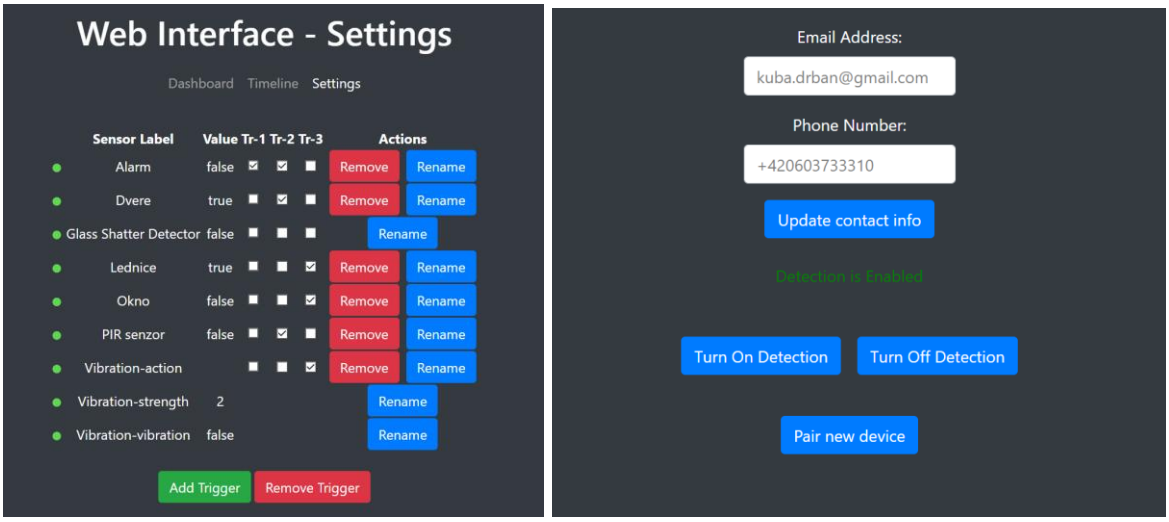
Nastavení zabezpečovacího systému

Druhou stránkou webového rozhraní, kterou lze vidět na Obrázek 11, je nastavení. Obsahuje podobný seznam senzorů jako Dashboard, avšak je rozšířený o další funkce. Všechna zaškrtávací políčka jsou aktivní, tudíž uživatel může nastavovat jednotlivé spouště. Každá spoušť je seznam senzorů, na kterých musí v krátkém časovém úseku (30–60 vteřin) dojít ke vzruchu, aby systém vyhodnotil situaci jako narušení objektu, zapnul alarm a zaslal notifikace s podrobnějšími informacemi uživateli.

Dále je zde možnost každý aktivní senzor v systému přejmenovat, aby si uživatel mohl systém zpřehlednit a rozeznat od sebe jednotlivé senzory. U senzorů, které jsou k systému připojeny pomocí sítě ZigBee je zde i tlačítko „Remove“, které daný senzor odpojí. Pro opětovné připojení je zapotřebí znova senzor spárovat.

Pod tabulkou jsou tlačítka „Add Trigger“ a „Remove Trigger“, která umožňují přidávání a odebírání spouští. Minimální počet je 1 spoušť a maximální hodnota není stanovena. Všechny změny týkající se senzorů se ukládají automaticky a není potřeba nic potvrzovat.

Aby se zajistilo, že uživatel dostane notifikace a zprávy o situaci, je zde také připravený formulář pro nastavení emailové adresy a telefonního čísla. V polích se vždy při načtení stránky zobrazí aktuální hodnota. Změnu těchto údajů je nutné potvrdit tlačítkem „Update contact info“.



Obrázek 11 stránka s nastavením

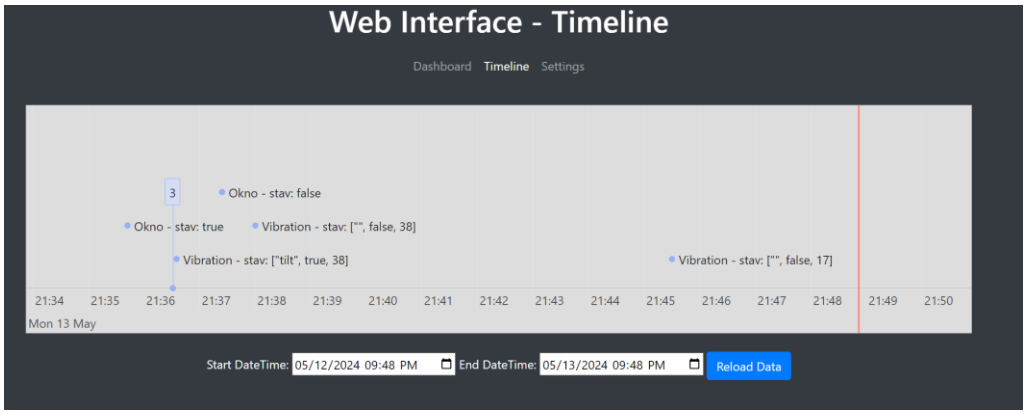
Další možností je vypnutí detekce objektů v záběru kamery a indikace, zdali je detekce spuštěna. Tato možnost je důležitá především v případě, kdy se pro systém využívá starší model Raspberry Pi, který není dostatečně výkonný, a není k dispozici externí výpočetní jednotka jako Google Coral AI Akcelerátor pro zpracování snímků. V tom případě by se Raspberry Pi přetěžovalo, což by mohlo vést k nestabilitě.

ZigBee síť během běžného provozu nepovoluje připojování nových zařízení. K tomu je zapotřebí v systému danou funkci povolit. Pro tento účel slouží tlačítko „Pair new device“, které umožní párování nových zařízení po omezenou dobu. V systému je definovaná doba pro párování na 5 minut, ale hodnotu lze v kódu, kde se generují MQTT zprávy, jednoduše změnit.

Zobrazení událostí za určité období

Poslední stránkou ve webovém rozhraní je „Timeline“. Jak je vidět na Obrázek 12, slouží k zobrazení dat v určitém časovém úseku. Po prvotním přechodu na tuto stránku je nastavený úsek na posledních 24 hodin.

K dispozici jsou však dvě pole, „Start DateTime“ a „End DateTime“, která umožňují navolit si vlastní časový úsek pro načtení dat z databáze. Po navolení je nutné data znova načíst tlačítkem „Reload Data“.



Obrázek 12 Ukázka zobrazení událostí v čase

V časové ose se jednotlivé události ukazují jako modré body s popisem, který se skládá z názvu senzoru a stavu. Pokud se v jednom čase stalo událostí víc, než je možné zobrazit, seskupí se a zobrazí se jako tlačítko s číslem, to je možné vidět v obrázku 4 v čase okolo 21:36. Seskupily se zde 3 události. Uživatel má možnost rozkliknout seskupení a časová osa se sama roztáhne, aby mohla zobrazit všechny takto skryté události.

Vertikální oranžová čára označuje aktuální čas.

Ke zhotovení časové osy je použita knihovna vis.js.

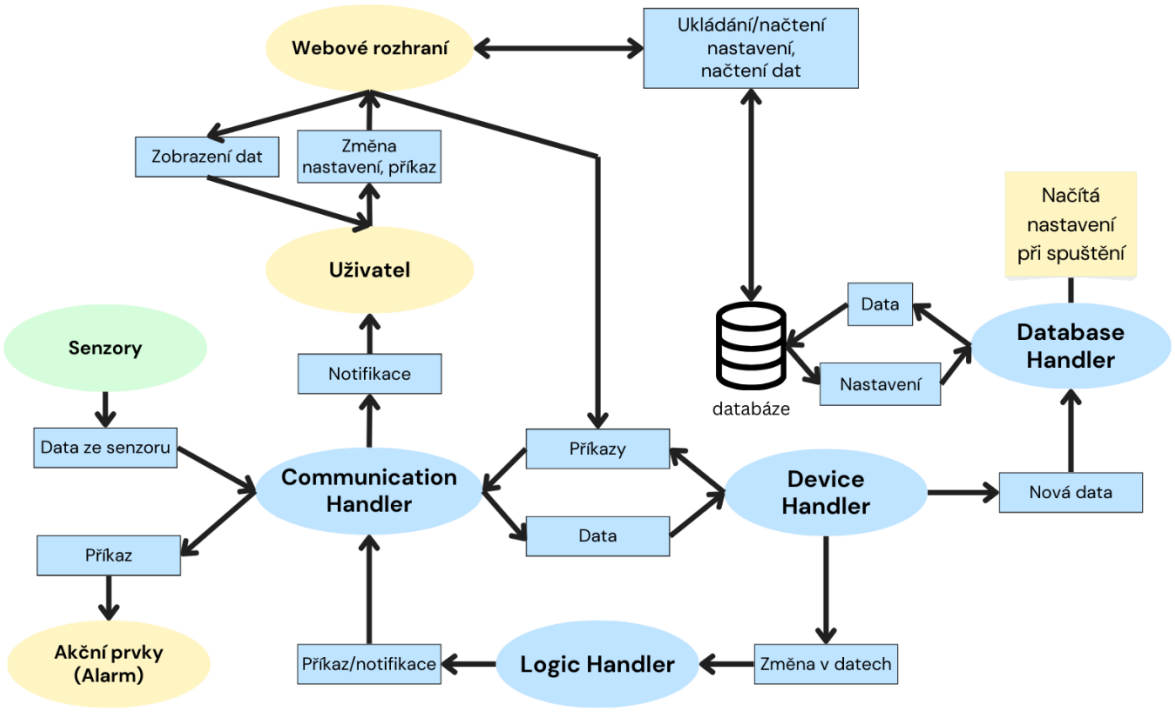
2.4.3 Vyhodnocení dat

K vyhodnocování dat slouží již zmíněná vlákna „Communication handler“ a „Logic handler“. Proces zpracování dat začíná ve vlákně „Communication handler“.

To přijme zprávu a rozhodne, co s ní. Vyhodnotí-li ji jako relevantní, přepošle ji dál do systému pro zpracování. Mezi takové zprávy například patří seznam aktivních

zařízení v ZigBee síti, který slouží k aktualizaci seznamu senzorů a akčních prvků v zabezpečovacím systému. Nebo přijetí zprávy o změně stavu senzorů, což vede k aktivaci vlákna „Logic handler“.

To v případě změny stavu jakéhokoliv senzoru zjistí, jestli se jedná o důležitý senzor, který je uživatelem určen k zabezpečení, nebo o senzor sloužící jen ke sběru informací.



Obrázek 13 Diagram funkce softwaru

Obrázek 13Obrázek 1 je diagram toho, jak model zabezpečovacího systému funguje. Zeleně jsou vstupní prvky, tedy senzory. Žlutě zbarvené jsou výstupní prvky a uživatel. Jednotlivé šipky ukazují, jakým směrem se předávají data, příkazy a notifikace. Modré oválné prvky představují jednotlivá vlákna zmíněná výše a obdélníkové prvky vyjadřují, co je předmětem komunikace mezi jednotlivými vlákny a zařízeními.

3 Porovnání modelu s ostatními systémy a ekonomická rozvaha

Při porovnání realizovaného modelu zabezpečovacího systému je nutné zohlednit, že tento model je plně otevřený jakýmkoliv modifikacím, proto je možné kdykoliv rozšířit funkčnost a upravit si řešení dle svých potřeb.

Pro porovnání je vybráno několik kritérii, které dle mého názoru jsou potřeba zohlednit při hledání vhodného řešení pro zabezpečení bytových prostor, a pro přehled slouží Tabulka 3, ve které jsou stručně popsány kritéria u jednotlivých systémů. Mezi vybraná kritéria patří konektivita, dostupnost senzorů, rozhraní a jednoduchost instalace, závislost na internetu či možnost definování vlastní logiky pro vyhodnocovaní.

Tabulka 3 Porovnání jednotlivých systémů

systém	Fibaro HC3	iGET	Homey Pro	Jablotron	Model s RPi
Konektivita	Z-Wave, Zigbee, Wi-Fi, Bluetooth	Zigbee, Bluetooth	Zigbee, Z-Wave, Bluetooth, Wi-fi, Matter, Thread	Omezená konektivita	Zigbee, Wi-Fi, Bluetooth
Senzory	Dle konektivity	Dle konektivity	Dle konektivity	Pouze Jablotron	Dle konektivity
Vlastní logika a skriptování	Podpora LUA jazyka	Reakce na změnu stavu, časovač	Skripty založené na JS	Jednoduchá reakce na událost	Dle programovacích schopností uživatele
Úložiště	Online i offline, interní	Primárně online, cloud	Online i offline, interní	Online i offline, SD karta	Online i offline, LAN, USB a SD karta
Závislost na internetu	volitelná pro vzdálený přístup	Vyžadováno pro úplnou funkčnost	volitelná pro vzdálený přístup	volitelná pro vzdálený přístup	volitelná pro vzdálený přístup
Instalace systému	uživatelem	uživatelem	uživatelem	odborníkem	Uživatelem, může být náročná
Orientační cena	~12000 kč + senzory	700–6000 kč + senzory	~11500 kč + senzory	24000 kč a více, + senzory	3230 kč + senzory

Cena u modelu s Raspberry Pi je počítána za samotné Raspberry Pi s analyzátorem packetů SONOFF ZigBee 3.0 USB Dongle Plus s čipem CC2652P a GSM modulem Waveshare R800C GSM/GPRS Hat. To stačí k tomu, aby mohlo Raspberry Pi fungovat jako centrála.

Konektivita

Vzhledem ke konektivitě a podpoře různých protokolů, nejlépe vychází systém Homey Pro. Ten podporuje i nejnovější protokoly Matter a Thread. Poté je zde Fibaro Home Center 3, které oproti modelu v této práci podporuje navíc i Z-Wave, avšak je možné dokoupit přijímač pro tento protokol a rozšířit tak možnosti u Raspberry Pi modelu.

V tomto případě zaostává Jablotron, který podporuje pouze spojení po kabelu či za využití proprietárního protokolu pro bezdrátové spojení mezi zařízeními.

Senzory

Toto kritérium úzce souvisí s konektivitou, jelikož ta udává, jaké senzory se mohou k centrální jednotce připojit. V tomhle ohledu vychází nejlépe ty, které podporují ZigBee a Z-Wave, co se množství různých senzorů týče. S ohledem na cenu jsou to systémy s podporou ZigBee.

Možnost vlastní logiky a skriptování

Přizpůsobení a automatizace systému je velmi důležitou vlastností, kterou je nutno zohlednit. Pokud se nehledí na schopnosti uživatele, nejlépe vyjde Raspberry Pi model, kde ve vlákně s logikou lze naprogramovat a vyhodnocovat data zcela libovolně za použití různých knihoven či dalších dat z internetu.

To však vyžaduje jisté znalosti, v mnoha případech i pokročilé, proto je tu pak Homey Pro a Fibaro HC3. Ty také umožňují psaní vlastních skriptů, avšak je to již v rámci daného systému a uživatel nemá tolik svobody při výběru jazyka a knihoven.

Ostatní systémy poté nabízí převážně jen jednoduché reakce na změny stavů (například rozsvícení světel při zapnutí alarmu apod.).

Úložiště

Je důležité, aby zabezbečovací systém mohl uživateli poskytnout ukládání dat. V tomto případě je nejvhodnější model s Raspberry Pi, jelikož umožňuje využít prostor jak na SD kartě se systémem, tak i externí disk nebo úložiště na síti.

V tomto ohledu je vhodný i systém značky Jablotron, který umožňuje použití vyměnitelné SD karty. Nakonec jsou tu systémy Fibaro HC3 a Homey Pro, které mají

interní paměť a ukládají data také lokálně. Bohužel systém iGET umí využít pouze cloud.

Závislost na internetu

Většina systémů vyžaduje internet převážně pro vzdálené ovládání, takže jeho absence nemá žádný vliv na funkci systému, kromě iGET.

Vzdálenou komunikaci je také možné navíc do jisté míry řešit i pomocí GSM modulu, který je například často obsažen v systémech Jablotron a je i součástí modelu zabezpečovacího systému s Raspberry Pi. Zde v aktuální verzi umožňuje oboustrannou komunikaci, avšak je zatím používána pro jednoduchou notifikaci v případě problému v hlídaném prostoru. Pro zpracování zpráv směrem od uživatele do systému by bylo nutné naprogramovat vyhodnocování jednotlivých předem definovaných příkazů.

Instalace systému

V tomto ohledu je vypracovaný model nevhodný pro uživatele, kteří chtějí jen bezstarostně koupit a zapojit „krabičky“ a zasahovat minimálně do již fungujícího systému. Zde nejlépe vychází Jablotron, který nainstaluje a nakonfiguruje odborník dle zákazníkova přání, a tak je s tím nejméně starostí.

Ostatní systémy jsou na tom mezi sebou podobně s obtížností instalace, pokud se jedná jen o jednoduché zapojení a zprovoznění systému bez využití pokročilých funkcí.

Porovnání cen

Musím podotknout, že ačkoliv například cena systému iGET je výrazně nižší oproti konkurenci, neobsahuje jejich systém ani zdaleka tolik pokročilých funkcí jako ostatní.

S pohledem na poměr cena: výkon vychází dle mého názoru model s Raspberry Pi, kde sice musí uživatel oželet komfort do jisté míry, jelikož instalace je náročnější a není zde podpora různých komunitních skriptů a aplikací, ale s trochou znalostí programování umožňuje hodně přizpůsobení a např. i rozšíření o podporu dalších protokolů. A to za necelou třetinu ceny systémů Fibaro HC3 a Homey Pro.

Na druhou stranu je zde Jablotron s cenou 24000 kč a více. Zde je nutné podotknout, že se systémem si uživatel také kupuje profesionální montáž, pravidelné servisní prohlídky a nespornou kvalitu zpracování jednotlivých zařízení.

3.1 Ekonomická úvaha výroby

V následující **Chyba! Nenalezen zdroj odkazů.** je seznam součástek, včetně konkrétního modelu, počtu kusů a ceny, které jsem použil pro naprogramování a testování celého zabezpečovacího systému. Ceny jsou uváděny včetně DPH a jsou aktuální ke dni 14.5.2024.

Tabulka 4 Seznam součástek použitých pro kompletaci modelu bezpečnostního systému

Součástka	**Model**	**Cena [kč]**	**Počet kusů**
Raspberry Pi	4B 4 GB	1629,00	1
Micro SD karta	Samsung MicroSDXC 128GB PRO Plus	499,00	1
Analyzátor Packetů	Sonoff ZBDongle-P	849,00	1
GSM modul	Waveshare 13460	727,00	1
USB Akcelerátor	Coral	1989,12	1
Všesměrový mikrofon	Audio-Technica ATR4697-USB	690,00	1
Senzor vibrací	AQARA Vibration Sensor	399,00	1
IP Kamera	Tapo C200 Pan/Tilt 1080p	859,00	1
Senzor kontaktu	Sonoff SNZB-04	172,00	3
PIR senzor	Sonoff SNZB-03	178,00	1
Alarm/siréna	WOOX R7051	579,00	1

Z Tabulka 4 lze vyčíst, že celková cena systému včetně DPH je 8914,12 kč. V této konfiguraci je systém schopný pořizovat kamerový záběr a detekovat objekty v záběru, detekovat pohyb například ve vstupní hale, detekovat otevření vstupních dveří a dvou oken, detekovat rozbití jednoho okna pomocí vibrací a tříštění skla obecně pomocí mikrofonu. Následně je schopný notifikovat uživatele jak přes internet pomocí zprávy do mailu, tak i SMS, a následně spustit automaticky alarm.

Nutné je také zohlednit časovou náročnost zprovoznění systému. Samotná instalace operačního systému nezabere více jak 30 minut. Následné nainstalování všech požadavků s dostatečně rychlým připojením k internetu trvá nejdéle 2 hodiny, včetně konfigurace. To vše za předpokladu, že všechna zařízení fungují bez jakéhokoliv problému a jsou v perfektním stavu. Samotný systém je poté možné nakopírovat na Raspberry Pi přes flash disk nebo z repozitáře na gitu. Celkový potřebný čas pro zhotovení jednoho modelu se tedy pohybuje okolo 3 hodin.

4 Závěr

Součástí práce bylo popsání několika možných řešení zabezpečovacího systémů v bytě včetně jejich funkcí a dostupnosti. Zjištění, které protokoly se používají v dnešní době pro komunikaci mezi senzory, kam se ukládají data a jaké jsou typické prvky, ze kterých se zabezpečovací systémy skládají. Zaměření bylo převážně na prostory v interiéru domů a bytů.

Výstupem dle zadání je návrh a realizace funkčního modelu zabezpečovacího systému. K tomu jsem využil 7 vstupních zařízení, jmenovitě 3 ks magnetických kontaktních senzorů, senzoru vibrací pro detekci otřesů oken či prosklených dveří a PIR senzor pohybu. Pro zlepšení detekce tříštění skla v bytě je použitý mikrofon a naprogramovaný senzor pro vyhodnocení zvuků ve hlídaných prostorech. Posledním vstupním prvkem je IP kamera, která poskytuje systému obrazový záznam a možnost detekovat různé objekty, které se mohou v bytě nacházet, jako například domácí mazlíčky či člověka. Pro výstup ze systému slouží alarm a notifikace pomocí emailů a SMS zpráv.

Samotný centrální prvek realizovaného modelu je vytvořen pomoci Raspberry Pi 4 B+ se 4 GB RAM paměti. Následně ZBDongle od firmy SONOFF, který umožňuje Raspberry Pi komunikovat v síti ZigBee. Pro zajištění komunikace a upozornění pomocí SMS zpráv je na GPIO piny nasazen GSM modul s předplacenou SIM kartou, a nakonec je zde Coral AI USB akcelerátor, který umožňuje rychlou detekci objektů v obraze, aniž by byl procesor na Raspberry Pi konstantně vytěžován téměř na 100 %.

K ovládání samotného zabezpečovacího systému slouží webové rozhraní, které umožňuje uživateli párovat nová ZigBee zařízení, pořídit snímek z kamery, spustit a vypnout alarm, změnit kontaktní údaje pro notifikace a nastavit podmínky, za kterých se alarm spustí automaticky. Dalším důležitým prvkem je časová osa, na které si uživatel může zobrazit data ze senzorů za určité období.

Na závěr práce je zde i podrobně popsána cena jednotlivých komponent realizovaného modelu zabezpečovacího systému a porovnání jednotlivých funkcí se systémy, které byly uvedeny na začátku.

Dalším možným krokem pro zlepšení funkcí systému by bylo naprogramování automatického parsování dat z webu Zigbee2MQTT, což by mělo umožnit uživateli připojovat nová zařízení bez nutnosti manuální definice. Také rozšíření realizovaného modelu o možnost registrace a přihlašování různých uživatelů s individuálními pravomocemi v rámci systému je dobrým krokem.

Použité literární zdroje

[1] J. Arellano, "Bluetooth vs. Wi-Fi for IoT: Which is Better?," [Online]. Available: https://www.verytechnology.com/iot-insights/bluetooth-vs-wifi-for-iot-which-is-better.

[2] DFRobot, „Smart Home Protocols Explained: Wi-Fi vs Bluetooth vs Zigbee vs Z-Wave Vs Thread and Matter," 18 Říjen 2023. [Online]. Available: https://www.dfrobot.com/blog-13453.html.

[3] K. K. Panigrahi, „Difference between BlueTooth and Zigbee," 27 Červenec 2022. [Online]. Available: https://www.tutorialspoint.com/difference-between-bluetooth-and-zigbee.

[4] Connectivity Standards Alliance, „Zigbee FAQ," [Online]. Available: https://csa-iot.org/all-solutions/zigbee/zigbee-faq/.

[5] Athom B. V., „Homey Pro," 2024. [Online]. Available: https://homey.app/en-us/homey-pro/.

[6] D. Bell, „Fibaro Home Center 3 vs Fibaro Center 3 Lite: A Comparison," 12 Červen 2023. [Online]. Available: www.vesternet.com/en-eu/blogs/smart-home/fibaro-home-center-3-vs-fibaro-lite-your-comprehensive-guide-to-mastering-home-automation.

[7] hlidejsimajetek.cz, „Sada zabezpečovacího systému pro malý byt Jablotron 100 Bezdrátová varianta," [Online]. Available: https://www.hlidejsimajetek.cz/bezdratove-sady-zabezpecovacich-systemu/sada-zabezpecovaciho-systemu-pro-maly-byt-jablotron-100-bezdratova-varianta.

[8] iGET.eu, „iGET HOME Gateway GW1," [Online]. Available: https://www.iget.eu/iget-home-gateway-gw1/.

[9] iGET.eu, „iGET HOME Gateway GW6," [Online]. Available: https://www.iget.eu/iget-home-gateway-gw6/.

[10] iGET.eu, „iGET HOME Alarm X5," [Online]. Available: https://www.iget.eu/iget-home-x5/.

[11] SmarterHOME, „FIBARO HOME CENTER 3 LITE - QUESTIONS AND ANSWERS," 12 Únor 2021. [Online]. Available: https://smarterhome.sk/en/blog/fibaro-home-center-3-lite-questions-and-answers_156.html.

[12] Jablotron, „Jablotron 100+ Uživatelský manuál,“ [Online]. Available: https://www.jablotron.com/cz/o-jablotronu/ke-stazeni/?filename=ja-100plus_user-cz_mmd59503.pdf&do=downloadFile.

[13] Credex Alarm Systems, „Jablotron SmartHub Home Assistant link,“ 4 Květen 2021. [Online]. Available: https://www.credexalarmsystems.eu/en/blog/jablotron-smarthub-home-assistant-link/.

[14] Raspberry Pi, „Raspberry Pi 4,“ [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/.

[15] Texas Instruments, „CC2531,“ [Online]. Available: https://www.ti.com/product/CC2531.

[16] ITEAD Intelligents Systems Co.,LTD, „SONOFF Zigbee 3.0 USB Dongle Plus,“ [Online]. Available: https://itead.cc/product/sonoff-zigbee-3-0-usb-dongle-plus/.

[17] Google, „A sound vocabulary and dataset,“ [Online]. Available: https://research.google.com/audioset/.

[18] Google LLC, „USB Accelerator,“ [Online]. Available: https://coral.ai/products/accelerator/.

[19] „Audio classification guide,“ 21 Květen 2024. [Online]. Available: https://ai.google.dev/edge/mediapipe/solutions/audio/audio_classifier.

[20] Google LLC, „Get started with the USB Accelerator,“ [Online]. Available: https://coral.ai/docs/accelerator/get-started/.

[21] Google LLC, „All models,“ [Online]. Available: https://coral.ai/models/all/.

[22] Zigbee2MQTT, „Supported Devices,“ [Online]. Available: https://www.zigbee2mqtt.io/supported-devices/.

[23] L. Dallinger, „Understanding an MQTT Packet: Ultimate Guide,“ 25 Květen 2023. [Online]. Available: https://cedalo.com/blog/mqtt-packet-guide/.

[24] Zigbee2MQTT, „Support new devices,“ 21 Květen 2024. [Online]. Available: https://www.zigbee2mqtt.io/advanced/support-new-devices/01_support_new_devices.html.

[25] Amazon, „What is MQTT?,“ [Online]. Available: https://aws.amazon.com/what-is/mqtt/.

[26] „Timeline,“ [Online]. Available: https://visjs.github.io/vis-timeline/docs/timeline/.

[27] Vesternet, „Understanding Z-Wave Networks, Nodes & Devices,“ [Online]. Available: https://www.vesternet.com/en-eu/pages/understanding-z-wave-networks-nodes-devices.

[28] Z-Wave Alliance, Inc., „How Certification Works,“ [Online]. Available: https://z-wavealliance.org/development-process-overview-2/.

[29] Texas Instruments Incorporated, „CC2531EMK,“ [Online]. Available: https://www.ti.com/tool/CC2531EMK.

[30] Shenzen Sonoff Technologies Co.,Ltd., „ZBDongle,“ 10 Srpen 2021. [Online]. Available: https://sonoff.tech/wp-content/uploads/2021/11/产品参数表-ZBDongle-P-20211008.pdf.

[31] K. Aloufi a O. Alhazmi, „MQTT protocol model,“ Listopad 2020. [Online]. Available: https://www.researchgate.net/figure/MQTT-protocol-model_fig1_347026819.

[32] Lumi United Technology Co., Ltd., „Aqara Vibration Sensor,“ [Online]. Available: https://www.aqara.com/eu/product/vibration-sensor/.

[33] K24 International s.r.o., „Sonoff SNZB-04,“ [Online]. Available: https://www.k24.cz/product/706396/Sonoff_SNZB_04.html.

[34] K24 International s.r.o., „K24.cz,“ [Online]. Available: https://www.k24.cz/product/702171/Sonoff_SNZB_03.html.

[35] Waveshare, „R800C GSM/GPRS HAT For Raspberry Pi,“ [Online]. Available: https://www.waveshare.com/r800c-gsm-gprs-hat.htm.

[36] „Co je MQTT a k čemu slouží ve IIoT? Popis protokolu MQTT,“ [Online]. Available: https://ipc2u.cz/blogs/news/mqtt-protokol.

[37] „MQTT - univerzální protokol pro cloudové a IoT aplikace,“ [Online]. Available: https://www.hw-group.com/cs/podpora/mqtt-univerzalni-protokol-pro-cloudove-a-iot-aplikace.

[38] „Raspberry Pi Documentation,“ [Online]. Available: https://www.raspberrypi.com/documentation/.