Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Klima vnitřních prostor

Vladimír Josefy

Bakalářská práce
2023

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Vladimír Josefy**
Osobní číslo:	**I19237**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Téma práce:	**Klima vnitřních prostor**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování

Cílem bakalářské práce je vytvoření aplikace, která zobrazí stav vnitřního klimatu objektu. Vstupní data pro aplikaci budou získávána pomocí LoRaWAN senzorů. Pro přenos zpráv od zařízení bude využita platforma CRA. Požadavky na aplikaci:

- vizualizace naměřených hodnot (např. CO2, teplota, vlhkost, světlo,...),
- zpracování alarmů - překročení limitů měřených hodnot,
- zobrazení pozice zařízení na mapě.

Součástí práce bude představení použitých technologií, popis sítě LoRaWAN a vytvořené aplikace.

Rozsah pracovní zprávy: **30 – 40**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

KÜHNEL, Claus. *Develop and Operate Your LoRaWAN IoT Nodes: Ready-to-use devices and self-built Arduino nodes in the "The Things Network"*. Elektor-Verlag, 2022. ISBN 9783895764943.

Objevte svět IoT [online]. Pixman, 2022 [cit. 2022-10-10]. Dostupné z: https://www.cra.cz/pripojeni-k-iot-siti-lorawan

Vedoucí bakalářské práce: **Ing. Soňa Neradová, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **16. prosince 2022**
Termín odevzdání bakalářské práce: **12. května 2023**

L.S.

Ing. Zdeněk Němec, Ph.D. v.r.
děkan

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

V Pardubicích dne 28. února 2023

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 12. 5. 2023

Vladimír Josefy

PODĚKOVÁNÍ

Tímto bych rád poděkoval své vedoucí bakalářské práce Ing. Soně Neradové, Ph.D. za odbornou pomoc a cenné rady, které mi pomohly při zpracování práce.

ANOTACE

Cílem bakalářské práce je návrh a implementace aplikace, která bude umožňovat vizualizaci a monitorování vnitřního klimatu objektu. Vstupní data pro aplikaci budou získávána pomocí zařízení připojených do sítě LoRaWAN. Pro přenos zpráv od zařízení bude využito platformy CRA. Aplikace bude umožňovat dohledání daného zařízení na mapě, vizualizaci měřených hodnot pomocí grafů a stanovení limitů měřených hodnot. O překročení stanovených limitů bude uživatel aplikace informován. Teoretická část práce poskytuje přehled o problematice internetu věcí, dále pojednává o sítích LPWA a obsahuje popis sítě LoRaWAN. Praktická část popisuje návrh a implementaci aplikace a obsahuje přehled využitých technologií a hardwarových komponent.

KLÍČOVÁ SLOVA

Internet věcí, webová aplikace, LoRa, LoRaWAN, monitorování, senzory, TypeScript, MicroPython

TITLE

Measuring of environmental values in buildings

ANNOTATION

The aim of the bachelor thesis is the design and implementation of a web application, which allows for the visualization and monitoring of environmental values in buildings. The input data will be generated using devices connected to the LoRaWAN network. Transmission of data from the device will be achieved by utilizing the CRA platform. The application will allow the user to display the geographical location of the device, to visualize measurement values using graphs, and to set limits for measured values. When a measurement exceeds the defined limits, the user shall be notified by the application. The theoretical part of the thesis is devoted to introducing the field of IoT, explaining LPWA networks and detailing the concepts used in the LoRaWAN network. The practical part concerns itself with the design and implementation of the web application and also provides a short overview of the technologies and hardware components used.

KEYWORDS

Internet of Things, web application, LoRa, LoRaWAN, monitoring, sensors, TypeScript, MicroPython

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

3GPP	3rd Generation Partnership Project
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
AFH	Adaptive Frequency Hopping
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
ARPANET	Advanced Research Projects Agency Network
CDMA	Code Division Multiple Access
CoAP	Constrained Application Protocol
CRC	Cyclic Redundancy Check
CRA	České Radiokomunikace
CSS	Chirp Spread Spectrum
DBPSK	Differential Binary Phase Shift Keying
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FFD	Full Function Device
FHSS	Frequency Hopping Spread Spectrum
GMSK	Gaussian Minimum Shift Keying
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISM	Industrial, Scientific, and Medical
JSON	JavaScript Object Notation
JWT	Json Web Tokens
LoRa	Long Range
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MCL	Maximum Coupling Loss
MQTT	Message Queuing Telemetry Transport
NB-IoT	Narrowband IoT
OFDMS	Orthogonal Frequency Division Multiple Access
OQPSK	Offset Quadrature Phase Shift Keying
ORM	Object Relational Mapping
QoS	Quality of Service
QR	Quick Response
REST	Representational State Transfer
RFD	Reduced Function Device
RFID	Radio Frequency Identification
RPMA	Random Phase Multiple Access
RSSI	Received Signal Strength Indication
SC-FDMA	Single-Carrier Frequency Division Multiple Access
SNR	Signal-to-noise Ratio
SoA	Service-oriented Architecture
SPOF	Single Point of Failure

SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
UDP	User Datagram Protocol
UNB	Ultra Narrow Band
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
Wi-Fi	Wireless Fidelity
WSN	Wireless Sensor Network
WWW	World Wide Web

ÚVOD

V dnešní době je internet věcí neboli IoT (Internet of Things) oblastí, která podstupuje obrovský růst. Technologie IoT se nyní objevuje téměř ve všech odvětvích, které nějakým způsobem využívají elektronická zařízení. Energetický průmysl například využívá zařízení IoT k monitorování a řízení spotřeby energie. Využití technologie IoT lze nalézt i ve zdravotnictví, kde umožňuje vzdálené monitorování pacientů. Zařízení IoT lze nalézt také na spotřebitelském trhu, kde jsou zastoupena zejména prostřednictvím nositelné elektroniky. [1]

Hlavním cílem práce je návrh a implementace aplikace, která umožňuje vizualizaci a monitorování vnitřního klimatu objektu. Mezi požadované vlastnosti aplikace patří zejména možnost zobrazovat pozici zařízení na mapě a vizualizovat měřené hodnoty pomocí grafů. Systém je implementován jako webová aplikace nasazená na platformě Vercel. Pro získávání dat ze zařízení je využito platformy CRA (České Radiokomunikace).

Teoretická část práce je věnována představení technologie IoT, pojednává o historii a o moderních způsobech využití této technologie. Dále jsou představeny vybrané technologie, které jsou v rámci IoT využívány. Probírány jsou také modely konektivity, díky kterým je možné zprostředkovávat komunikaci a výměnu dat. Práce dále pojednává o komunikačních protokolech a o technologiích, které zprostředkovávají komunikaci na aplikační vrstvě. Následuje představení pojmu sítí LPWA (Low Power Wide Area), které obsahuje charakterizaci cílů a technik návrhu těchto sítí. Po představení samotného pojmu LPWA jsou také blíže charakterizovány vybrané sítě. Poslední kapitola teoretické části je věnována technologií LoRa a LoRaWAN, tyto technologie jsou popsány podrobněji, jelikož nachází využití v praktické části práce.

Praktická část obsahuje popis požadovaných vlastností aplikace a návrh řešení. V praktické části jsou také popisovány hardwarové komponenty, které v systému figurují jako zdroje dat. Následně je vysvětlen způsob programování hardwarových komponent V další části jsou popsány jednotlivé technologie, které jsou v systému využité. Následuje popis databázového schématu a vlastní implementace aplikace.

1 INTERNET VĚCÍ

Internet věcí, zkráceně IoT z anglického Internet of Things, je pojem, označující soubor propojených, jednoznačně adresovatelných objektů (věcí), které komunikují prostřednictvím standardizovaných komunikačních protokolů. Objekty mezi sebou nemusí komunikovat výhradně prostřednictvím internetu, pojem zahrnuje také komunikaci, probíhající v lokální síti. Tato konektivita umožňuje objekty využívat s přidanou hodnotou, ve srovnání s případy, kdy jsou objekty využívány izolovaným způsobem. V ekosystému internetu věcí totiž nejsou klíčovými prvky samotné objekty ale data, která jsou objekty poskytována a sdílena. [1]

Samotná věc je z hlediska IoT neživý objekt, obsahující software, elektroniku a senzory, díky kterým je objekt schopný snímat nějakou veličinu či veličiny a produkovat tak měření, která je možné sdílet s dalšími věcmi. Data jsou s ostatními objekty sdílena za účelem jejich zpracování, což umožňuje automatizovat rozhodovací procesy na základě obdržených dat. Důsledkem je značná míra autonomie systému, která umožňuje jeho běh bez nutnosti častých zásahů člověka. [1], [2]

1.1 Historie

Přestože internet věcí podstupuje svůj zatím největší rozvoj právě v současnosti, tak koncepty, na kterých je celý ekosystém stavěn, je možné chronologicky situovat už do první poloviny 19. století, kdy byl s vynálezem elektromagnetického telegrafu úspěšně implementován návrh zařízení, které je schopné pomocí přenosu elektrických signálů sdílet data. [3]

Zásluha o první propojené zařízení patří programátorům z Carnegie Mellon University, kteří se v 80. letech 20. století rozhodli pokusit, pomocí připojení do sítě ARPANET, vzdáleně monitorovat teplotu a dostupnost nápojů Coca Cola v jednom z automatů v areálu univerzity. Dalším významným milníkem je rok 1990, kdy John Romkey a Simon Hackett využili protokolu TCP/IP k připojení toustovače k internetu, díky čemuž jej bylo možné vzdáleně zapínat a vypínat. [3]

V roce 1991 využili vědci z univerzity Cambridge první prototyp webkamery ke sledování množství kávy v kávovaru v jejich laboratoři. Webkamera byla naprogramována, aby ve specifických časových intervalech pořizovala snímky kávovaru, které byly poté zasílány na lokální počítače, což umožňovalo kontrolovat kávovar na dálku. [3]

Nejvýznamnějším milníkem pro fenomén internetu věcí je však rok 1999, kdy byl poprvé zformulován pojem „The Internet of Things“, stalo se tak během prezentace pro firmu Procter

& Gamble, když takto Kevin Ashton označil technologii, která pomocí identifikace na rádiové frekvenci umožňovala propojit zařízení za účelem zjednodušení řízení inventarizace a spotřebitelského řetězce. Přestože Kevin Ashton byl původcem pojmu, později vyjádřil názor, že výstižnějším označením mohlo být spíše „Internet for Things“. [4]

S přechodem do 21. století pozvolně vstupoval internet věcí do veřejného povědomí, pojmu byla věnována mediální pozornost a na trh přicházeli nové technologie a zařízení. V roce 2000 byla například na trh uvedena chytrá lednička od firmy LG, která umožňovala uživatelům nakupovat online a provádět videohovory. Dalším významným zástupcem byl robot Nabaztag, který informoval uživatele o aktuálních novinkách, změnách na akciovém trhu a také byl schopný poskytovat předpověď počasí. O rostoucí popularitě internetu věcí svědčí také skutečnost, že v roce 2008 byla ve Švýcarsku uskutečněna první mezinárodní konference k dané tématice a společnost Cisco již v té době zaznamenávala, že počet zařízení připojených k internetu přesahoval počet obyvatelů světa. Skutečný rozmach zařízení IoT nastal rokem 2011 s příchodem protokolu IPv6. Následující léta s sebou přinášeli inovativní zařízení od chytrých termostatů až k samořídícím vozidlům a internet věcí byl zakomponován prakticky do každého odvětví průmyslu. [3]

1.2 Moderní využití IoT

Schopnost automatizovat rozhodovací procesy a zefektivnit lidské vnímání světa znamená, že technologie IoT nenalézá své využití pouze v oblastech průmyslu. Všudypřítomnost zařízení IoT v současnosti znamená, že je můžeme pozorovat také v domácnostech spotřebitelů, kde umožňují zjednodušit či dokonce plně automatizovat každodenní činnosti člověka.

- **Agrikultura –** S růstem světové populace bude růst také poptávka po potravinách a zemědělství je jedním z odvětví, které se této výzvě bude muset postavit. Zužitkováním technologie IoT mohou zemědělci zvýšit celkovou produkci potravin, snížit ztráty a zdokonalit výkonnost zemědělských operací. Díky rozličným senzorům IoT je možné získávat přesnější informace o stavu půdy a rostlin, přesněji dávkovat hnojiva, pesticidy a herbicidy a minimalizovat tak jejich negativní vliv na životní prostředí. [5]
- **Zdravotnictví –** Technologie IoT mohou být využity k monitorování stavu pacientů v reálném čase, typické je například sledování srdeční frekvence, krevního tlaku, hladiny glukózy v krvi. Vzdálené monitorování stavu pacienta také pomáhá snižovat délku pobytu v nemocnici a může pomáhat předcházet opakovaným návratům. Dalším

přínosem je sledování hygieny, kdy různé senzory mohou monitorovat čistotu v místnosti. Senzory také mohou usnadňovat procesy správy majetku, kdy je možné sledovat zásoby léků a podmínky skladování, nebo polohu lékařského vybavení, jako jsou defibrilátory, invalidní vozíky či kyslíkové pumpy. [6]

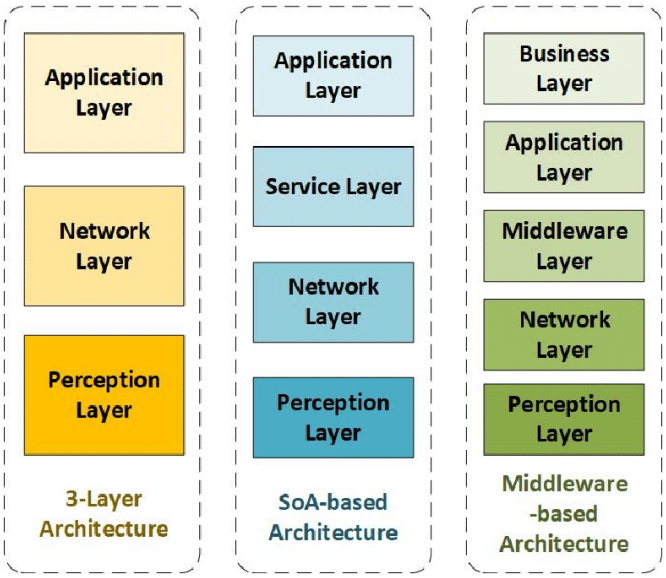
- **Logistika –** Pomocí senzorů je možné sledovat a v reálném čase řídit různé aspekty logistického řetězce. [5]
- **Chytré domácnosti** – Spotřebiče a chytrá zařízení jako jsou například, televizory, termostaty, robotické vysavače, spínače světel či kávovary mohou pomocí technologie IoT komunikovat a sdílet mezi sebou data v reálném čase, díky čemuž je možné plánovat i automatizovat běžné činnosti v rámci domácnosti. Kromě automatizace domácnosti je také přínosem IoT vyšší míra zabezpečení domácnosti pomocí chytrých zvonků, bezpečnostních kamer a poplašných zařízení. Uživatelé tak mohou pohodlně sledovat stav domácnosti na dálku. [7]
- **Chytrá města** – Nárust městské populace značně zatěžuje městskou infrastrukturu a veřejné služby. Napojení zařízení do infrastruktury internetu věcí pomáhá k zvýšení efektivity městských služeb a snížení nákladů. Díky monitorování a analýze dopravních situací je například možné optimalizovat semafory a dynamicky reagovat na stav na silnicích. Chytré osvětlení umožňuje měnit intenzitu pouličních světel v reakci na pohyb vozidel a chodců, což vede k významným energetickým úsporám a také ke snížení světelného znečištění. Díky chytrým měřičům napojeným do chytré energetické sítě mohou poskytovatelé energií efektivněji spravovat dodávku energie a uživatelé mohou sledovat svoji spotřebu energii a budovat tak povědomí o spotřebě a možné úspoře. Využití kapacitních senzorů ke sledování úrovně odpadu v kontejnerech a následná analýza zefektivňuje plánování trasy pro svoz odpadu. [8]

1.3 Architektura

Kapitola byla vypracována dle zdroje [9].

Jedním ze zásadních problémů, kterému čelí technologické odvětví ve snaze podpořit nasazování systémů IoT, je návrh referenční architektury, která by podporovala současné požadavky a zároveň byla dostatečně flexibilní a rozšiřitelná. Výsledná architektura by musela být dostatečně škálovatelná, aby byla schopná podporovat stále rostoucí počet zařízení bez znatelného dopadu na výkon. Měla by také být interoperabilní, aby spolu zařízení od různých výrobců byla schopná komunikovat a kooperovat. V rámci architektury by mělo být možné provádět sběr a analýzu dat distribuovaným způsobem a architektura by měla být zabezpečená a schopná fungovat s omezenými prostředky.

V současné době neexistuje jednotná referenční architektura a navzdory snahám o standardizaci se její zavedení jeví jako velmi komplexní problém. Hlavním důvodem je různorodost využití technologie IoT, kde každý implementovaný systém tvarují návrhová specifika konkrétní domény, ve které je využíván. Situaci dále komplikují tržní subjekty, které mají sklony prosazovat vlastní platformy pro řešení podobných problému.



Obrázek 1: Typické architektury systémů IoT. [9]

1.3.1 Třívrstvá architektura

Obecná architektura se skládá z percepční, síťové a aplikační vrstvy.

- **Percepční vrstva –** Představuje fyzickou úroveň objektů, které jsou schopné interagovat s okolním prostředím a díky výpočetním schopnostem jsou v jistém slova smyslu „chytré“ a „inteligentní“. Pojem chytré zařízení se zaobírá technologickými

aspekty (využité chytré technologie), zatímco pojem inteligentní objekt vypovídá o funkcionálních aspektech, tj. schopnost sebeidentifikace, samotestování a sebediagnostiky. Chytré objekty, sloužící jako základní prvky IoT, mohou být jednoduchá zařízení vybavená senzory a výpočetními schopnostmi, nebo může jít o běžně využívané objekty, jako jsou např. lednička, auto nebo televizor. Obecně jsou chytré objekty schopné mezi sebou komunikovat a připojovat se ke zdrojům na internetu za účelem využití dat a služeb. Podle specifické oblasti, kde je IoT využito mohou dále objekty například využitím senzorů sbírat informace o okolním prostředí nebo s okolím za pomoci akčních prvků přímo manipulovat.

- **Síťová vrstva –** Zodpovídá za přenos dat, získaných z percepční vrstvy, k aplikační vrstvě. K jejímu fungování lze využívat různých protokolů, je však nutné brát na vědomí klady i zápory daných protokolů a vybírat ty nejvhodnější pro danou situaci. Například protokol IPv6 byl primárně navržen k vyřešení problematiky vyčerpání adresního prostoru, se kterou se potýkala starší verze IPv4. Protokol byl však navržen pro drátové sítě a nebyl tak vhodný pro využití v bezdrátových senzorových sítích, které jsou složené ze zařízení, pro které je charakteristická nízká výpočetní schopnost a nízká spotřeba energie. Specificky pro potřeby bezdrátových senzorových sítí byl navržen protokol 6LoWPAN, díky kterému je možné vyhnout se nutnosti zahrnovat do systému zařízení sloužící jako brány.
- **Aplikační vrstva –** Zahrnuje veškerý software nutný k poskytování specifické služby, dochází zde k filtrování, agregaci a zpracování dat která jsou následně poskytována koncovým uživatelům, k čemuž se často využívá speciální software zvaný middleware, který také slouží k maskování heterogeneity nižších vrstev.

1.3.2 Architektura orientovaná na služby

Architektura orientovaná na služby neboli SoA z anglického service-oriented architecture, člení aplikaci na jednotlivé funkční komponenty, které jsou propojené pomocí protokolů a rozhraní. Architektura umožňuje opětovné použití jednotlivých softwarových a hardwarových komponent. SoA lze do IoT zakomponovat pomocí vložení nové vrstvy mezi vrstvu síťovou a aplikační, tato nová vrstva služeb zodpovídá za objevování požadavků na služby, skládání služeb pro komunikaci s připojenými objekty, spravování mechanismů důvěry, pomocí kterých jsou požadavky na služby ověřovány a vrstva také poskytuje rozhraní pomocí kterého mohou služby interagovat.

1.3.3 Pětivrstvá architektura

Další významnou architekturou v oblasti IoT je pětivrstvá architektura, také označována jako architektura middleware. V posledních letech jsou na systémy IoT kladeny vysoké požadavky z hlediska škálovatelnosti, interoperability a spolehlivosti, další rozvoj tak závisí na technologickém pokroku a návrhu nových, inovativních a efektivnějších modelů a postupů. V tomto ohledu umožňuje pětivrstvá architektura tvořit a strukturovat aplikace IoT efektivněji.

Pětivrstvá architektura se skládá z následujících částí: percepční vrstva, síťová vrstva, vrstva middleware, aplikační vrstva a vrstva byznysová. Zejména vrstva middleware plní klíčové funkce, má na starost shromažďování a filtrování dat z hardwarových zařízení, zjišťování informací a řízení přístupu k zařízením pro různé aplikace.

Obecně zde pojem middleware označuje specializovaný software, který vytváří abstrakci mezi technologií IoT a různými aplikacemi. Slouží k zakrytí detailů jednotlivých technologií a poskytuje jednotná rozhraní, díky kterým se vývojáři mohou soustředit na specifika vývoje aplikací, bez nutnosti zabývat se vzájemnou kompatibilitou mezi aplikacemi a infrastrukturou. Využití middleware nabývá v současnosti významu zejména kvůli své roli ve zjednodušení vývoje nových služeb a integrace starých technologií do nových. Hlavní výhody middleware tak jsou:

- Podpora pro různé aplikace,
- kompatibilita s různými operačními systémy a platformami,
- distribuovaný výpočet a interakce služeb v heterogenním prostředí,
- podpora standardizovaných protokolů,
- dostupnost standardizovaných rozhraní, umožňujících portabilitu a interoperabilitu.

1.4 Technologie umožňující bezdrátové připojení

1.4.1 Bezdrátová senzorová síť

Bezdrátová senzorová síť, anglicky wireless sensor network (WSN), je označení pro sadu prostorově rozložených senzorových uzlů, které jsou využívány pro monitorování environmentálních podmínek. Své využití nachází v různých typech aplikací IoT, mohou sloužit například k monitorování čistoty ovzduší, kvality vody nebo k prevenci přírodních katastrof. Na obrázku 2 lze vidět příklad využití bezdrátové senzorové sítě na bojišti, kde mohou senzory být strategicky rozmístěny na území nikoho za cílem sběru strategických informací, senzory v takové síti mají schopnost sebeorganizace a jsou schopny detekovat a klasifikovat cíle pomocí akustických a magnetických signálů. [10]

Obrázek 2: Příklad využití bezdrátové senzorové sítě na bojišti. [10]

Senzorové uzly jsou typicky malé a mají k dispozici omezené prostředky, tuto skutečnost je nutné brát v potaz v aplikacích IoT, které využívají WSN, zejména při návrhu distribuovaných algoritmů a komunikačních protokolů. Podle stylu přenosu dat lze WSN členit na centralizované a decentralizované. V centralizovaných sítích jsou data směřována na konkrétní koncový systém, který obstarává zpracování dat a jejich další přenos. Nevýhodou tohoto přístupu je, že koncový systém se stává klíčovým bodem infrastruktury a jeho výpadek znamená výpadek celé sítě, tato situace je běžně označována jako SPOF neboli single point of failure. Decentralizovaný přístup naopak svěřuje odpovědnost za přenos a zpracování dat jednotlivým senzorovým uzlům. [10], [11]

1.4.2 Identifikace na rádiové frekvenci

Identifikace na rádiové frekvenci, zkratkou RFID, hraje v ekosystému IoT klíčovou roli, jakožto přední identifikační technologie a do budoucna se očekává, že plně nahradí systémy čárových kódů. [10]

Systém RFID se skládá ze tří hlavních částí. Tag slouží k uchování informace, kterou je možné získat pomocí čtečky, ke komunikaci mezi tagem a čtecím médiem jsou využívány antény. Čtečka s anténou vysílá příkaz transpondéru a čeká na odpověď. Příkaz může být v adresovaném či neadresovaném režimu, čtečka tak může vyhledávat určité tagy. Každý odpovídající tag v dosahu čtečky zaznamená signál, přičemž energie z něj je využita k probuzení a napájení interních obvodů. Tag signál dekóduje, ověří jeho platnost a odpoví čtečce, odpověď je přenesena pomocí modulace vlny dopadající ze čtečky. Hlavní myšlenka spočívá v tom, že čtečka komunikaci iniciuje a tag odpovídá. [10], [12]

Systém je schopen pracovat na různých radiových frekvencích, podle frekvence, která je ke komunikaci využitá, systémy dělíme na nízkofrekvenční, vysokofrekvenční, ultrafrekvenční a mikrovlnné. Tagy je možné dělit podle způsobu napájení. Pasivní tagy nemají vlastní zdroj energie, k napájení využívají energii příchozího signálu. Aktivní tagy mají naopak vlastní baterii a také svůj vlastní vysílač. Existují také semi-pasivní tagy, které mají vlastní zdroj energie pro napájení interních obvodů, avšak ke komunikaci využívají odražený signál. [10], [12]

V rámci IoT by měl být každý objekt jednoznačně identifikovatelný, případně klasifikovatelný jakožto prvek konkrétní třídy. RFID není jediný mechanismus, kterým je tohoto možné docílit, lze využít například QR kódy nebo IP. Přestože je RFID v oblasti IoT velmi populární technologie, její využití má i svá negativa. Využití bez adekvátního zabezpečení otevírá možnost pro zneužití tagů jejich neoprávněnou modifikací. Velmi častým problémem je také kolize signálů, která nastává v situacích, kdy odpovídá vícero tagů zároveň, to může vést k prodlevám se získáním informace. Dalším problémem je také nutnost jednotného komunikačního protokolu v zájmu interoperability, zařízení od různých výrobců mohou totiž využívat rozdílná kódování. V případě aktivních tagů je také nutno brát v úvahu životnost baterie. [10]

1.4.3 Fog computing

Zpracováno dle zdroje [13].

Mnoho průmyslových odvětví se stává pro zvládání každodenních úkolů stále závislejších na inteligentních zařízeních. Inteligentní systémy generují prostřednictvím různých aplikací a senzorů velký počet dat a různá průmyslová odvětví jsou tak nucena potýkat se s problematikou produkce a zpracovávání obrovského objemu dat. Data generovaná zařízeními jsou analyzována za účelem extrakce informací. Díky vlastnostem jako je škálovatelnost a přístupnost se stává velmi populárním přístupem přesun infrastruktury organizace do cloudu. Nicméně ne všechna data, generovaná velkým množstvím senzorů, je možné přesunout do cloudu, jelikož tento přístup by mohl do systému zavádět nepřípustnou latenci. Atraktivním způsobem, jak skloubit pozitiva přesunu infrastruktury do cloudu se specifickými požadavky, existujícími v prostředí IoT, je již zmiňovaný fog computing.

Fog computing slouží v prostředí IoT k minimalizaci přenosu dat do prostředí cloudu za účelem analýzy a zpracování, což poskytuje lepší výkon a efektivitu. Jako uzly využívá koncová zařízení, vybavená výpočetními schopnostmi, úložištěm a připojením k síti. Uzlem mohou být například přepínače, směrovače, servery nebo kamery. Díky tomuto přístupu je možné přesunout úkony související se skladováním, zpracováním a analýzou dat blíže k zařízením IoT, což umožňuje minimalizovat latenci a poskytovat zpětnou vazbu v reálném čase.

Jako další způsob, jak řešit problematiku zpracování dat v reálném čase se nabízí technologie zvaná edge computing, která obdobně jako fog computing přesouvá výpočetní úlohy na okrajová zařízení, hlavní rozdíl však spočívá v tom, že fog computing využívá nejen zdroje pro zpracování dat v lokální síti, ale zároveň i zdroje v cloudu. [14]

Tabulka 1: Srovnání pojmů fog computing a edge computing. [13], [15]

Fog computing	**Edge computing**
Přesouvá výpočetní operace na hardware připojený do lokální sítě nebo přímo na hardware lokální sítě.	Výpočetní operace běžně probíhají přímo na zařízeních IoT, se kterými jsou senzory a akční prvky propojeny.
Data jsou zpracovávána na uzlech v lokální síti.	Data jsou zpracovávána přímo na zařízeních IoT bez relokace do cloudu nebo do datových center.
Potenciální bezpečností rizika související s přenosem dat do cloudu.	Bez nutnosti přenosu dat do cloudu je možné se vyhnout jistým bezpečnostním rizikům.
Vyšší latence související s přenosem dat.	Nižší latence díky uchovávání dat přímo na zařízení.
Využívané v situacích, kdy je třeba zpracovávat velké množství dat a současně respektovat požadavek na zpětnou vazbu v reálném čase.	Běžně využívané v aplikacích, které nevyžadují masivní výpočetní schopnosti dostupné za využití cloudové infrastruktury.

1.5 Konektivita

Způsob, kterým lze v systémech IoT strukturovat připojení a komunikaci různorodých zařízení lze vystihnout pomocí modelů konektivity, v roce 2015 byl výborem Internet Architecture Board (IAB) vydán dokument, který popisuje čtyři nejběžnější modely, využívané pro síťový provoz a konektivitu v prostředí IoT. Tyto modely zvýrazňuji flexibilitu zařízení IoT v ohledu strukturování síťového provozu. [16]

1.5.1 Model device-to-device

Tento model vystihuje situaci, kdy mezi sebou napřímo komunikují alespoň dvě zařízení, tj. bez využití prostředníka. Je tak umožněna přímá výměna dat mezi zařízeními, bez nutnosti spoléhat na centrální infrastrukturu nebo síťový uzel. Komunikace může být zprostředkována pomocí různých protokolů jako jsou Bluetooth, Zigbee nebo Z-Wave. Ke komunikaci je také možné využít internet. [16], [17]

Tento model tedy umožňuje zařízením, která využívají kompatibilní komunikační protokol, výměnu zpráv za účelem plnění své funkce. Zpravidla je aplikován na situace, kdy je očekáváný objem vyměňovaných dat nízký, což je zejména typické pro zařízení v prostředí chytrých domácností jako jsou například chytré žárovky, termostaty, zámky dveří nebo podobná zařízení. [16]

Výzvou tohoto modelu je zejména zachování interoperability. Pokud dva odlišní výrobci chtějí umožnit vzájemnou komunikaci mezi jejich zařízeními, pak je nutno shody v sadě využívaných protokolů. Například v situaci, kdy je na jedné straně využíván komunikační protokol Z-Wave a na druhé straně je využíván komunikační protokol Zigbee není kompatibilita možná. To ve výsledku zásadně omezuje koncového zákazníka, jelikož na tuto skutečnost také musí brát zřetel. [16]

1.5.2 Model device-to-cloud

Jde o model, zaměřující se na přímé propojení zařízení IoT s cloudovými službami, díky čemuž je možná výměna dat. Tento styl konektivity potenciálně umožňuje uživateli vzdálený přístup k zařízení a také jeho vzdálenou správu. Model ke komunikaci většinou využívá existujících komunikačních mechanismů, jako jsou Ethernet nebo Wi-Fi. [16], [17]

Příklady využití tohoto modelu lze nalézt v jistých spotřebitelských zařízeních, například chytrý termostat od firmy Google Nest, dříve Nest Labs, zasílá svá data do databáze v cloudu, kde je možná jejich efektivní analýza, na jejíž základě je pak možné informovat uživatele o spotřebě energie v jeho domácnosti. [16], [18]

1.5.3 Model device-to-gateway

Zpracováno dle zdroje [19].

V případech, kdy výrobce chytrých objektů využívá protokolů, které jsou v cílovém trhu hojně zastoupené, se jako dobrá volba modelu jeví model device-to-cloud. V některých případech je však nutné využít méně zastoupených technologií nebo podporovat speciální aplikační funkce, například lokální autentizaci a autorizaci, v zájmu interoperability se staršími zařízeními, která nevyužívají IP. V těchto případech je nutné zavést do systému bránu, která bude sloužit jakožto most mezi odlišnými technologiemi a vykonávat potřebné funkce. Zařízení, plnící tuto funkci, jsou často nabízena stejným výrobcem, jako zařízení, vynucující integraci brány do modelu. Většinou z důvodu využití proprietárních protokolů.

Do budoucna se očekává návrh a implementace obecných bran, což může pro koncové uživatele znamenat nižší komplexitu infrastruktury a nižší náklady. Návrh a implementace se mohou stát o to jednodušší, pokud budou v prostředí IoT využívány obecné internetové protokoly, tím se zamezí nutnosti existence bran na úrovni aplikační vrstvy, které by jinak museli existovat k vzájemnému překladu různých aplikačních protokolů. Dalším negativem nuceného využití bran na aplikační vrstvě je také skutečnost, že nasazování takovýchto systému je složitější a náchylnější k chybám.

Tento vzor je typický pro takové chytré objekty, u kterých je požadována schopnost interakce v reálném čase a také možnost vzdálené konfigurace. Je-li bránou mobilní zařízení jako například chytrý telefon, lze uvažovat, že spojení zařízení s bránou může být přerušované, což často bývá případem například u nositelných zařízení, která nevyžadují neustálé připojení k internetu. Z hlediska interoperability jsou chytré telefony zajímavé svým sofistikovaným mechanismem pro doručování aktualizací prostřednictvím obchodů s aplikacemi, to může umožňovat rozšiřovat funkcionalitu nejen telefonu ale v některých případech i cílového zařízení. Díky možnosti vytvářet pro specifická zařízení aplikace na míru je interoperabilita spíše problémem nižší vrstvy.

1.5.4 Model back-end data sharing

Jde o komunikační architekturu, která umožňuje uživatelům exportovat a analyzovat data chytrých objektů v kombinaci s daty z jiných zdrojů. Jde o rozšíření existujícího modelu device-to-cloud, který má v jistých situacích nechtěnou tendenci tvořit datová sila, jelikož zařízení a systémy zastoupené v modelu device-to-cloud zasílají data pouze na platformu konkrétního poskytovatele. Tento model také umožňuje plnit požadavky na přenositelnost dat,

efektivní implementace modelu umožní uživatelům libovolně přesouvat data při změnách IoT služeb. [16]

1.6 Bezdrátové komunikační protokoly

1.6.1 Wi-Fi

Technologie Wi-Fi si prošla od svého vzniku podstatnými změnami a úpravami, každá nová verze s sebou zpravidla přinesla vylepšení z hlediska rychlosti, přenosové vzdálenosti a výkonu. Originální standard 802.11 byl vydán institucí IEEE už v roce 1997 s maximální přenosovou rychlostí 1–2 Mbit/s. S postupným vývojem technologie byla v roce 1999 představena nová verze 802.11b, která umožňovala dosáhnout přenosových rychlostí až 11 Mbit/s, to v kombinaci s nižší cenou vedlo k rapidnímu rozšíření standardu 802.11b jakožto nejpopulárnější bezdrátové technologie svého času. [20]

Standard 802.11a, který byl představen v roce 2012 umožňoval dosáhnout rychlostí až 54 Mbit/s díky využití frekvenčního pásma 5 GHz, využití vyšší frekvence však znamenalo nižší dosah než verze 802.11b/g, které využívají frekvenční pásmo 2,4 GHz. Standard 802.11g, který byl ratifikovaný v roce 2003, umožňoval dosáhnout rychlostí až 54 Mbit/s za využití frekvenčního pásma 2,4 GHz a zachování zpětné kompatibility se zařízeními pracujícími se standardem 802.11b. Verze 802.11n, která vyšla v roce 2009, s sebou přinesla dramatický posun vpřed z hlediska přenosových rychlostí. Tato verze pracuje na frekvenčních pásmech 2,4 GHz i 5 GHz a umožňuje dosáhnout přenosových rychlostí až kolem 600 Mbit/s. Verze 802.11ac, která vyšla v roce 2013, buduje na technologiích využitých ve verzi 802.11n a umožňuje přenosové rychlosti v řádech gigabitů. [20]

V roce 2014 byla vydána verze 802.11af občas také zvaná „White-fi“ nebo „Super Wi-Fi“, která využívá technologie kognitivního rádia k přenosu na nevyužívaných kanálech za minimalizace interference. Využívá frekvenčního pásma v rozmezí 54–790 MHz. [20]

1.6.2 Bluetooth

Vývoj technologie Bluetooth začal koncem roku 1998, když z iniciativy společností Ericsson, IBM, Intel, Nokia a Toshiba došlo k vzniku skupiny Bluetooth Special Industry Group, jejíž cílem byl vývoj a propagace technologie, umožňující bezdrátovou komunikaci na krátké vzdálenosti v pásmu 2,4 GHz. V létě roku 1999 byla společně s dokumentací oficiálně zveřejněna první verze technologie Bluetooth 1.0A. [21]

Technologie využívá rozsahu frekvenčního pásma 2,4–2,485 GHz a rádiové frekvenční kanály jsou rozestaveny po 1 MHz. Komunikace mezi dvěma či více zařízeními probíhá v rámci sítě zvané piconet, jde o ad-hoc síť, která spojuje jedno hlavní zařízení (master), které komunikaci iniciovalo, s jedním až sedmi zařízeními slave. Jedno zařízení může zastávat obě role, ne však v rámci stejného piconetu. Situaci, kdy se tímto způsobem některé piconety překrývají, tj. sdílí alespoň jedno zařízení zastávající obě role, je označována pojmem scatternet. [22]

Zařízení, operující v pásmu, musí být schopné tolerovat ostatní zařízení bez nadměrné interference. K minimalizaci kolizí paketů se využívá upravená forma technologie frequency-hopping spread spectrum (FHSS), zvaná adaptive frequency hopping. Jak již bylo zmiňováno, frekvenční pásmo je rozdělené na jednotlivé kanály, mezi kterými se při přenosu dat přeskakuje. Technologie AHS tento koncept rozvádí ještě dál, kanály, které jsou nadměrně vytížené a rušené jsou dynamicky sledovány a vyřazovány ze sekvence skoků. [23]

V oblasti IoT je obzvlášť důležitá speciální verze technologie, zvaná Bluetooth Low Energy případně také Bluetooth Smart. Tato verze využívá pro komunikaci menší množství kanálů, které jsou rozestaveny po 2 MHz, což umožňuje rychlejší navazování spojení. [22]

1.6.3 Z-Wave

Z-Wave je bezdrátový komunikační protokol, která se převážně využívá pro aplikace chytrých domácností. Běžná síť Z-Wave se skládá z několika zařízení IoT a primárního ovládacího prvku, zvaného smart home hub, který je jako jediný připojený k internetu. Díky využití smíšené topologie a zdrojového směrování je možné signál přeposílat napříč vícero zařízeními, dokud není dosaženo cílového zařízení nebo není přesažen limit skoků, sítě Z-Wave podporují maximálně čtyři skoky. [24]

Technologie funguje na frekvenčím pásmu pod 1 GHz, pro Evropu specificky pásmo 868,42 MHz, vyhýbá se tedy již hustě obsazenému pásmu 2,4 GHz a minimalizuje tak interferenci. Protokol je zamýšlen pro přenos malých datových paketů a nabízí propustnosti 9,6 kbit/s, 40 kbit/s a 100 kbit/s. Nabízí také podporu pro IPv6 a šifrování přenášených dat pomocí šifrování AES128. Dosah signálu je v rozmezí 30-100 m, k dosažení optimální síly signálu se však v praxi doporučuje rozmísťovat od sebe zařízení maximálně na vzdálenosti okolo 15 metrů kvůli tlumícím vlivům zdí a stavebních materiálů. [24]

1.6.4 Zigbee

Zigbee je bezdrátový komunikační protokol, vyvíjený uskupením Connectivity Standards Alliance, dříve Zigbee Alliance, které zahrnuje přes 400 členských společností, mezi které patří například společnosti Apple, Comcast, Google nebo Samsung. [26], [27]

Ke svému fungování využívá specifikaci IEEE 802.15.4, ratifikovanou v roce 2003. Jde o protokol zamýšleny k využití v nízkoenergetických sítí IoT s nízkým datovým tokem a s nízkými provozními náklady. Typicky vyžaduje maximálně 1 mW a za venkovních podmínek poskytuje dosah až 150 m. V Evropě lze provozovat na frekvenčním pásmu 868 MHz, ve kterém dovoluje propustnost až 20 kbit/s, zatímco v Austrálii a v Severní Americe lze využít frekvenčního pásma 915 MHz, pro které je horní hranice propustnosti mírně vyšší s hodnotou 40 kbit/s. Celosvětově je také dostupné pásmo 2,4 GHz, pro které propustnost šplhá až na hodnotu 250 kbit/s. Své využití nachází zejména v oblastech chytrých domácností, podobně jako protokol Z-Wave. [28]

Standard IEEE 802.15.4 využívá 64bitové adresovací schéma v kombinaci s krátkými adresami o délce 16 bitů, to teoreticky umožňuje v rámci jedné sítě Zigbee podporovat přes 65 000 uzlů. [28]

Z hlediska fyzické vrstvy, tj. dle standardu IEEE 802.15.4, můžeme členit zařízení na dva typy. Plně funkční zařízení (FFD – Full Function Device), která mohou vykonávat v rámci standardu všechny nutné funkce včetně funkcí směrování, koordinace. Dalším typem zařízení jsou zařízení s omezenou funkčností (RFD – Reduced Function Device), která implementují pouze omezenou verzi standardu IEEE 802.15.4. Tato zařízení nejsou schopná směrovat pakety a musí být v rámci sítě asociovány se zařízením FFD a slouží jako koncová zařízení vykonávající jednodušší úlohy jako je například měření veličin. [28]

Uzly v rámci vyšších vrstev, které definuje protokol Zigbee, lze logicky členit na tři různé typy. Výčet je zpracován dle zdroje [28]:

- **Koordinátor** – Kořenový prvek sítě Zigbee, v každé individuální sítě je přítomen právě jeden koordinátor, který zodpovídá za inicializaci sítě, volí například využívaný kanál a unikátní identifikátor sítě. Může také ukládat informace o síti a bezpečnostních klíčích. Slouží také jako most mezi sítí Zigbee a případnou externí sítí.
- **Směrovač –** Směrovače slouží v síti Zigbee jako mezičlánky, sloužící k přenosu dat z ostatních zařízení, mohou se připojovat k již existujícím sítím.

- **Koncová zařízení –** Slouží jako zdroje dat, většinou jde o zařízení napájená baterií, nebo s nízkou spotřebou energie. Implementují dostatečnou funkcionalitu na komunikaci s nadřazeným prvek, kterým je buď směrovač, nebo koordinátor. Redukovaná funkcionalita umožňuje minimalizovat cenu, tato zařízení nemusí na rozdíl od zbylých dvou být aktivní po celou dobu setrvání v síti.

1.7 Technologie pro komunikaci na aplikační vrstvě

1.7.1 HTTP

Protokol HTTP neboli Hypertext Transfer Protokol, je základním stavebním kamenem celosvětové sítě WWW – World Wide Web. Za jeho vznik je odpovědný Tim Berners-Lee, který v roce 1989 sepsal návrh na implementaci hypertextového systému napříč internetem. Původně se projekt nazýval Mesh, během implementace v roce 1990 došlo k přejmenování na již známý World Wide Web. [29]

Protokol si prošel několika verzemi, prvotní verze HTTP/0.9 byla velmi jednoduchým prototypem, požadavky byly jednořádkové a umožňovaly pouze využití metody GET. Verze HTTP/1.0 s sebou přinesla koncept hlaviček dotazů i odpovědí, další novinkou bylo zahrnutí statusového kódu v odpovědi, díky čemuž mohly prohlížeče rozpoznávat úspěch či selhání daného požadavku. Tato rozšíření byla postupně vydávána v průběhu let 1991–1995. [29]

Současně s prací na HTTP/1.0 probíhala i snaha o standardizaci a na začátku roku 1997 byla vydána verze HTTP/1.1, která byla první standardizovanou verzí. K další převratné změně došlo roku 1994, kdy byla společností Netscape Communications uvedena nová vrstva, vložená mezi vrstvu transportní (TCP/IP) a aplikační (HTTP), tato vrstva zvaná SSL neboli Secure Socket Layer, sloužila k šifrování komunikace, a později byla standardizována ve formě Transport Layer Security – TLS. [29]

Protokol je bezstavový, využívá struktury klient-server a komunikačního modelu request-response, na server jsou zasílány dotazy, které server zpracovává a posílá na ně odpovědi. [30]

1.7.2 MQTT

Protokol byl vytvořen v roce 1999 autory Andy Standford-Clark a Arlen Nipper. Vznikl z potřeby propojit ropovod prostřednictvím satelitu co nejefektivnějším způsobem. Protokol byl navržen tak, aby efektivně využíval šířku pásma, aby byl jednoduchý na implementaci a nenáročný na provoz, aby podporoval rozličné datové formáty, aby během přenosu zajišťoval mechanismy QoS a aby byl schopný udržovat informace o konkrétní relaci. V době vydání

nebyl protokol veřejně dostupný, byl proprietárním vlastnictvím firmy IBM, která jej využívala interně. První veřejně dostupná verze, kterou bylo možné využívat bez poplatku, byla verze MQTT 3.1 zveřejněná v roce 2010. [31]

Komunikační vzor publish-subscribe, který je v MQTT využiván, poskytuje alternativu k tradičnímu komunikačnímu vzoru klient-server, ve kterém dochází k přímé komunikaci mezi klientem a koncovým bodem. Architektura publish-subscribe umožňuje oddělit klienta, který zprávu odesílá (publisher), od klienta nebo klientů, kteří zprávy přijímají (subscriber). Pár publisher-subscriber nikdy nekomunikuje napřímo, klienti si dokonce ani nepotřebují být vědomí existence druhé strany. Veškerou komunikaci zajišťuje prostředník – broker, jehož úkolem je filtrace zpráv a jejich korektní distribuce zainteresovaným odběratelům. [32]

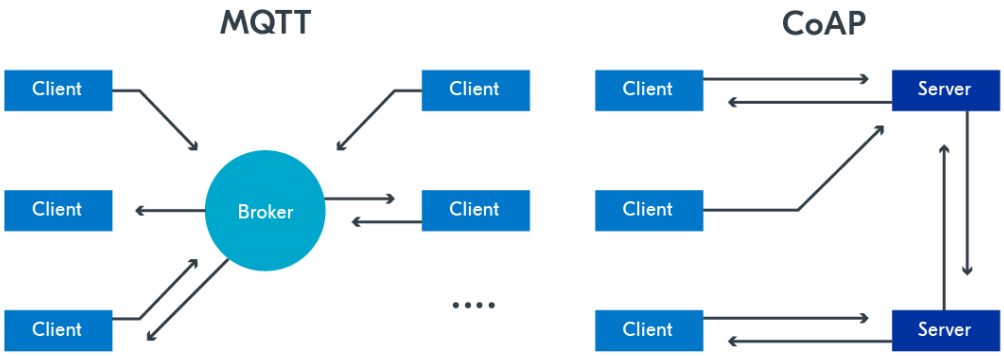
Technologie je častokrát mylně pojímána jakožto fronta zpráv, pravděpodobně z části názvu MQ, ta se občas špatně vykládá jakožto Message Queue. Název je však ve skutečnosti přejat z produktu MQSeries od firmy IBM. Mezi technologií fronty zpráv a MQTT jsou zásadní rozdíly. Fronta zpráv skladuje zprávy do té doby, než jsou konzumovány, v případě, že zprávu nikdo nekonzumuje, zpráva setrvává ve frontě. Není možné tak pohodlně zprávy ignorovat tak jednoduchým způsobem, jako v MQTT, kde stačí dosáhnout situace, kdy specifické téma nemá žádného odběratele. Tradiční fronty zpráv umožňují zprávu konzumovat právě jednomu klientovi, chování v rámci MQTT je odlišné, zprávu obdrží každý odběratel daného tématu. Fronty zpráv jsou méně flexibilní. Před vlastním využitím fronty zpráv, je potřeba danou frontu explicitně vytvořit, MQTT je v tomto ohledu více flexibilní a umožnuje vznik témat stylem ad-hoc. [32]

1.7.3 CoAp

Protokol CoAp neboli Contrained Application Protocol, je specializovaný přenosový protokol, zamýšlený pro využívání v nízkopříkonových a ztrátových sítích, jejichž uzly mají typicky k dispozici omezené prostředky, což je velmi užitečné zejména v oblasti IoT. Mezi typické oblasti využití patří automatizace budov či využití v oblasti chytré energetiky. [33]

Interakční model protokolu CoAp je velmi podobný protokolu HTTP, klient zasílá požadavky, které pomocí kódu metody definují akci k provedení nad některým zdrojem na serveru. Zdroj je možné identifikovat pomocí URI – Uniform Resource Identifier. Server po zpracování požadavku posílá odpověď se statusovým kódem. Na rozdíl od protokolu HTTP, který typicky běží na TCP, jsou v protokolu CoAP tyto výměny řešeny asynchronním

způsobem pomocí přenosu založeném na datagramech (např. UDP). Protokol je navržen tak, aby byla možná pohodlná spolupráce s protokolem HTTP. [33], [34]



Obrázek 3: Srovnání architektury protokolů CoAP a MQTT. [34]

2 SÍTĚ LPWA

Vypracováno podle zdrojů [35], [36].

V posledních letech se pro rozvoj IoT staly klíčové technologie LPWAN, celým jménem Low Power Wide Area Network, jde o sítě, které jsou speciálně navržené tak, aby umožňovaly dlouhodobé, bezdrátové připojení mezi různými zařízeními na velké vzdálenosti za minimální spotřeby energie. Tato kombinace je zásadní pro zajištění dlouhodobého provozu zařízení IoT, která mohou být umístěna v odlehlých nebo těžko dostupných oblastech, kde je nutností využívat jako zdroj napájení baterie.

Principem sítí LPWA je možnost komunikace na velké vzdálenosti (řádově jde o desítky kilometrů) za velmi nízké spotřeby energie, čehož je dosaženo díky specializaci na přenos malého množství dat bez nutnosti vysokorychlostního přenosu. Těmito charakteristikami nabývají odlišnosti od tradičních celulárních sítí, které jsou optimalizovány pro vysokorychlostní přenos velkého množství dat za ceny vyšší spotřeby energie. Dalším nedostatkem tradičních celulárních sítí vzhledem k využití v prostředí IoT je jejich vyšší pořizovací cena, jelikož celulární zařízení musí být schopná zpracovávat komplexní signál optimalizovaný pro vysokorychlostní přenos dat.

Principy LPWA sítí tedy spočívají v akceptaci vyšší latence a nižší přenosové rychlosti v zájmu energetické a cenové efektivity a možnosti přenášet malý objem dat na velké vzdálenosti. Z těchto vlastností také vyplývá skutečnost, že tyto technologie není vhodné aplikovat v případech, kdy je vyžadováno přenosu velkého množství dat za minimalizace latence, což může být typické například pro automobilové komunikační systémy.

2.1 Cíle a techniky návrhu

Kapitola byla vypracována podle zdroje [36].

2.1.1 Komunikace na velké vzdálenosti

Pro technologie LPWAN je vyžadována nejen schopnost pokrytí velkých vzdáleností ale také velmi dobrá schopnost šíření signálu ve vnitřních prostorech, které mohou být těžce dosažitelné. V porovnání s tradičními celulárními systémy je cílem, nabízet v těchto situacích až o 20 dB vyšší sílu signálu, čehož je docíleno následujícími technikami:

- **Využití nízkofrekvenčního pásma** – Většina sítí LPWA využívá pásmo Sub-GHz, které umožňuje spolehlivou a energeticky nenáročnou komunikaci. Signály nižší frekvence totiž při přítomnosti překážek zaznamenávají menší útlum a menší míru

vícecestného šíření, které může degradovat kvalitu signálu. Dalším důvodem volby pásma je také skutečnost, že mnoho populárních, bezdrátových komunikačních technologií (Wi-Fi, Bluetooth, Zigbee) využívá pásma 2,4 GHz a nižší pásmo je tak méně obsazené, to slouží k minimalizaci interference.

- **Modulace signálu –** V městském prostředí je pomocí technologií LPWAN umožněna komunikace na vzdálenosti jednotek kilometrů, ve venkovském prostředí až na vzdálenosti desítek kilometrů. Sítě jsou navrženy tak aby energetická bilance spojení dosahovala zhruba hodnoty 150 dB. Fyzická vrstva volí nižší modulační rychlost, což umožňuje pro každý přenášený symbol generovat silnější signál, díky čemuž mohou přijímače úspěšně dekódovat i výrazně tlumený signál přenášený na větší vzdálenosti.

2.1.2 Energeticky nenáročná komunikace

Pro snížení nákladů, spojených s údržbou a provozem zařízení, je žádoucí zprostředkovávat komunikaci za co nejvyšších energetických úspor (s ohledem na plnění ostatních požadavků). Zařízení napájená baterií by měla být provozuschopná až po dobu deseti let. Splnění zmiňovaného cíle je umožněno díky specifickým technikám:

- **Volba topologie** – Smíšená topologie, jejíž využití je typické pro bezdrátové sítě krátkého dosahu, není pro účely propojení velkého množství geograficky vzdálených zařízení ideální volbou, důvodem je nejen komparativně vysoká pořizovací cena ale také tendence nadměrně zatěžovat konkrétní uzly při směrování síťového provozu (s dopadem na provozuschopnost zařízení z důvodů vyčerpání energie). Jako efektivní řešení se tudíž nabízí přímé propojení koncových zařízení se základnovými stanicemi, výsledkem je využití topologie hvězdy, zařízení tak nemusí naslouchat síťovému provozu od ostatních zařízení za účelem přesměrování, což s sebou přináší významné energetické úspory

- **Duty cycling –** Pojem duty cycling označuje situace, kdy dochází ke střídavému vypínání a zapínaní energeticky náročných komponent, zejména jde o datový transceiver. Duty cycling je možné přizpůsobit případům užití daného zařízení, v případech, kdy zařízení potřebuje pouze odesílat data, stačí aktivovat vysílač před samotným vysíláním dat. Nastane-li situace, kdy zařízení nejen potřebuje data posílat, ale také naslouchat příchozím zprávám, může se volit postup domluvy naslouchacího rozvrhu s danou základnovou stanicí. Zařízení poté aktivuje transceiver ve specifických dohodnutých časových okamžicích.

- **Odlehčené řízení přístupu k médiu –** Většina protokolů pro řízení přístupu k médiu (MAC – Media Access Control) využívaných pro celulární sítě nebo pro bezdrátové sítě nízkého rozsahu je pro použití v sítích LPWA příliš komplexní. Samotná synchronizace potřebná ke korektnímu fungování některých z těchto protokolů může být dokonce náročnější než neobjemný a nečastý přenos dat typický pro sítě LPWA. Přesná synchronizace, kterou tato schémata vyžadují, může také být nad rámec schopností extrémně levných zařízení, která jsou často využívána v rámci sítí LPWA. Z těchto důvodů se pro sítě LPWA často volí jednoduchá schémata náhodného přístupu. Sítě jako jsou Sigfox nebo LoRaWAN volí protokol s náhodným přístupem zvaný Aloha, zatímco sítě NB-IoT nebo Ingenu volí cestu protokolů založených na časovém multiplexingu (TDMA –Time division multiple access).
- **Přesun odpovědností ze zařízení –** Dobrým způsobem, jak snižovat složitost koncových zařízení a šetřit spotřebu energie je přesun složitých úkonů jako je zpracování signálů a dat na jiné systémy.

2.1.3 Cenová dostupnost

Úspěch sítí LPWA spočívá v jejich schopnosti propojovat velký počet cenově dostupných koncových zařízení, mimo již zmiňovaných technik, tj. využití topologie hvězdy a přesun odpovědností pryč ze zařízení, se využívají také následující přístupy:

- **Redukce složitosti hardwaru –** Oproti celulárním sítím a sítím nízkého rozsahu není potřeba pracovat s komplexním signálem, to umožňuje výrobcům navrhovat poměrně jednoduché a cenově dostupné součástky.
- **Minimální infrastruktura –** Díky vysokému dosahu stačí k propojení desítek tisíc koncových zařízení jedna základnová stanice, to umožňuje relativně levný provoz sítě.
- **Využití bezlicenčního frekvenčního pásma** – Cena spojena s licencováním nového pásma je v přímém rozporu s požadavky levného síťového provozu a cenové dostupnosti, proto je většina sítí LPWA provozována na nelicencovaném pásmu ISM.

2.1.4 Škálovatelnost

Schopnost propojovat velké množství zařízení, která přenáší málo objemná data je pro sítě LPWA klíčovým požadavkem, k plnění tohoto cíle se využívá několika různých technik:

- **Diversifikace –** Pro podporu připojení co největšího počtu zařízení je nutností efektivně využívat dostupné prostředky jako jsou čas, dostupné komunikační kanály a dostupný

hardware. Efektivní využití těchto prostředků může být výpočetně či technologicky náročné a hardware levných koncových zařízení těmto požadavkům nemusí vyhovovat. Z toho důvodu se využívá kooperace výkonnějších komponent celého systému jako jsou například základnové stanice a systémy zpracování dat. Technologie LPWAN využívají vícekanálovou komunikaci a k přenosu se také využívá vícero antén, což umožňuje paralelizovat přenos dat. Dalšími důsledky jsou také navýšení spolehlivosti komunikace pomocí redundantních přenosů a zvýšená odolnost vůči interferenci.

- **Zahuštění sítě –** Dalším způsobem, pomocí kterého je možné v dané oblasti poskytovat připojení většímu množství zařízení, je navýšení počtu základnových stanic. Tento přístup je typický pro tradiční celulární sítě, pro které však existují sofistikované technologie, které umožňují hustý výskyt základnových stanic za minimalizace interference. Pro efektivní využití zmiňovaného postupu v oblasti sítí LPWA tak vyvstává potřeba vývoje nových technologií.
- **Adaptivní výběr kanálu a přenosové rychlosti –** Sítě LPWA musí podporovat velký počet připojených zařízení, zároveň je také potřeba optimalizovat parametry jednotlivých spojení v zájmu spolehlivé a energeticky efektivní komunikace. Efektivní úprava parametrů daného spojení vyžaduje jeho monitorování a také koordinaci mezi koncovým zařízením a základnovou stanicí. Uplatnění zmiňovaných mechanismů může být omezováno v závislosti na specifické technologii LPWAN a v důsledku mohou být volené jednodušší mechanismy pro zajištění spolehlivosti, příkladem může být opakovaný přenos. Většina LPWA sítí umožňuje přístup k médiu nekoordinovaným a náhodným přístupem, aby se zachovala jednoduchost koncových zařízení, tato charakteristika se však jeví jako faktor, který může omezovat míru škálovatelnosti těchto technologií.

2.2 Přehled vybraných sítí LPWA

Následující podkapitola zahrnuje přehled a charakteristiku vybraných sítí LPWA, přičemž technologiím LoRa a LoRaWAN je věnována samostatná kapitola.

2.2.1 NB-IoT

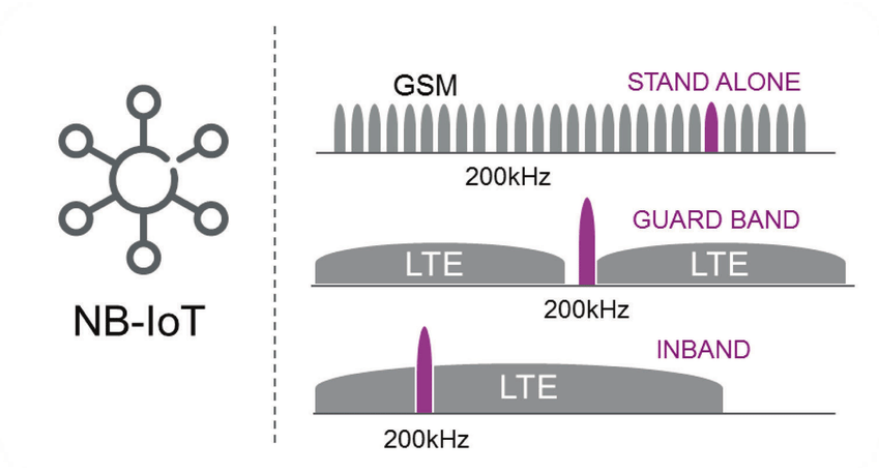
Jde o standard vyvinutý skupinou 3GPP a v roce 2016 vydaný jako součást 13. vydání standardů, jednalo se o nový rádiový přístupový systém využívající existujícího standardu LTE. Funkcionalita standardu LTE však byla redukována na minimální přípustnou úroveň v zájmu cenových a energetických úspor pro koncová zařízení, lze říci, že ze standardu byla vybrána

pouze funkcionalita efektivně využitelná v prostředí IoT. Mezí návrhové cíle specifikace patří pokrytí MCL 164 dB a podpora až 50 000 koncových zařízení pro každou buňku s možností navýšení kapacity pomocí přidání dalších nosičů. [36], [37]

Šířka pásma NB-IoT je 200 kHz, což odpovídá jednomu zdrojovému bloku v sítích GSM, LTE. Uplink spojení využívá technologii SC-FDMA (single-carrier frequency division multiple access) a downlink spojení využívá technologi OFDMA (Orthogonal Frequency Division Multiple Access). Pro komunikaci uplink, tj. odchozí ze zařízení, činí přenosová rychlost 20 kbit/s, zatímco komunikace downlink, tj. příchozí do zařízení, zvládá přenosovou rychlost až 250 kbit/s. Zařízení napájené z akumulátoru, které za den přenese v průměru data o velikosti 200 bajtů, by mělo vydržet v provozu až po dobu deseti let. [36]

Díky interoperabilitě s technologiemi LTE,GSM nabízí dle zdroje [37] síť NB-IoT provoz ve třech režimech:

- **Stand-alone** – část spektra GSM se nahradí nosičem NB-IoT.
- **Guard band operation –** používá se nevyužitá část ochranného pásma LTE.
- **In-band operation –** přímé využití zdrojových bloků LTE.



Obrázek 4: Možnosti nasazení NB-IoT. [38]

2.2.2 Weightless

Technologie byla původně vyvinuta společností Neul, což byl britský startup sídlící v Cambridge. který se specializoval na technologie bezdrátových komunikací. První verze technologie byla představena v roce 2011 a byla navržena tak, aby využívala nevyužitých kanálů vyhrazených pro televizní vysílání, tzv. white space. [39], [40]

V minulosti technologie představovala sadu tří standardů Weightless-W, Weightless-N a Weightless-P pod správou organizace Weightless Alliance, dříve zvané Weightless Special Interest Group, která i nadále podporuje rozvoj standardu. Jako nejslibnější se však jevila verze Weightless-P, která byla skupinou přejmenována čistě na Weightless a v dnešní době soustředí skupina svoji pozornost právě na tuto centrální technologii. [41], [42]

Specifikace Weightless-W budoval na základech technologie vyvíjené zmiňovanou společností Neul, využití volných kanálů vyhrazených pro televizní vysílání však s sebou přinášelo jisté komplikace. V odlišných geografických oblastech může být využití daného pásma omezováno regulacemi a samotné pásmo nemusí být všude dostupné. Dalším problémem je návrh koncových uzlů, které jsou typicky zamýšlené pro fungovaní ve specifické části daného spektra. Dostupné kanály se však také mohou lišit svojí frekvencí, v konkrétní lokaci může být například dostupný kanál 500 mHz, zatímco jiná lokace zpřístupňuje kanál 700 mHz, tato skutečnost značně komplikuje návrh jednotného systému, který by byl schopný se těmto specifikám přizpůsobit. [39] Technologie využívá širokou škálu modulačních schémat, faktorů šíření a velikostí paketů. V závislosti na charakteristice spojení by technologie měla umožňovat obousměrný přenos dat o rychlostech v rozmezí 1 kbit/s až 10 Mbit/s a umožňovat spojení až na vzdálenosti 5 km. Kvůli velké sadě funkcí protokolu je výdrž zařízení napájených akumulátorem odhadována na dobu tří let, přičemž jejich pořizovací cena je ve srovnání s alternativami poněkud vyšší. [43] Technologie nachází využití zejména v oblastech chytré těžby a distribuce plynu a ropy. [39]

Specifikace Weightless-N je technologie pracující na ultra úzkém pásmu (UNB), využívající modulačního schématu DBPSK, umožňujícího jednosměrnou komunikaci o rychlosti 100 bit/s na vzdálenosti obdobné technologii Weightless-W. Specifikace je vhodná zejména pro využití k odesílání dat ze senzorů. Díky jednoduchosti technologie jsou koncová zařízení charakteristická nízkou pořizovací cenou a při napájení akumulátorem by měla být provozuschopná až po dobu deseti let. [43]

Specifikace Weightless-P, v dnešní době již známá čistě pod jménem Weightless, je technologie odvozená od komunikačního protokolu Platanus společnosti M2Communications. Technologie využívá kanály o šířce 12,5 kHz s řízením přístupu pomocí FDMA (Frequency Division Multiple Access), TDMA. Umožňuje provoz v pásmu ISM i v licencovaném pásmu. Využívá úzkopásmových modulačních schémat GMSK (Gaussian Minimum Shift Keying) a OQPSK (Offset Quadrature Phase Shift Keying), díky čemuž je možná energeticky efektivní komunikace s adaptivní přenosovou rychlostí od 200 bit/s až k 100 kbit/s. Technologie je zaměřená zejména na využití v průmyslových odvětví, prioritou je tedy spolehlivost. Mezi klíčové vlastnosti patří automatické přeposílání zpráv při selhání doručení, oboustranně potvrzovaná komunikace, provádění frekvenčních skoků za účelem minimalizace rušení, využití dopředné korekce chyb (FEC – Forward Error Correction) a podpora pro roaming a handover. Ve srovnání s ostatními specifikacemi nabízí nižší dosah okolo 2 km. Kvůli relativní složitosti umožňuje provozuschopnost pro zařízení napájená akumulátorem zhruba po dobu tří let. [43], [44]

Ve všech zmiňovaných specifikacích bylo k zabezpečení komunikace využito šifrování AES128. [43]

2.2.3 Ingenu

Zpracováno podle zdroje [45].

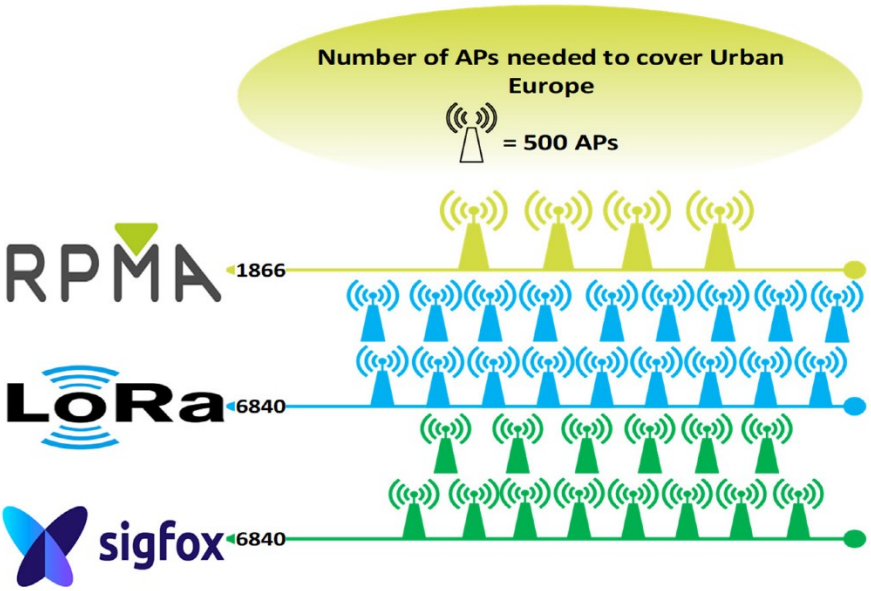
Platforma je založená na proprietární technologii random phase multiple access (RPMA), která byla patentována v roce 2010 společností Ingenu. Každý přístupový bod umožnuje pokrýt oblast o rozloze až 300 čtverečních mílí, což je v porovnání s celulárními sítěmi značný rozsah.

Technologie byla od základu vyvinuta společností Ingenu a využívá nových modulačních technik, které snižují náklady na provoz a poskytují podporu pro větší počet zařízení a vyšší plochu pokrytí. Díky optimalizaci citlivosti přijímače je možné dosáhnout vysoké kvality signálu bez ztráty kapacity pro koncová zařízení. Koncová zařízení také mohou upravovat energii využívanou k přenosu a minimalizovat tak vzájemnou interferenci. Navzdory těmto výhodám může docházet k rušení, jelikož technologie využívá již velmi obsazené frekvenční pásmo 2,4 GHz.

RPMA umožňuje současnou demodulaci až 1200 signálů, v případě, že jsou vysílány na stejné frekvenci. Mezi přístupovým bodem a koncovým zařízením je udržována striktní synchronizace, aby bylo zajištěno, že koncová zařízení vysílají signál, který se vejde do specifikovaných rámců o konkrétní velikosti. Koncová zařízení vysílají signály s náhodným

zpožděním, které je dopočítáno tak, aby nedošlo k překročení velikosti rámce, ve kterém je signál vysílán.

Technologie RPMA umožňuje obousměrnou komunikaci, avšak je pozorovatelná mírná asymetrie. Během downlink komunikace rozdělují přístupové body signály pro jednotlivá koncová zařízení pomocí CDMA (Code Division Multiple Access).



Obrázek 5: Srovnání pokrytí pomocí technologií RPMA, LoRa, Sigfox. [45]

3 LORA A PROTOKOL LORAWAN

3.1 LoRa

LoRa je označení pro proprietární modulační techniku, využitelnou v oblasti sítí LPWA. Název vychází ze slov long range a vystihuje tak jednu z klíčových charakteristik technologie – možnost komunikace na velké vzdálenosti. Jako ostatní již zmiňované technologie využívané v prostředí sítí LPWA se také zaměřuje na energeticky efektivní přenos malého počtu dat. Výdrž koncových zařízení implementujících technologii LoRa by měla, v případě napájení akumulátorem, dosahovat až doby 10 let. [46]

Technologie vznikla ve francouzské společnosti Cycleo, původně měla umožňovat bezdrátovou komunikaci vodoměrů, plynoměrů a elektroměrů. Za tímto účelem došlo k využití již existující modulační technologie Chirp Spread Spectrum (CSS), která byla v té době využívána primárně v radarových a sonarových systémech. Společnost Cycleo byla v roce 2012 odkoupena společností Semtech a v roce 2015 vznikla skupina LoRa Alliance, která doposud technologii spravuje. [47]

3.1.1 Modulace

Technologie LoRa využívá proprietární modulační techniku odvozenou od existující technologie Chirp Spread Spectrum. K přenosu dat využívá princip generování chirp signálů, přičemž chirp je sinusový pulz, jehož frekvence buď lineárně stoupá (up-chirp) nebo klesá (down-chirp). Díky linearitě pulzů je frekvenční posun mezi vysílačem a přijímačem úměrný časovým posunům, které lze jednoduše odstranit v dekodéru. Díky této vlastnosti je technologie také odolná vůči Dopplerovu jevu, což umožňuje využití pro pohyblivá zařízení. Frekvenční posun může dosahovat až 20% šířky pásma bez znatelného vlivu na výkonnost dekódování, tato skutečnost umožňuje levnější výrobu vysílačů. [48]

Přenos jednoho symbolu trvá poměrně dlouhou dobu, což znamená, že technologie je rezistentní vůči krátkodobé interferenci vznikající aktivitou systému implementujících technologii FHSS. Případné chyby zavedené do komunikace je také možné opravit pomocí využití dopředné korekce chyb. [48]

Dle zdroje [48] lze modulaci upravovat pomocí modifikace následujících parametrů:

- **Šířka pásma (Bandwith) –** Podporuje hodnoty 125 kHz nebo 500 kHz. Vyšší šířka pásma (za fixního činitele rozprostření) umožňuje větší přenosovou rychlost za cenu snížení citlivosti přijímače. [46]

- **Činitel rozprostření (Spreading Factor) –** Udává kolik pulzů je využito pro přenesení jednoho symbolu, přičemž délku sekvence pulzů uvádí vztah 2^{SF}. Při využití vícero pulzů dochází k rozprostření energie signálu napříč frekvenčním spektrem, to umožňuje přijímači rozlišovat signály s horším poměrem signálu a šumu (SNR – Signal-to-noise ratio). [46]

Tabulka 2: Vliv činitele rozprostření na datový tok a dosah. [46]

Činitel rozprostření (SF)	Datový tok (bitrate)	Dosah
SF10	980 bit/s	8 km
SF9	1760 bit/s	6 km
SF8	3125 bit/s	4 km
SF7	5470 bit/s	2 km

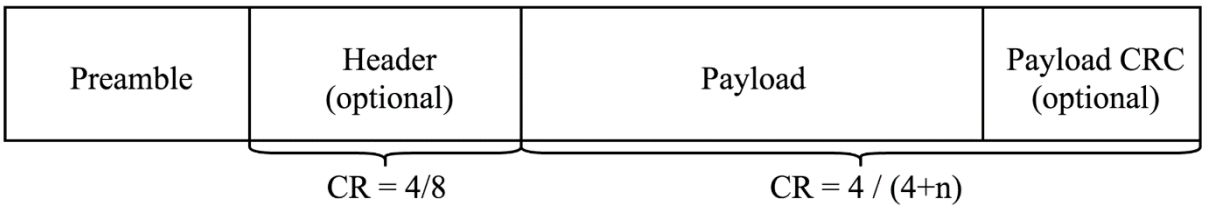
Kódový poměr (Code rate) – Vyjadřuje míru redundance v přenášené informaci, která slouží k opravě případných chyb. Pro protokol LoRaWAN nabývá fixní hodnoty 4/5 (jeden paritní bit pro čtyři datové). [46]

3.1.2 Struktura rámce

Vypracováno podle zdroje [48]

Struktura rámce je znázorněna na obrázku 6. První část zvaná preamble začíná sekvencí konstantích pulzů up-chirp, které pokrývají celé frekvenční pásmo. Poslední dva pulzy up-chirp kódují tzv. sync word (kódové slovo), jde o hodnotu o velikosti jednoho bajtu, která slouží k rozlišení odlišných sítí využívajících stejného frekvenčního pásma. Zařízení naslouchají pouze zprávám, které obsahují vybrané kódové slovo.

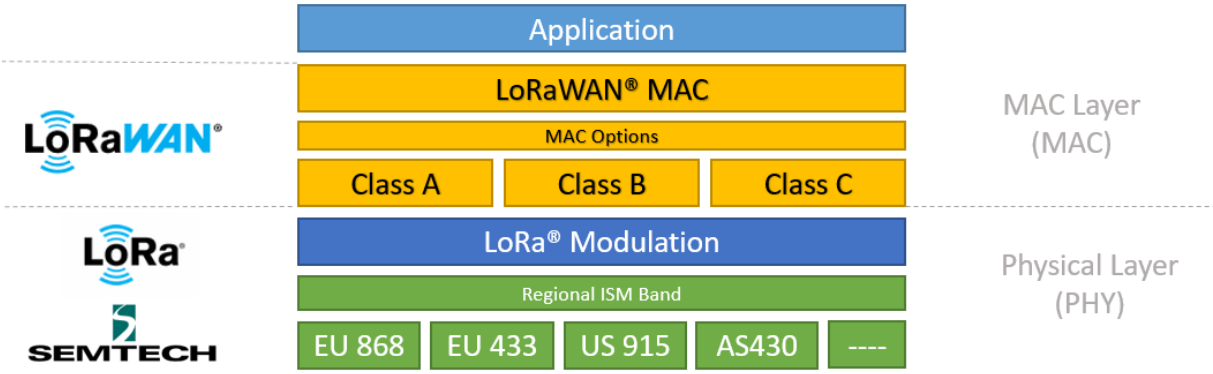
Další částí je volitelná hlavička, která využívá kódový poměr 4/8, obsahuje informace o velikosti datového obsahu (payload) v bajtech, o použitém kódovém poměru a dává vědět, jestli je rámec zakončen polem cyklického redundantního součtu (CRC). Pomocí kontrolního součtu je možné zkontrolovat, byl-li rámec přenesen bez chyb. Samotná hlavička také obsahuje kontrolní součet. V případě, že se uvedená hodnota CRC neshoduje s vypočítanou hodnotou, je rámec zahozen. Informace přenášené v hlavičce mohou být předem známé, v tom případě není potřeba hlavičku do rámce zahrnovat.



Obrázek 6: Struktura rámce LoRa. [48]

3.2 LoRaWAN

LoRaWAN představuje komunikační protokol vyšší vrstvy, který umožňuje obousměrnou bezdrátovou komunikaci na velké vzdálenosti. Na rozdíl od proprietární technologie LoRa je protokol LoRaWAN otevřeným standardem. Za správu protokolu zodpovídá skupina LoRa Alliance. [46]



Obrázek 7: Rozdělení LoRa a LoRaWAN. [46]

Síť LoRaWAN dle zdroje [46] obsahuje několik různých prvků:

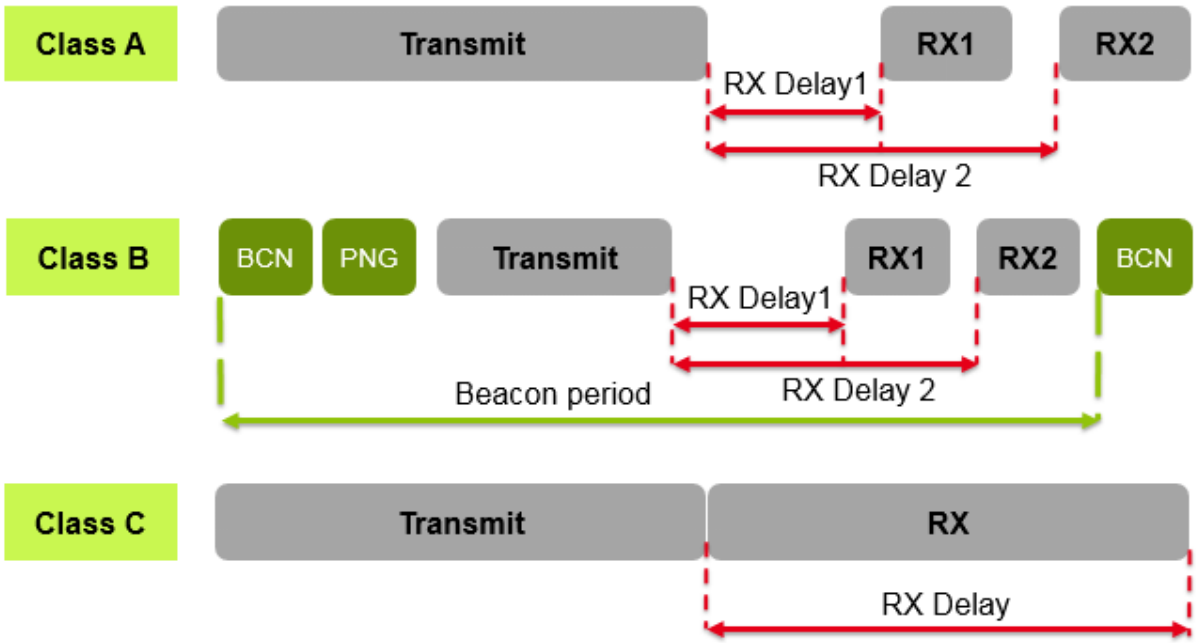
- **Koncové zařízení** – Představuje jej senzor nebo akční prvek, který je pomocí brány bezdrátově připojen do sítě LoRaWAN.
- **Brána** – Naslouchá zprávám z koncových zařízení a kontroluje jejich integritu. V případě, že je zpráva v pořádku, brána přidává ke zprávě dodatečná metadata (časové razítko, indikátor síly přijímaného signálu) a přeposílá jí na síťový server. Zprávy z jednoho koncového zařízení jsou zpracovávány všemi branami v dosahu.
- **Síťový server** – Zprostředkovává doručení zprávy korektní aplikaci, zodpovídá za správu a řízení komunikace v rámci sítě. Zajišťuje zabezpečení zpráv a kontroluje autenticitu koncových zařízení. Požadavky koncových zařízení na vstup do sítě přeposílá na join server.

- **Aplikační server –** Zpracovává a vyhodnocuje doručená data.
- **Join Server –** Spravuje proces připojení koncového zařízení do sítě. O každém zařízení udržuje následující informace: DevEUI které slouží jako unikátní identifikátor koncového zařízení. AppKey a NwkKey což jsou klíče, sloužící k šifrování komunikace. Dále server také udržuje identifikátor konkrétního aplikačního serveru a servisní profil zařízení.

3.2.1 Koncová zařízení

Vypracováno dle zdroje [46].

Pojem označuje uživatelská zařízení, která jsou bezdrátově připojena do sítě LoRaWAN. Podle požadavků kladených ze strany aplikace je lze dělit na tři třídy. Všechna koncová zařízení musí podporovat funkcionalitu třídy A. Zařízení třídy B musí podporovat také funkcionalitu třídy A. Zařízení třídy C musí podporovat funkcionalitu tříd A i B. Mezi konkrétním zařízením a bránou neexistuje fixní vztah, tudíž jedno zařízení může být obslouženo vícero branami zároveň.



Obrázek 8: Komunikace koncových zařízení sítě LoRaWAN. [49]

Třída A

Zařízení je typicky v úsporném režimu, v reakci na monitorovaný jev přechází do pohotovostního režimu a iniciuje přenos zprávy. Po dokončení přenosu zprávy uplink naslouchá zařízení po nastavitelný časový interval, typicky po dobu jedné sekundy, příchozím zprávám. Po uplynutí intervalu přechází zařízení opět do úsporného režimu, ze kterého se za

určitý časový interval opět probudí a opět naslouchá. Mimo tato dvě okna není možné se zařízením komunikovat. Zařízení se nepokusí o poslání další zprávy uplink dokud buď nebyla přijatá zpráva downlink, nebo nevypršelo druhé okno k přijetí zprávy.

Třída B

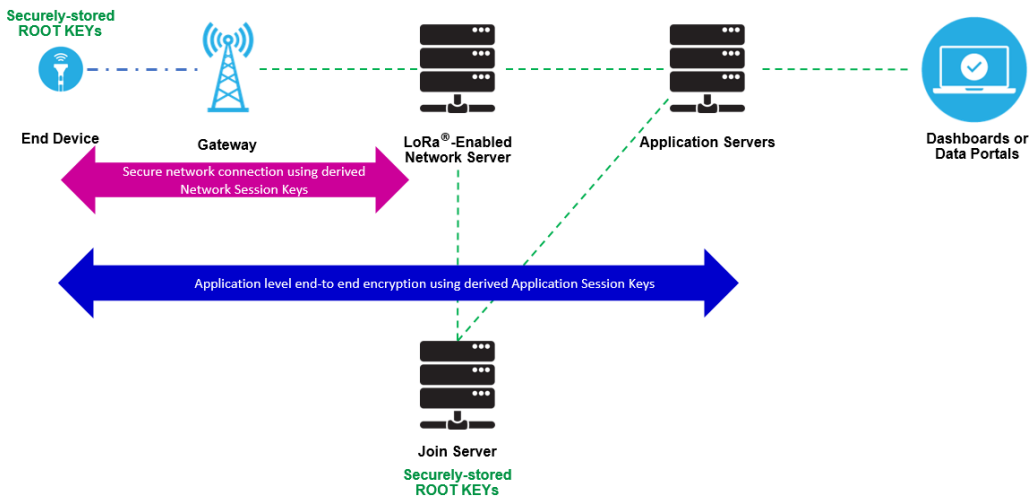
Zařízení třídy B (Beacon) rozšiřují chování třídy A o předdefinované časové intervaly, zvané ping slot, během kterých naslouchají příchozím zprávám. Za účelem synchronizace vysílají brány pravidelně zprávy, pomocí kterých mohou koncová zařízení upravit svůj interní čas, aby byly jejich naslouchací intervaly korektně synchronizované. Zmiňovaný proces se označuje jako beaconing.

Třída C

Zařízení této třídy naslouchají příchozím zprávám neustále, tento proces zajišťuje nejnižší latenci, ale je energeticky náročný, tudíž je vhodnější pro zařízení napájená ze sítě.

3.2.2 Zabezpečení

Síť využívá koncového šifrování pro zabezpečení datového obsahu vyměňovaného mezi aplikačním serverem a koncovým zařízením. Využívá šifrování AES128. Síťový server zodpovídá za kontrolu integrity zpráv a jejich následné přesměrování aplikačnímu serveru, který je schopný obsah dešifrovat pomocí odvozeného klíče. Systém využívá 128bitových klíčů AppKey (Application Key) a NwkKey (Network Key), ze kterých jsou odvozeny dočasné klíče AppSKey a NwkSKey, princip fungovaní je vystižen na obrázku 9. [46], [50]



Obrázek 9: Zabezpečení komunikace v rámci sítě LoRaWAN. [46]

3.2.3 Aktivace zařízení

Během aktivace je zařízení vybaveno parametry DevAddr, NwkSKey a AppSKey. NwkSKey je uložen na zařízení a na síťovém serveru, zatímco AppSKey je uložen na zařízení a na aplikačním serveru – jak vystihuje obrázek 9. Parametr DevAddr slouží k identifikaci zařízení v rámci síťového serveru, obsahuje prefix AddrPrefix sloužící k identifikaci sítě. Zařízení je možné aktivovat dvěma způsoby. [50]

Activation by Personalization (ABP)

Koncové zařízení je vázáno ke specifické síti. DevEUI, DevAddr, NwkSKey i AppSKey jsou uloženy přímo na zařízení. Zařízení je tedy připraveno okamžité komunikace v rámci sítě a není tak třeba procedury připojování. [50]

Over the Air Activation (OTAA)

Složitější a bezpečnější metoda, díky které není zařízení vázáno na konkrétní síť. Koncové zařízení posílá zprávu Join Request, ve které uvádí hodnoty JoinEUI, DevEUI a DevNonce. JoinEUI je identifikátor join serveru, který udržuje informace o daném zařízení. DevEUI je unikátní identifikátor koncového zařízení. DevNonce je čítač, který je inkrementován v každé zprávě Join Request. Kladná odpověď serveru – Join Accept – obsahuje parametry DevAddr, síťový identifikátor NetID a čítač JoinNonce. Následně dochází ke generaci odvozených klíčů. [46], [50]

4 NÁVRH SYSTÉMU

4.1 Požadované vlastnosti

Cílem práce je vytvoření aplikace, pomocí které je možné zobrazovat stav vnitřního klimatu objektu. Data budou získávána pomocí senzorů a komunikace bude probíhat pomocí sítě LoRaWAN, k čemuž bude využito platformy CRA. Na aplikaci je kladeno několik požadavků:

- Vizualizace měřených hodnot.
- Uživatel by měl být schopen nastavit pro danou měřenou veličinu prahové hodnoty, o jejichž překročení by měl být aplikací informován.
- Uživatel by měl být schopný zobrazit pozici daného zařízení na mapě.

4.2 Řešení

Výsledný systém využívá koncových zařízení, která jsou registrována v platformě CRA. Registraci a odstranění zařízení může uživatel provést přímo ve webové aplikaci. Platforma CRA zodpovídá za přeposílání zpráv ze zařízení webové aplikaci. Pro perzistenci dat a zpracování alarmů je využito databáze PostgreSQL.

5 IMPLEMENTACE ŘEŠENÍ

5.1 Hardwarové komponenty

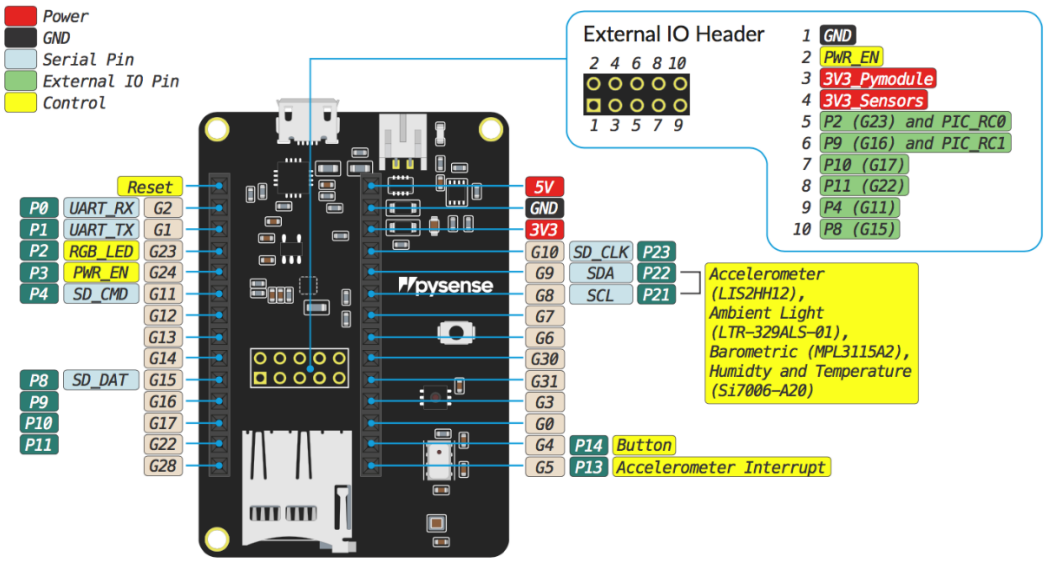
5.1.1 LoPy

Kompaktní vývojová deska od společnosti Pycom, určená pro využití v oblasti IoT. Využívá mikrokontroleru ESP32 a podporuje různé bezdrátové komunikační protokoly jako jsou Wi-Fi, Bluetooth a LoRa. [51], [52]

Obrázek 10: Vývojová deska LoPy. [52]

5.1.2 Pysense

Vývojový modul od společnosti Pycom, slouží jako expanzní deska pro zařízení LoPy. Obsahuje několik zabudovaných senzorů, pomocí kterých je možné monitorovat okolní prostředí. [53]



Obrázek 11: Pysense pinout. [53]

5.1.3 Programování hardwarových komponent

K programování koncových zařízení bylo využito programu Visual Studio Code a rozšíření Pymakr, pomocí kterého byl kód na zařízení nahrán. Program běžící na zařízení byl implementován v jazyce MicroPython. Na zařízení byly také nahrány externí knihovny https://github.com/pycom/pycom-libraries/releases/, které umožnily komunikaci se senzory. Do sítě LoRaWAN jsou zařízení připojována pomocí metody OTAA. Import knihoven a připojení do sítě LoRaWAN je možné vidět v následující ukázce (reálné hodnoty app_eui a app_key byly v ukázce nahrazeny).

```
from network import LoRa
import socket
import binascii
from pycoproc_1 import Pycoproc
import machine
from LIS2HH12 import LIS2HH12
from SI7006A20 import SI7006A20
from LTR329ALS01 import LTR329ALS01
from MPL3115A2 import MPL3115A2,ALTITUDE,PRESSURE

lora = LoRa(mode=LoRa.LORAWAN)
app_eui = binascii.unhexlify('DEADBEEFDEADBEEF')
app_key = binascii.unhexlify('DEADBEEFDEADBEEFDEADBEEFDEADBEEF')
lora.join(activation=LoRa.OTAA, auth=(app_eui, app_key), timeout=0)
while not lora.has_joined():
    time.sleep(2.5)
    print('Joining lora network...')
s = socket.socket(socket.AF_LORA, socket.SOCK_RAW)
s.setsockopt(socket.SOL_LORA, socket.SO_DR, 5)
s.setblocking(True)
s.send(payload)
```

5.2 Využité technologie

Pro inicializaci webové aplikace bylo využito šablony Create T3 App, která během inicializace umožňuje zakomponovat do frameworku Next.js několik užitečných knihoven, které umožňují rychlý a pohodlný vývoj. Pro vývoj webové aplikace byl využit jazyk TypeScript a řada doplňujících open-source balíčků instalovaných pomoci NPM. Pro zobrazení ikon je v aplikaci využito balíčku Heroicons.

5.2.1 Next.js

Populární framework, umožňující tvorbu webových aplikací a statických stránek. Využívá knihovnu React. Hlavním cílem je urychlení a zjednodušení procesu vývoje. Poskytuje mnoho užitečných vlastností, mezi které patří například automatické načítání dat nebo řešení pro navigaci (routing). [54]

5.2.2 React

Jde o populární open-source knihovnu pro tvorbu interaktivních uživatelských rozhraní, je navržena pro usnadnění vývoje interaktivních a responzivních webových aplikací. Jedním z hlavních principů technologie je její architektura, která je založena na hierarchicky strukturovaných komponentech. Komponent představuje znovupoužitelnou část uživatelského rozhraní, která má vlastní stav a vlastnosti, díky čemuž je možné tvořit modulární a dynamická uživatelská rozhraní. [55]

5.2.3 Prisma

Prisma je open-source nástroj ORM (Object Relational Mapping), který je možné využívat v aplikacích Node.js. Pomocí definice databázového schématu umožňuje vygenerovat typově bezpečného databázového klienta, kterého je možné využívat v aplikaci. Umožňuje tak interakcí s databází přímo v programovacím jazyce aplikace. [56]

5.2.4 tRPC

Typově bezpečná end-to-end knihovna pro vytváření API pomocí TypeScriptu. Eliminuje nutnost tvorby tradičních REST API. Umožňuje definici metod na serveru a zpřístupňuje je pro využití na klientovi. [57]

5.2.5 NextAuth.js

Jde o flexibilní open-source knihovnu, poskytující řešení pro autentizaci v aplikacích využívajících frameworku Next.js. Knihovna zahrnuje vestavěnou podporu pro šifrované JWT (Json Web Tokens). [58]

5.2.6 TailwindCSS

CSS framework, který umožňuje psát tzv. utility-first CSS. Poskytuje předdefinované třídy, pomocí kterých je možné stylování aplikovat přímo na konkrétní elementy HTML. Během kompilace framework kontroluje využití tříd a zahrnuje pouze potřebné. [59]

5.2.7 Supabase Realtime Client

Jde o knihovnu, umožňující tvorbu reaktivních aplikací, které naslouchají změnám v databázi v reálném čase. Umožňuje odebírat změnám v databázi, na které je poté možné reagovat v koncové aplikaci. [60]

5.2.8 Zod

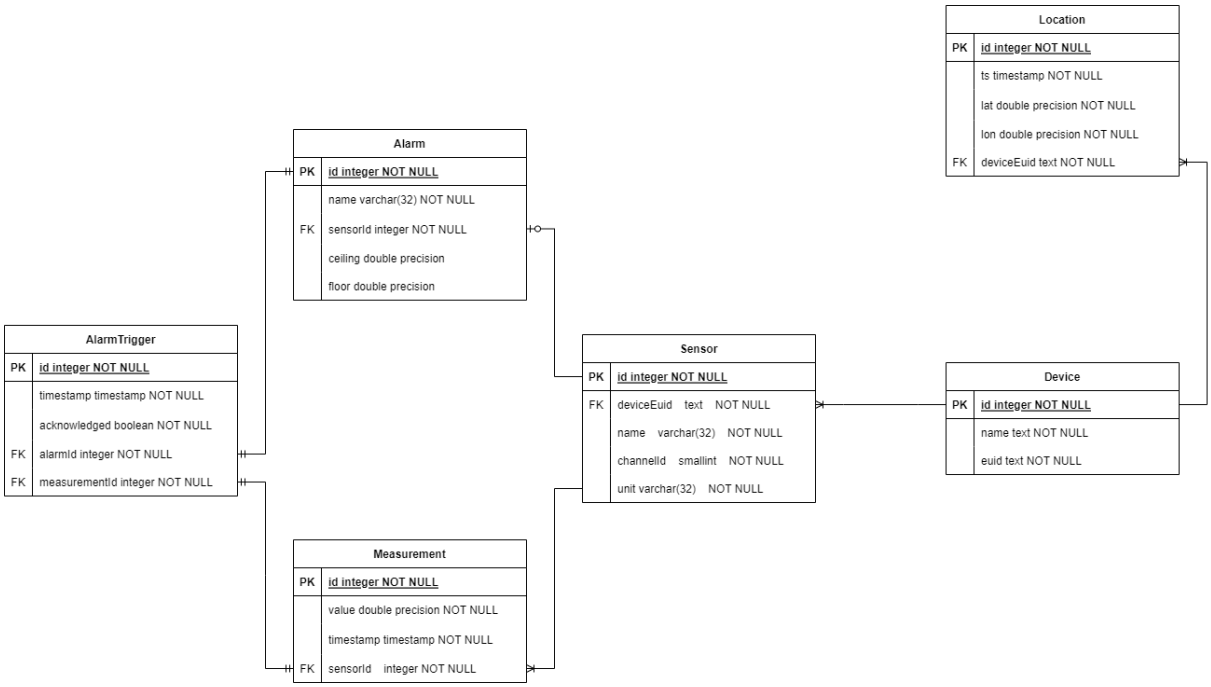
Zod je knihovna pro validaci a parsování dat. Klíčovou vlastností knihovny je skutečnost, že umožňuje definovat schéma, které zároveň slouží jako validátor i jako typová definice. Není tak třeba udržovat synchronizaci mezi validačním systémem a systémem pro typovou kontrolu. Knihovna je plně kompatibilní s jazykem TypeScript. [61]

5.2.9 Headless UI

Headless UI je knihovna poskytující nestylované komponenty pro frameworky Vue a React. Základní myšlenkou této knihovny je poskytnutí „bezhlavých“ (headless) komponent, které lze využít v rámci tvorby uživatelského rozhraní. Komponenty jsou dodávané s funkcionalitou, ale bez jakéhokoliv předdefinovaného stylování. Knihovnu vytvořil tým Tailwind Labs, který také stojí za populárním frameworkem Tailwind CSS. [62]

5.3 Databázové schéma

Databáze PostgreSQL obsahuje 6 tabulek. Tabulka *Device* uchovává pouze základní informace o zařízení, tj. jeho devEUI a jméno. Tabulka *Sensor* reprezentuje konkrétní měřené veličiny na zařízení, pole *channelId* slouží k dekódování konkrétní měřené hodnoty z datového obsahu zpráv ze zařízení. Každý senzor může mít nastavený *Alarm,* který slouží k monitorování měřených hodnot, ty jsou ukládány do tabulky *Measurement*. Databáze obsahuje trigger, který při vkládání měření kontroluje, nedošlo-li k překročení prahových hodnot sledovaných alarmem. Pokud dojde k překročení hodnoty, do tabulky *AlarmTrigger* je vložen nový řádek. Aplikace uživatele informuje, existují-li v tabulce *AlarmTrigger* nepotvrzené alarmy. Model je možné vidět na obrázku 12.



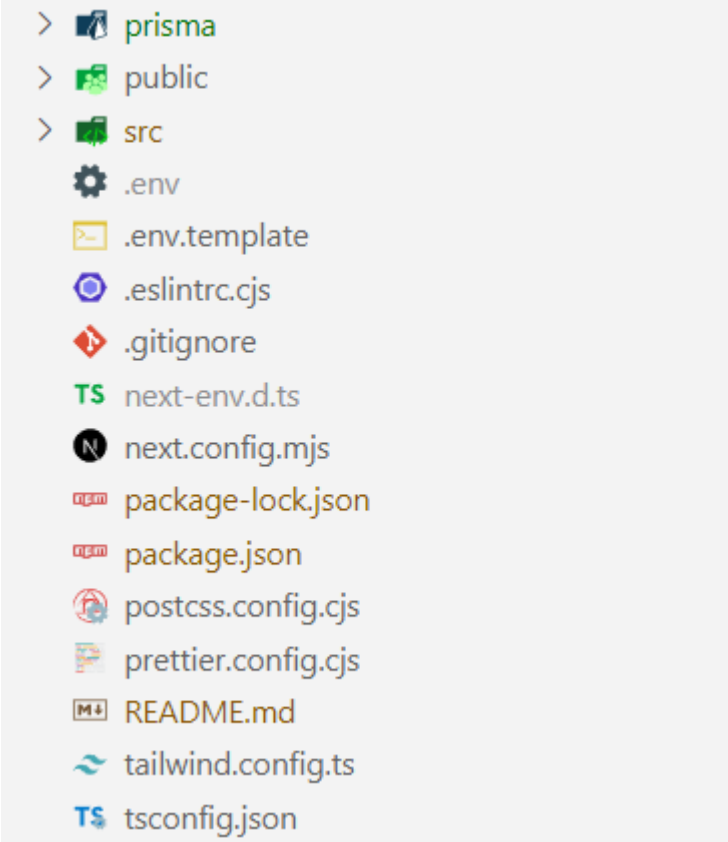
Obrázek 12: Databázový model.

5.4 Struktura aplikace

Kořenový adresář obsahuje konfigurační soubory vzniklé během inicializace aplikace. Dále obsahuje soubory .env a .env.mjs které slouží k nastavení a validaci proměnných prostředí. Adresář prisma obsahuje soubor schema.prisma ve kterém je definováno schéma databáze a způsob připojení k databázi. Pomocí tohoto souboru může knihovna Prisma generovat typově bezpečného klienta, za jehož využití je možné interagovat s databází přímo v aplikaci. Posledním důležitým adresářem je adresář src, který obsahuje zdrojové kódy. Adresář src je dělen na několik podadresářů:

- components – Obsahuje komponenty využité v aplikaci.
- hooks – Obsahuje vlastní React Hook pro správu modálního dialogu.
- layouts – Obsahuje definici hlavního rozložení uživatelského rozhraní aplikace, jednotlivé stránky je poté možné „zasadit“ do zmiňovaného rozložení.
- pages – Framework Next.js implementuje definici cest na úrovni souborového systému. Každý soubor exportující funkci je automaticky dostupný jako cesta. Framework podporuje i vnořené cesty, dynamické směrování a také cesty API. Soubory umístěné do adresáře pages/api jsou tak frameworkem chápány jakožto endpoint.

- server – Obsahuje kód obstarávající autentizaci pomocí knihovny NextAuth.js. Obsahuje také kód sloužící pro interakci s databází, za tímto účelem je využito knihovny tRPC a nástroje Prisma.
- styles – Složka obsahuje CSS soubory pro definici stylů.
- utils – Obsahuje užitečné funkce využívané v aplikaci na vícero místech. Obsahuje také soubor schemas.ts, ve kterém jsou definována schémata datových objektů. Schémata jsou tvořena pomocí validační knihovny Zod. Další důležitou částí je soubor supabase.ts, ten definuje způsob připojení k databázi za účelem monitorování aktivních alarmů.



Obrázek 13: Adresářová struktura projektu.

5.5 Autentizace

Autentizaci obstarává knihovna NextAuth.js, využívá se princip delegované autentizace, kdy se přihlašovací údaje předávají SSO (Single Sign-On) platformě od CRA. V případě, že SSO platforma potvrdí požadavek na přihlášení a je získán validní přístupový token, je autentizace považována za úspěšnou. Jelikož přístup k platformě CRA je zprostředkován pomocí testovacího univerzitního účtu, server ještě před odesláním požadavku na platformu kontroluje,

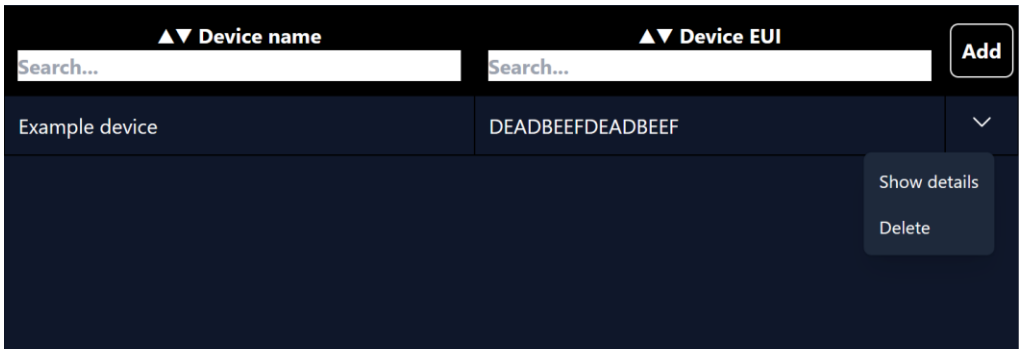
zdali přihlašovací údaje odpovídají tomuto zmiňovanému účtu. Aplikace je veřejně dostupná a tento krok brání situaci, kdy je možné se přihlásit pomocí libovolného platného účtu platformy. Přístupový token je v aplikaci využit výhradně pro přidávání a odebírání konkrétních zařízení, což se musí promítnout do konkrétního projektu definovaném na platformě CRA.

Přístupový token je uchováván v šifrovaném JWT, přičemž vše spravuje zmiňovaná knihovna NextAuth.js. Projekt obsahuje soubor *middleware.tsx*, ve kterém je kontrolována platnost tokenu při každém přechodu na stránku se zařízeními. Jelikož token má životnost 7200 sekund, tak je možné udržet aktivní sezení do doby vypršení tokenu. Díky middleware je možné uživatele požádat o opětovné přihlášení v případech expirace tokenu. Tento mechanismus je vidět v následující ukázce.

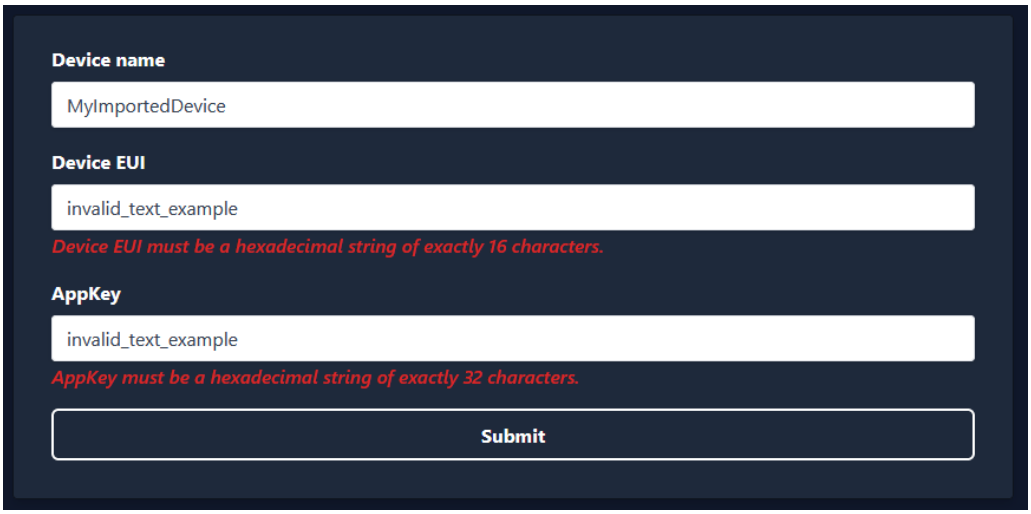
```
import { withAuth } from "next-auth/middleware";
/**
 * Middleware to check if our CRA access_token has expired.
 */
export default withAuth({
  callbacks: {
    authorized: ({token}) => !token?.isExpired ?? false
  }
})
export const config = { matcher: [ "/devices/:path*"] }
```

5.6 Správa zařízení

Všechna zařízení, která jsou v systému přítomna, jsou zobrazena v tabulce na stránce *devices*. Pomocí tlačítka může uživatel přejít na formulář, kde je mu umožněno přidat nové zařízení. Každá položka zařízení nabízí také menu, pomocí kterého může uživatel zařízení odstranit nebo přejít na stránku, kde je vizualizována geografická lokace zařízení. Formulář je vytvořen pomocí knihovny react-hook-form a využívá také její integrace s validační knihovnou Zod. Přidání a odstranění zařízení je řešeno pomocí HTTP dotazů na endpoint *api/device/[euid]*, kde je navíc řešena přítomnost zařízení ve směrovací skupině definované v projektu na platformě CRA. Zařízení musí být v rámci platformy CRA také přiřazeno do příslušné směrovací skupiny, aby došlo k přesměrování zpráv do webové aplikace.



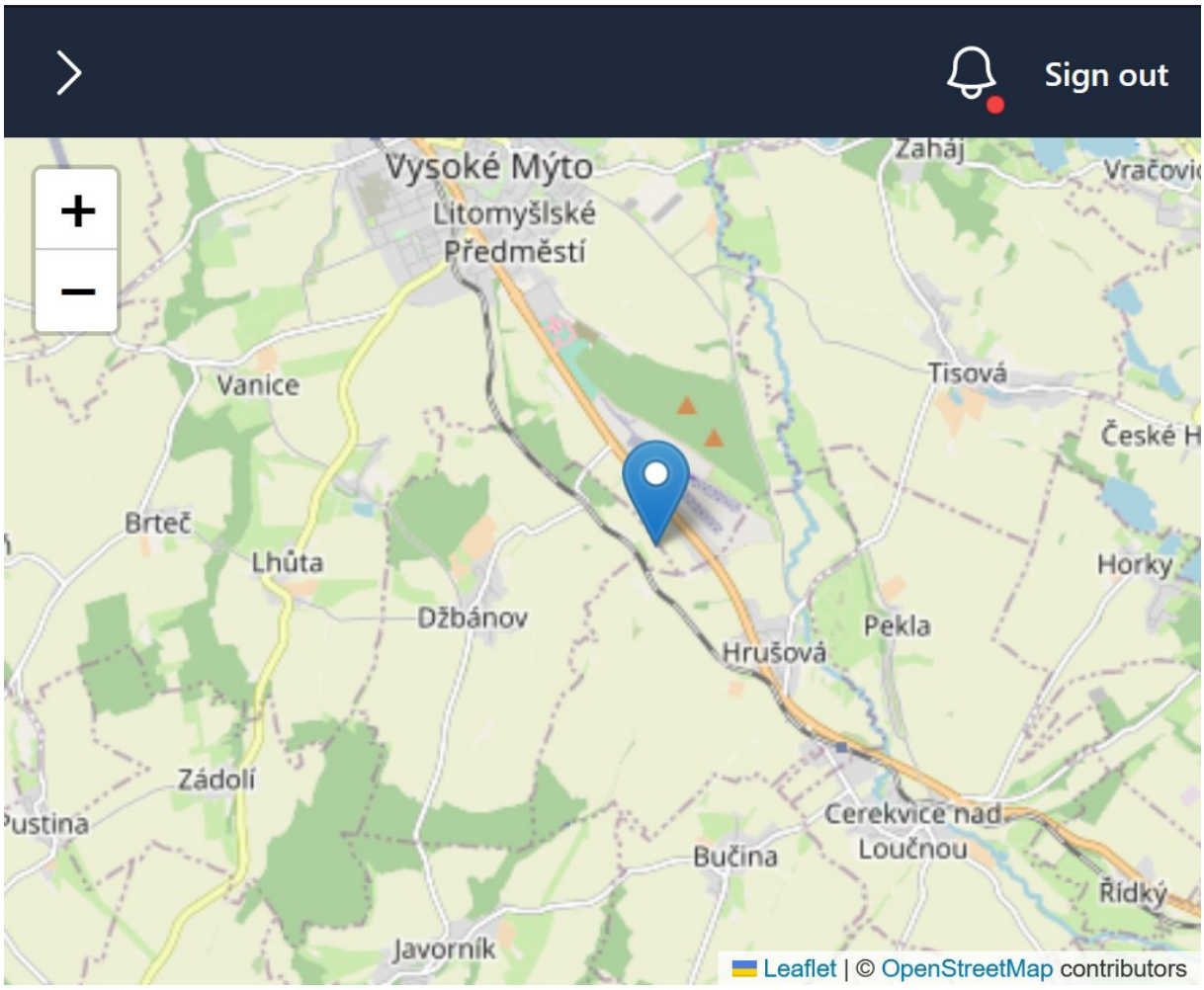
Obrázek 14: Náhled zařízení.



Obrázek 15: Formulář pro přidání zařízení.

5.6.1 Vizualizace lokace zařízení

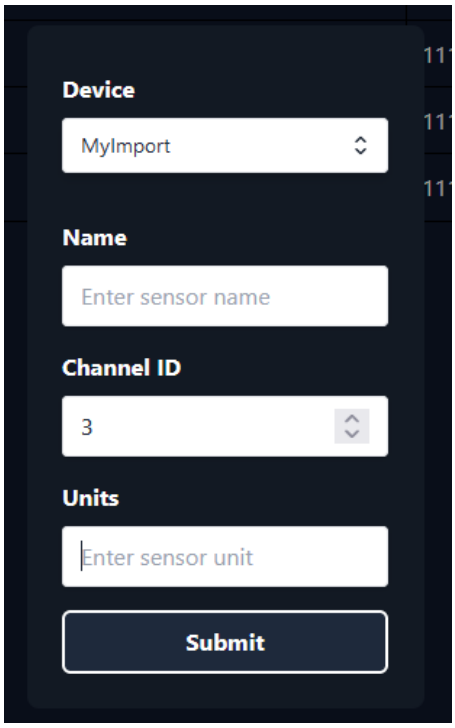
Lokace zařízení je vyobrazena pomocí mapy, která byla implementována za využití knihovny react-leaflet. Samotná data pro lokalizaci zařízení jsou získávána pomocí zpracování příchozí zprávy ze zařízení. Pokud obsahuje zpráva informaci o alespoň tří branách, může být lokace zařízení aproximována pomocí hodnot RSSI (received signal strength indication), SNR (signal to noise ratio) a geografických souřadnic brány.



Obrázek 16: Zobrazení geografické lokace zařízení.

5.7 Správa senzorů

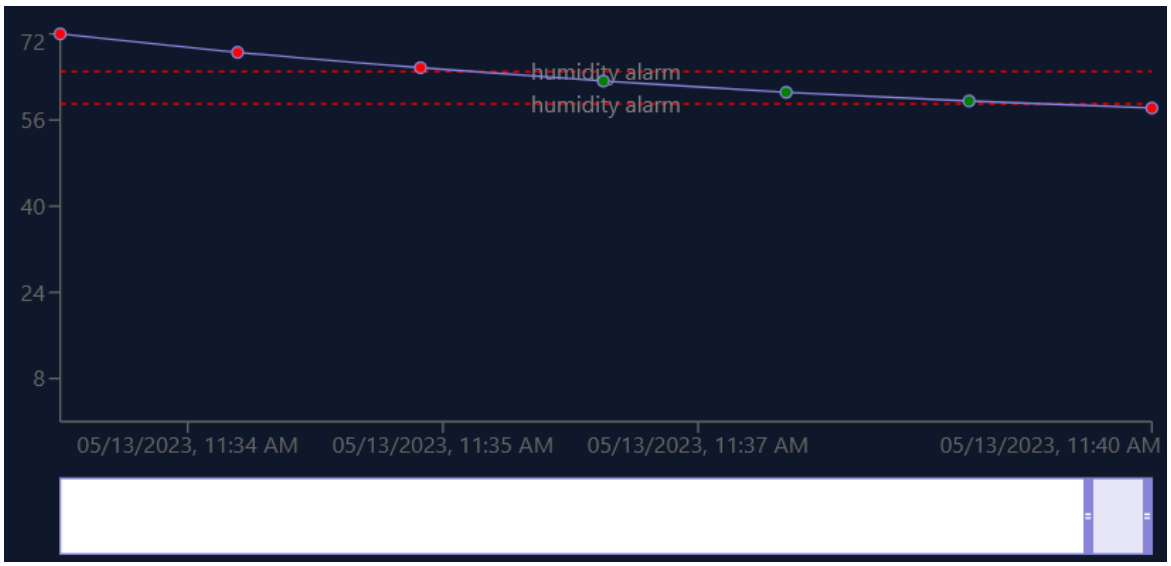
Senzory může uživatel spravovat podobně jako zařízení, při kliknutí na tlačítko je uživateli zobrazen formulář pro přidání zařízení. Zde může uživatel zvolit přiřazené zařízení, jméno senzoru a parametr channel ID, který slouží k asociaci měřených hodnot se specifickým senzorem. Volitelně může uživatel také senzoru přidělit jednotku. Formulář je možné vidět na obrázku 17.



Obrázek 17: Formulář pro přidání senzoru.

5.7.1 Vizualizace měřených hodnot

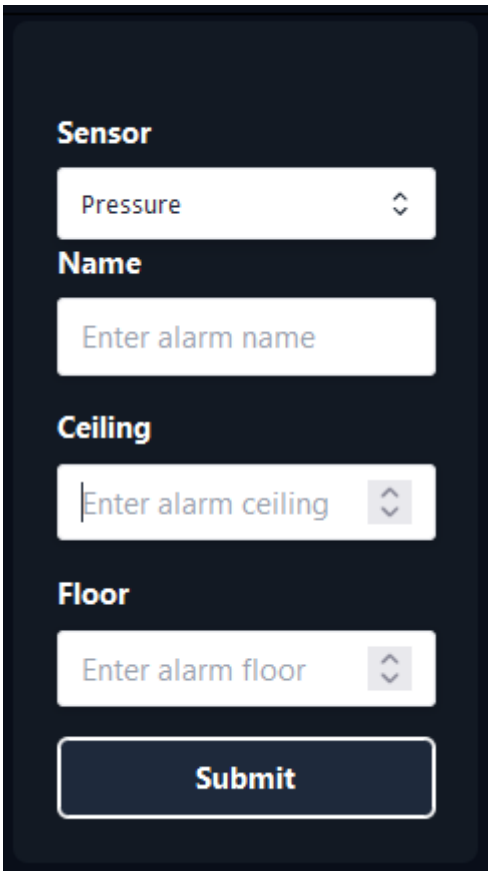
Měřené hodnoty jsou zobrazeny pomocí grafu. K implementaci grafu je využito knihovny Recharts. Výsledný graf je možné vidět na obrázku 18. Graf obsahuje posuvník, pomocí kterého je možné zobrazovat hodnoty ze specifického časového rozmezí. V případě, že má konkrétní senzor definovaný alarm, jsou také vizualizovány prahové hodnoty alarmu.



Obrázek 18: Vizualizace měřených hodnot.

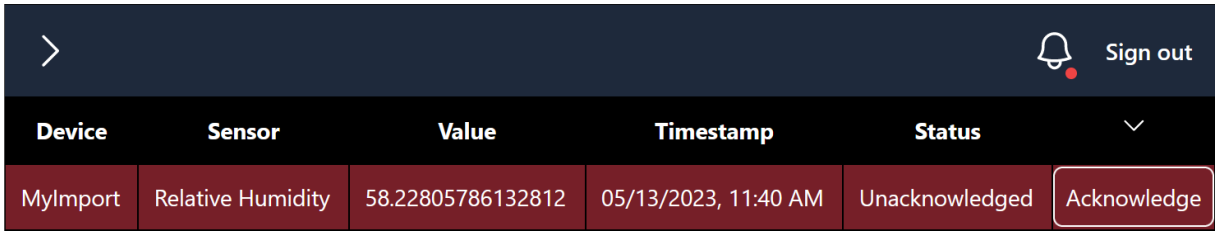
5.8 Správa alarmů

Uživatel může pro každý senzor nastavit alarm, který obsahuje dvě prahové hodnoty floor a ceiling. Překročení hodnoty ceiling vede k aktivaci alarmu. Hodnota floor vystihuje minimální přípustnou hodnotu, je-li měřená hodnota menší, dojde také k aktivaci alarmu.



Obrázek 19: Formulář pro nastavení alarmu.

Je-li v systému přítomna nepotvrzená aktivace alarmu, uživatel je informován pomocí notifikační ikony v horní liště aplikace. Stránka *alarms/triggers* dále umožňuje zobrazovat historii aktivací alarmů. Uživatel může na této stránce také potvrdit aktivní nepotvrzený alarm nebo zneplatnit potvrzení již potvrzeného alarmu.



Obrázek 20: Zobrazení historie aktivací alarmů a notifikace na horní liště.

5.9 Zpracování zpráv ze zařízení

Zprávy ze zařízení jsou přeposílány na endpoint *api/sensor-data* ve formátu JSON. Každý dotaz musí být doprovázen validním autorizačním klíčem. Autorizační klíč je pro daný endpoint nastaven v projektu platformy CRA. Formát zprávy je možné vidět v následující ukázce, v ukázce jsou zahrnuté pouze klíče, které jsou využité v rámci zpracování dat.

```
{
   "ts":1683970484395,
   "gws":[
      {
         "rssi":-109,
         "snr":4.2,
         "ts":1683970484395,
         "gweui":"B827EBFFFF07FBB1",
         "lat":49.950963,
         "lon":16.155044
      }
   ],
   "data":"010047c1048002004351400003004 1cf45c40400428921bc",
   "EUI":"70B3D5499ED89AA2"
}
```

Pole ts je využito pro tvorbu časového razítka daného měření nebo aktivace alarmu. Pole gws obsahuje informaci o branách a je využito pro odhad lokace zařízení v případě, že pole bran obsahuje informaci alespoň o tří branách. Pole data obsahuje konkrétní datový obsah zasílaný ze zařízení. Pole EUI slouží k identifikaci konkrétního koncového zařízení.

5.9.1 Formát datového obsahu

Formát datového obsahu nabývá struktury, kterou je možno vidět na obrázku 21. Datový obsah představuje měření získaná ze senzorů. Každé měření pro konkrétní senzor obsahuje tři pole: id kanálu, přesnost, hodnota. Channel ID slouží k rozpoznání senzoru na daném zařízení, díky čemuž je možné asociovat konkrétní měřené hodnoty s konkrétním senzorem. Pole precision (přesnost) slouží k indikaci datového rozsahu přenášené hodnoty. Nabývá-li pole precision hodnoty 0, pak je hodnota měření reprezentována čtyřmi bajty. Pokud je hodnota pole precision větší než nula, hodnota měření nabývá velikosti osmi bajtů. Pole je zachováno spíše v zájmu rozšiřitelnosti aplikace (např. formou podpory pro konkrétní datové typy), jelikož výsledná aplikace pracuje s datovým typem Number a databáze hodnoty uchovává pod datovým typem double precision.

1 byte	1 byte	n bytes	1 byte	1 byte	n bytes	1 byte	1 byte	n bytes
Channel ID	Precision	Value	Channel ID	Precision	Value	Channel ID	Precision	Value

Obrázek 21: Struktura datového obsahu.

5.10 Nasazení

5.10.1 Verzování

K verzování je využito technologie Git. Na platformě GitHub byl vytvořen soukromý repozitář, který uchovává zdrojové kódy webové aplikace. Během vývoje je tak možné mít kompletní přehled o změnách v aplikaci a zdrojové kódy jsou tímto způsobem zálohovány.

5.10.2 Databáze

K nasazení databáze je využito platformy Supabase, připojení k databázi je zprostředkováno pomocí nástroje Prisma. Konfigurace připojení k databázi je obsažená v souboru *schema.prisma* a má následující podobu:

```
datasource db {
  provider  = "postgresql"
  url       = env("DATABASE_URL")
  directUrl = env("DIRECT_URL")
}

generator client {
  provider = "prisma-client-js"
}
```

V souboru jsou také obsaženy databázové modely. Pole *url* a *directUrl* slouží pro připojení k databázi, přičemž hodnota URL je uchována v proměnné prostředí.

5.10.3 Webová aplikace

Nasazení webové aplikace probíhá pomocí platformy Vercel, přičemž samotný proces nasazení je velmi jednoduchý. Platforma umožňuje propojení s repozitářem Git. Po napojení repozitáře je aplikace automaticky kompilována a nasazena. Následně je aplikace zpřístupněna na vygenerované adrese URL. Při změnách na produkční větvi propojeného repozitáře dochází automaticky k opětovné kompilaci a k nasazení nové verze aplikace.

ZÁVĚR

Cílem bakalářské práce bylo navrhnout a vytvořit aplikaci, pomocí které je možné monitorovat vnitřní stav objektu. Aplikace umožňuje vizualizaci měřených dat, zobrazení geografické lokace zařízení na mapě a nastavování prahových hodnot – limitů. Aplikace také uživateli umožňuje spravovat přidaná zařízení, senzory i nastavené alarmy. Pro přenos zpráv od zařízení je úspěšně využito platformy CRA, která přeposílá zprávy na definovaný endpoint webové aplikace. Všechny uvedené cíle práce byly úspěšně splněny.

Každé zařízení může prostřednictvím platformy CRA v rámci jednoho dne zaslat maximálně 360 zpráv, chceme-li snímat v průběhu dne rovnoměrně, pak tento limit odpovídá jedné zprávě každých pět minut. S tímto omezením nejde monitorovat klima vnitřních prostor v reálném čase po dobu celého dne, jelikož by velmi brzo došlo k naplnění denního limitu.

Aplikaci by jistě bylo možné dále rozvíjet několika směry. Bylo by například možné rozšířit podporu měřených dat o více datových typů nebo například provést sofistikovanější integraci s platformou CRA, která by uživateli umožňovala přímou správu projektů na platformě.

POUŽITÁ LITERATURA

[1] POHANKA, Pavel. Internet věcí. *Data Distribution Service* [online]. Česká republika, Brno: Pavel Pohanka, 06. 10. 2020 [cit. 2023-05-05]. Dostupné z: https://pavelpohanka.cz/internet-of-things/.

[2] KOĎOUSKOVÁ, Barbora. Internet věcí (IoT): definice, příklady využití, produkty. *Rascasone* [online]. Česká republika, Praha: Rascasone, 03. 05. 2023 [cit. 2023-05-05]. Dostupné z: https://www.rascasone.com/cs/blog/iot-internet-veci-definice-produkty-historie.

[3] KHVOYNITSKAYA, Sandra. The IoT history and future. *Itransition: Software Development Company* [online]. USA, Lakewood: Itransition, 25. 11. 2019 [cit. 2023-05-07]. Dostupné z: https://www.itransition.com/blog/iot-history.

[4] History of the Internet of Things. *Eleven Fifty Academy: Nonprofit Coding and Cybersecurity Bootcamp* [online]. USA, Indianapolis: Eleven Fifty Academy, 28. 12. 2020 [cit. 2023-05-07]. Dostupné z: https://www.elevenfifty.org/blog/the-history-of-the-internet-of-things.

[5] Top 10 Real-World IoT Applications & Uses in 2023. *Intellipaat: Online Professional Training Courses and Certification* [online]. India, Bengalore: Intellipaat, 14. 03. 2023 [cit. 2023-05-07]. Dostupné z: https://intellipaat.com/blog/iot-applications-and-uses.

[6] KARJAGI, Rajashekhar a Manish JINDAL. IoT in Healthcare Industry | IoT Applications in Healthcare. *Wipro* [online]. India, Bengaluru: Wipro, © 2023 [cit. 2023-05-07]. Dostupné z: https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/.

[7] CAMPBELL, Alex. Guide to IoT Smart Home. *HelpWire* [online]. USA, Alexandria: HelpWire, 16. 12. 2022 [cit. 2023-05-07]. Dostupné z: https://www.helpwire.app/blog/iot-smart-home/.

[8] SIMMONS, Adam. Smart City and Internet of Things (IoT) Technology. *Dgtl Infra: Digital Infrastructure* [online]. USA, New York: Dgtl Infra, 19. 1. 2023 [cit. 2023-05-07]. Dostupné z: https://dgtlinfra.com/smart-city-internet-of-things-iot/.

[9] LOMBARDI, Marco, Francesco PASCALE a Domenico SANTANIELLO. Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information* [online]. 2021, 12(2) [cit. 2023-05-06]. ISSN 2078-2489. Dostupné z: doi:10.3390/info12020087.

[10] SOBIN, C. C. A Survey on Architecture, Protocols and Challenges in IoT. *Wireless Personal Communications* [online]. 2020, 112(3), 1383-1429 [cit. 2023-05-07]. ISSN 0929-6212. Dostupné z: doi:10.1007/s11277-020-07108-5.

[11] KUMAR, Shivam. Wireless Sensor Network (WSN). *GeeksforGeeks: A Computer Science portal for geeks* [online]. India, Noida: GeeksforGeeks, 17. 3. 2023 [cit. 2023-05-07]. Dostupné z: https://www.geeksforgeeks.org/wireless-sensor-network-wsn/.

[12] WANT, R. An Introduction to RFID Technology. *IEEE Pervasive Computing* [online]. 2006, 5(1), 25-33 [cit. 2023-05-07]. ISSN 1536-1268. Dostupné z: doi:10.1109/MPRV.2006.2.

[13] H., Sabireen a Neelanarayanan V. A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges. *ICT Express* [online]. 2021, **7**(2), 162-176 [cit. 2023-05-07]. ISSN 24059595. Dostupné z: doi:10.1016/j.icte.2021.05.004.

[14] Fog Computing. *IoT portál: Brána do světa internetu věcí* [online]. Česká republika: IoT portál, 16. 6. 2017 [cit. 2023-05-07]. Dostupné z: https://www.iot-portal.cz/2017/06/16/fog-computing/.

[15] ASHTARI, Hossein. Edge Computing vs. Fog Computing: 10 Key Comparisons. *Spiceworks: Business and Industry News, Analysis and Expert Insights* [online]. USA, Texas: Spiceworks, 10. 2. 2022 [cit. 2023-05-07]. Dostupné z: https://www.spiceworks.com/tech/cloud/articles/edge-vs-fog-computing/.

[16] ROSE, Karen, Scott ELDRIDGE a Lyman CHAPIN. THE INTERNET OF THINGS: AN OVERVIEW. *Internet Society: Build, Promote, and Defend the Internet* [online]. Switzerland, Geneva: Internet Society, October 2015 [cit. 2023-05-07]. Dostupné z: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf.

[17] APRIL, Chris. The Four Internet of Things Connectivity Models Explained. *Channel Futures: Leading Channel Partners Forward* [online]. UK, London: Informa, 29. 4. 2016 [cit. 2023-05-07]. Dostupné z: https://www.channelfutures.com/best-practices/the-four-internet-of-things-connectivity-models-explained.

[18] BATERNA, Quina. What Is a Nest Thermostat and How Does It Work. *MUO: Technology, Simplified* [online]. Canada, Montreal: Valnet, 25. 8. 2022 [cit. 2023-05-07]. Dostupné z: https://www.makeuseof.com/how-does-nest-thermostat-work/.

[19] TSCHOFENIG, Hannes, Jari ARKKO, Dave THALER a Danny R. MCPHERSON. *RFC 7452: Architectural Considerations in Smart Object Networking* [online]. March 2015 [cit. 2023-05-07]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc7452.

[20] The History of WiFi: 1971 to Today. *CableFree: 4G & 5G 10 Gigabit Wireless Technology* [online]. UK, Oxford: Wireless Excellence, 18. 5. 2017 [cit. 2023-05-07]. Dostupné z: https://www.cablefree.net/wireless-technology/history-of-wifi-technology/.

[21] BISDIKIAN, C. An overview of the Bluetooth wireless technology. *IEEE Communications Magazine* [online]. 2001, 39(12), 86-94 [cit. 2023-05-07]. ISSN 0163-6804. Dostupné z: doi:10.1109/35.968817.

[22] ZEADALLY, Sherali, Farhan SIDDIQUI a Zubair BAIG. 25 Years of Bluetooth Technology. *Future Internet* [online]. 2019, 11(9) [cit. 2023-05-07]. ISSN 1999-5903. Dostupné z: doi:10.3390/fi11090194.

[23] MARCEL, Jason. How Bluetooth Technology Uses Adaptive Frequency Hopping to Overcome Packet Interference. *Bluetooth® Technology Website* [online]. USA, Washington: Bluetooth SIG, 15. 11. 2020 [cit. 2023-05-07]. Dostupné z: https://www.bluetooth.com/blog/how-bluetooth-technology-uses-adaptive-frequency-hopping-to-overcome-packet-interference/.

[24] SHEA, Sharon. What is Z-Wave: Definition from TechTarget. *TechTarget* [online]. USA, Newton: TechTarget, 29. 8. 2018 [cit. 2023-05-07]. Dostupné z: https://www.techtarget.com/iotagenda/definition/Z-Wave.

[25] Discover Zigbee Protocol 3.0: Digi International. *Digi International: IIoT Devices and Services for M2M Networking* [online]. USA, Hopkins: Digi International, © 2023 [cit. 2023-05-07]. Dostupné z: https://www.digi.com/solutions/by-technology/zigbee-wireless-standard.

[26] Zigbee: Complete IOT Solution. *CSA-IOT: Connectivity Standards Alliance* [online]. USA, Davis: Connectivity Standards Alliance, © 2022 [cit. 2023-05-07]. Dostupné z: https://csa-iot.org/all-solutions/zigbee/.

[27] Our Members. *CSA-IOT: Connectivity Standards Alliance* [online]. USA, Davis: Connectivity Standards Alliance, © 2022 [cit. 2023-05-07]. Dostupné z: https://csa-iot.org/members/.

[28] RAMYA, C. Muthu, M SHANMUGARAJ a R PRABAKARAN. Study on ZigBee technology. In: *2011 3rd International Conference on Electronics Computer Technology* [online]. IEEE, 2011, 2011, s. 297-301 [cit. 2023-05-07]. ISBN 978-1-4244-8678-6. Dostupné z: doi:10.1109/ICECTECH.2011.5942102.

[29] Evolution of HTTP. *MDN Web Docs* [online]. Mountain View, California: Mozilla Foundation, 10. 4. 2023 [cit. 2023-05-07]. Dostupné z: https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Evolution_of_HTTP.

[30] An overview of HTTP. *MDN Web Docs* [online]. Mountain View, California: Mozilla Foundation, 10. 4. 2023 [cit. 2023-05-07]. Dostupné z: https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview.

[31] Introducing the MQTT Protocol - MQTT Essentials: Part 1. *HiveMQ: Enterprise ready MQTT to move your IoT data* [online]. Germany, Landshut: HiveMQ, 12. 1. 2015 [cit. 2023-05-07]. Dostupné z: https://www.hivemq.com/blog/mqtt-essentials-part-1-introducing-mqtt/.

[32] Publish & Subscribe - MQTT Essentials: Part 2. *HiveMQ: Enterprise ready MQTT to move your IoT data* [online]. Germany, Landshut: HiveMQ, 12. 01. 2015 [cit. 2023-05-07]. Dostupné z: https://www.hivemq.com/blog/mqtt-essentials-part2-publish-subscribe/.

[33] SHELBY, Zach, Klaus HARTKE a Carsten BORMANN. *RFC 7252: The Constrained Application Protocol (CoAP)* [online]. June 2014 [cit. 2023-05-07]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc7252.

[34] CoAP protocol: Nordic Developer Academy. *Nordic Developer Academy* [online]. Norway, Trondheim: Nordic Semiconductor, © 2022 [cit. 2023-05-07]. Dostupné z: https://academy.nordicsemi.com/topic/lesson-5-coap-protocol/.

[35] MEKKI, Kais, Eddy BAJIC, Frederic CHAXEL a Fernand MEYER. Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT. In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* [online]. IEEE, 2018, 2018, s. 197-202 [cit. 2023-05-07]. ISBN 978-1-5386-3227-7. Dostupné z: doi:10.1109/PERCOMW.2018.8480255.

[36] RAZA, Usman, Parag KULKARNI a Mahesh SOORIYABANDARA. *Low Power Wide Area Networks: An Overview* [online]. 2017, 19(2), 855-873 [cit. 2023-05-07]. ISSN 1553-877X. Dostupné z: doi:10.1109/COMST.2017.2652320.

[37] MEKKI, Kais, Eddy BAJIC, Frederic CHAXEL a Fernand MEYER. Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT. In: *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* [online]. IEEE, 2018, 2018, s. 197-202 [cit. 2023-05-07]. ISBN 978-1-5386-3227-7. Dostupné z: doi:10.1109/PERCOMW.2018.8480255.

[38] IDOWU-BISMARK, Bode. NB-IoT deployment scenarios. *ResearchGate: Find and share research* [online]. Germany, Berlin: ResearchGate, 01. 10. 2017 [cit. 2023-05-07]. Dostupné z: https://www.researchgate.net/figure/NB-IoT-deployment-scenarios_fig2_320182831.

[39] HALSTEAD, Jennifer. What Is Weightless. *IoT Asset Monitoring & Tracking Solution: Link Labs* [online]. USA, Annapolis: Link Labs, 23. 11. 2015 [cit. 2023-05-07]. Dostupné z: https://www.link-labs.com/blog/what-is-weightless.

[40] DAVIES, Alex. Neul's legacy: three Weightless specs and Huawei's '4.5G'. *Rethink Technology Research ltd* [online]. UK, Bristol: Rethink Technology Research, © 2023 [cit. 2023-05-07]. Dostupné z: https://rethinkresearch.biz/articles/neuls-legacy-three-weightless-specs-and-huaweis-4-5g/.

[41] About Weightless Alliance. *Weightless Alliance* [online]. UK, Bristol: Weightless Alliance [cit. 2023-05-07]. Dostupné z: https://www.weightless-alliance.org/about.

[42] Background: Weightless SIG. *Weightless Alliance* [online]. UK, Bristol: Weightless Alliance [cit. 2023-05-07]. Dostupné z: https://www.weightless-alliance.org/background.

[43] SANCHEZ-IBORRA, Ramon a Maria-Dolores CANO. State of the Art in LP-WAN Solutions for Industrial IoT Services. *Sensors* [online]. 2016, 16(5) [cit. 2023-05-07]. ISSN 1424-8220. Dostupné z: doi:10.3390/s16050708.

[44] Technology: Weightless SIG. *Weightless Alliance* [online]. UK, Bristol: Weightless Alliance [cit. 2023-05-07]. Dostupné z: https://www.weightless-alliance.org/technology.

[45] ALMUHAYA, Mukarram A. M., Waheb A. JABBAR, Noorazliza SULAIMAN a Suliman ABDULMALEK. A Survey on LoRaWAN Technology: Recent Trends, Opportunities, Simulation Tools and Future Directions. *Electronics* [online]. 2022, 11(1) [cit. 2023-05-07]. ISSN 2079-9292. Dostupné z: doi:10.3390/electronics11010164.

[46] LoRa and LoRaWAN: Technical overview. *Semtech LoRa: DEVELOPER PORTAL* [online]. USA, California: Semtech Corporation, © 2023 [cit. 2023-05-07]. Dostupné z: https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/.

[47] SLATS, Lauren. A Brief History of LoRa®: Three Inventors Share Their Personal Story at The Things Conference. *Semtech: Semtech Semiconductor, IoT Systems and Cloud Connectivity* [online]. USA, California: Semtech Corporation, 08. 01. 2020 [cit. 2023-05-07]. Dostupné z: https://blog.semtech.com/a-brief-history-of-lora-three-inventors-share-their-personal-story-at-the-things-conference.

[48] AUGUSTIN, Aloÿs, Jiazi YI, Thomas CLAUSEN a William TOWNSLEY. A Study of LoRa. *Sensors* [online]. 2016, 16(9) [cit. 2023-05-07]. ISSN 1424-8220. Dostupné z: doi:10.3390/s16091466.

[49] Different LoRaWAN classes. *ResearchGate: Find and share research* [online]. Germany, Berlin: ResearchGate, 30. 06. 2018 [cit. 2023-05-07]. Dostupné z: https://www.researchgate.net/figure/Different-LoRaWAN-classes_fig18_326134076.

[50] SELLER, Olivier. LoRaWAN Security. *Journal of ICT Standardization* [online]. Denmark: River Publishers, 2021, 9(1) [cit. 2023-05-07]. ISSN 2246-0853. Dostupné z: doi:10.13052/jicts2245-800X.915.

[51] Lopy Datasheet. *Pycom: Next Generation Internet of Things Platform* [online]. Netherlands, Eindhoven: Pycom [cit. 2023-05-07]. Dostupné z: https://pycom.io/wp-content/uploads/2018/08/lopy-specsheet.pdf.

[52] LoPy. *Pycom: go invent* [online]. Netherlands, Eindhoven: Pycom [cit. 2023-05-07]. Dostupné z: https://docs.pycom.io/datasheets/development/lopy/.

[53] Pysense. *Pycom: go invent* [online]. Netherlands, Eindhoven: Pycom [cit. 2023-05-07]. Dostupné z: https://docs.pycom.io/datasheets/expansionboards/pysense/.

[54] What is Next.js. *Next.js by Vercel* [online]. USA, California: Vercel, © 2023 [cit. 2023-05-07]. Dostupné z: https://nextjs.org/learn/foundations/about-nextjs/what-is-nextjs.

[55] HERBERT, David. What is React.js? (Uses, Examples, & More). *HubSpot Blog: Marketing, Sales, Agency, and Customer Success Content* [online]. US, Massachusetts: HubSpot, 27. 06. 2022 [cit. 2023-05-07]. Dostupné z: https://blog.hubspot.com/website/react-js.

[56] What is Prisma? *Prisma: Next-generation ORM for Node.js & TypeScript* [online]. Germany, Berlin: Prisma Data, © 2023 [cit. 2023-05-07]. Dostupné z: https://www.prisma.io/docs/concepts/overview/what-is-prisma.

[57] TYSON, Matthew. Intro to tRPC: Integrated, full-stack TypeScript. *InfoWorld: Technology insight for the enterprise* [online]. San Francisco: InfoWorld, 30. 03. 2023 [cit. 2023-05-07]. Dostupné z: https://www.infoworld.com/article/3690275/intro-to-trpc-integrated-full-stack-typescript.html.

[58] ASIUWHU, Ejiro. NextAuth.js for client-side authentication in Next.js. *LogRocket Blog: Resources to Help Product Teams Ship Amazing Digital Experiences* [online]. USA, Boston: LogRocket, 08. 03. 2022 [cit. 2023-05-07]. Dostupné z: https://blog.logrocket.com/nextauth-js-for-next-js-client-side-authentication/.

[59] DRAYCOTT-WHEATLEY, Chris. Utility-first CSS with Tailwind. *NearForm* [online]. Ireland, Tramore: NearForm, 06. 02. 2019 [cit. 2023-05-07]. Dostupné z: https://www.nearform.com/blog/utility-first-css-with-tailwind/.

[60] Realtime Quickstart: Supabase Docs. *Supabase* [online]. Supabase, 05. 05. 2023 [cit. 2023-05-07]. Dostupné z: https://supabase.com/docs/guides/realtime/quickstart.

[61] ANSHUL, Abhinav. Schema validation in TypeScript with Zod. *LogRocket Blog: Resources to Help Product Teams Ship Amazing Digital Experiences* [online]. USA,

Boston: LogRocket, 08. 03. 2022 [cit. 2023-05-07]. Dostupné z: https://blog.logrocket.com/schema-validation-typescript-zod/.

[62] SORDYL, Krzysztof. Headless UI Libraries: The Key to Flexible and Accessible User Interfaces. *DEV Community* [online]. 18. 12. 2022 [cit. 2023-05-07]. Dostupné z: https://dev.to/verthon/headless-ui-libraries-the-key-to-flexible-and-accessible-user-interfaces-546p.