

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií



Bakalářská práce

Internet věcí a jeho implementace v regionálním rozvoji

Karel Sylvar

© 2023 ČZU v Praze

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Karel Sylvar

Informatika

Název práce

Internet věcí a jeho implementace v regionálním rozvoji

Název anglicky

Internet of Things and its implementation in regional development.

Cíle práce

Hlavním cílem práce je analýza IoT technologií v dané lokalitě a návrh jejich využití pro podporu regionálního rozvoje.

Dílčí cíle bakalářské práce jsou:

- Vytvořit přehled literatury a analýzu v oblasti současných informačních technologií užívaných s cílem podpořit rozvoj regionů.
- Na základě vybraných charakteristik provést analýzu vhodných IoT řešení.
- Analyzovat konflikt v oblasti sběru dat z těchto zařízení ve vztahu k GDPR.
- Provedení pilotního ověření ve vybrané lokalitě.

Metodika

Teoretická část je založena na studiu a analýze odborných a vědeckých zdrojů z oblasti internetu věcí, především z oblasti jejich instalace a využití pro podporu regionálního rozvoje, sběru dat a jejich následné anonymizaci ve vztahu k GDPR. Na základě syntézy poznatků teoretické části a vyhodnocení výsledků praktické části budou formulovány závěry práce.

Doporučený rozsah práce

40 – 50 stran

Klíčová slova

internet věcí, sběr dat, anonymizace, GDPR, odesílání dat , monitoring, IoT

Doporučené zdroje informací

Citační database Web of Science a Scopus

CHMELÁŘOVÁ, Magdalena, Helena KOLIBOVÁ a Věra JUŘÍČKOVÁ. Internet věcí a chytrá města v regionální perspektivě. Opava: Slezská univerzita v Opavě, Fakulta veřejných politik v Opavě, 2019. ISBN 978-80-7510-358-1.

RAJ, Pethuru a Anupama C. RAMAN. The Internet of things: enabling technologies, platforms, and use cases. Boca Raton: CRC Press/Taylor & Francis Group, [2017]. ISBN 978-1498761284.

WU, Chuan-Kun. Internet of things security: architectures and security measures. Singapore: Springer, [2021]. Advances in computer science and technology. ISBN 978-981-16-1371-5.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

doc. Ing. Jan Jarolímek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 14. 11. 2022

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci s názvem „Internet věcí a jeho implementace v regionálním rozvoji“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Rosovicích dne 1.3.2023

Poděkování

Rád bych touto cestou poděkoval vedoucímu mé bakalářské práce doc. Ing. Janu Jarolímkovi, Ph.D. za odborné vedení při psaní této práce. Dále bych rád poděkoval konzultantce mé bakalářské práce Ing. Tereze Burešové za prvotní konzultace při formulování zadání a celkovou ochotu a podnětné připomínky při psaní této práce.

Internet věcí a jeho implementace v regionálním rozvoji

Abstrakt

Cílem této práce je vytvořit aktuální teoretická východiska týkající se internetu věcí s ohledem na nejnovější technologické trendy a technologie, které IoT přináší. Je vytvořen přehled technologického prostředí IoT s ohledem na klíčové vlastnosti IoT systémů, a tedy na konektivitu, zdroje elektrického napájení, problematiku instalace zařízení a vztah sběru dat s ohledem na GDPR. Jsou uvedeny příklady IoT řešení v regionálních institucích, kde IoT pomáhá zlepšit efektivitu a podmínky fungování institucí. V praktické části bakalářské práce jsou analyzovány dostupné sítě pro konektivitu IoT systémů, jsou hodnoceny silné a slabé stránky těchto sítí, včetně příležitostí a ohrožení. Následně je provedeno pilotní ověření již funkčního IoT systému v lokalitě Lázeňských lesů Karlovy Vary, kde cílem tohoto IoT systému je získat alternativní způsob počítání počtu návštěvníků. V rámci pilotního ověření je brán ohled na použitý Hardware a je analyzována zvolená technologie přenosu dat. Jsou analyzovány výsledky sběru dat s jejich vztahu k GDPR a jsou porovnávány technologie sběru dat s ohledem na již zpracovaná data. Je také analyzován stav baterie a pokles jejího napětí u IoT zařízení ve vztahu k dlouhodobému fungování zařízení. Jsou formulovány závěry práce a doporučení k pilotnímu ověření. V závěru jsou hodnoceny výsledky této práce.

Klíčová slova: Internet věcí, sběr dat, anonymizace, GDPR, odesílání dat, monitoring, IoT

Internet of Things and its implementation in regional development

Abstract

The objective of Bachelor thesis is to develop a current theoretical background on the Internet of Things with respect to the latest technological trends and technologies that IoT brings. An overview of the IoT technology environment is provided concerning the key features of IoT systems, specifically connectivity, power supply, device installation issues, and the relationship of data collection with respect to GDPR. The examples are presented in IoT solutions in regional institutions where IoT helps to improve the efficiency and conditions of the institutions. The practical part of the bachelor thesis reviewed available networks for IoT systems connectivity, strengths, and weaknesses of these networks are evaluated, including opportunities and threats. A pilot verification is done on already functional IoT system located at Karlovy vary Lázeňské lesy location, where this IoT system aims to provide an alternative way of counting the number of visitors. During the pilot verification, the applied hardware is taken into attention and the chosen data transmission technology is also analysed. The results of the data collection are analysed with respect to the GDPR, and the data collection technologies are analysed in relation to the already collected data. The battery status and voltage drop of IoT devices are also analysed in relation to the long-term operation of the device. Evaluations and recommendations for pilot verification are formulated. The results of this thesis are evaluated in the conclusion.

Keywords: Internet of Things, data collection, anonymization, GDPR, data sending, monitoring, IoT

Obsah

1. Úvod.....	12
2. Cíl práce a metodika	13
3. Teoretická východiska	14
3.1 Internet věcí.....	14
3.1.1 Koncepce Smart.....	14
3.1.2 Konektivita.....	14
3.1.2.1 LPWAN.....	15
3.1.2.2 Mobilní sítě.....	18
3.1.2.3 WPAN sítě.....	18
3.1.2.4 LAN.....	19
3.1.2.5 Porovnání.....	21
3.1.3 Napájení	21
3.1.3.1 Energy harvesting.....	22
3.1.3.2 Zdroje pro získávání energie	23
3.2 Příklady integrace IoT	25
3.2.1 Chytré letiště.....	25
3.2.1.1 Airport 1.0	25
3.2.1.2 Airport 2.0	25
3.2.1.3 Airport 3.0	26
3.2.2 IoT ve zdravotnictví.....	27
3.2.2.1 Klinická péče	27
3.2.2.2 Monitorování na dálku	28
3.2.3 Další IoT prvky v regionech	28
3.2.3.1 IoT Elektroměr / vodoměr	29
3.2.3.2 Chytré parkoviště.....	29
3.2.3.3 Využití IoT v rámci služeb obchodů	29
3.2.3.4 IoT v komunálních službách	30
3.2.3.5 Použití senzorů v zemědělství	30
3.2.4 Problémy při instalaci IoT	30
3.2.4.1 Rozmanitost zařízení	31
3.2.4.2 Nedostatečně naddimenzovaná infrastruktura IoT	31
3.2.4.3 Rychlý vývoj aplikací a technologií	31

3.2.4.4	Ochrana osobních údajů	31
3.2.4.5	Problematika instalace zařízení	32
3.3	Sběr Dat.....	33
3.3.1	Cloud Computing.....	33
3.3.2	Konflikt sběru dat ve vztahu k GDPR	34
3.3.2.1	Anonymizace dat	35
3.3.2.2	Pseudonymizace dat.....	38
4.	Vlastní práce	40
4.1	Analýza IoT řešení	40
4.1.1	Analýza konektivity	40
4.1.1.1	LPWAN síť.....	41
4.1.1.2	Mobilní síť.....	42
4.1.1.3	LAN síť.....	43
4.1.1.4	WPAN síť	44
4.2	Pilotní ověření ve vybrané lokalitě.....	45
4.2.1	Použité technologie a jejich analýza	45
4.2.1.1	Popis IoT hardwaru.....	45
4.2.1.2	Analýza IoT hardware	46
4.2.1.3	Konektivita v oblasti Lázeňských lesů	46
4.2.2	Sběr dat	49
4.2.2.1	Pseudonymizace MAC adresy	50
4.2.3	Zpracování dat přes rozhraní Grafana.....	51
4.2.4	Rozdíly naměřených hodnot v závislosti na technologii	52
4.2.5	Statické zařízení v dosahu, které ovlivňují výsledky měření.....	54
4.2.6	Napětí baterií v závislosti na počasí.....	56
5.	Zhodnocení a doporučení	58
5.1	Použitý hardware včetně sítě technologie SigFox.....	58
5.2	Sběr dat s ohledem na vztah k GDPR	58
5.3	Porovnání technologií pro sledování počtu návštěvníků.....	59
5.4	Sledování stavu baterie.....	59
6.	Závěr.....	60
7.	Seznam použitých zdrojů.....	61
7.1	Odborné publikace	61
7.2	Internetové zdroje.....	63

8. Seznam obrázků, tabulek, grafů a zkratk	66
8.1 Seznam obrázků	66
8.2 Seznam tabulek	67
8.3 Seznam grafů.....	67
8.4 Seznam použitých zkratk.....	68

1. Úvod

Internet věcí je pojem, který je znám také pod označením jako Internet of Things, či zkráceně IoT. Jedná se o datové propojení předmětů, které posílají svoje posbíraná data, či nabízejí služby. IoT se již stalo součástí dnešní civilizace, i když si to mnohokrát lidé ani neuvědomují. Po regionech lze nalézt mnoho druhů zařízení, které komunikují přes síť internet. Důležitým prvkem IoT sítí je jejich konektivita, která umožňuje odesílání dat pomocí malého množství energie, nebo naopak posílání velkého množství nasbíraných dat. Existuje velké množství sítí a každá má jiné vhodné použití. Data je navíc potřeba anonymizovat kvůli ochraně osobních údajů, případně vzniká nutnost sbírat souhlasy o sběru a zpracování dat v rámci GDPR.

Zařízení IoT pomáhají zefektivnit služby a vylepšit kvalitu života. Pomocí chytrých parkovišť lze velmi snadno zaparkovat, bez nutnosti dlouhého hledání volného místa. Díky chytrým měřičům lze zas ušetřit finance v rámci chytrého odpojování zařízení, když zrovna není majitel doma. Velké instituce také již integrují IoT prvky v rámci zkvalitňování jejich služeb, například chytré letiště mohou pomoci při navigaci v prostředí areálu a dynamicky nabízet různé slevové akce anebo informovat o stavu nadcházejícího letu pomocí mobilního telefonu.

2. Cíl práce a metodika

Hlavním cílem práce je analýza IoT technologií v dané lokalitě a návrh jejich využití pro podporu regionálního rozvoje.

Dílčí cíle bakalářské práce jsou:

- Vytvořit přehled literatury a analýzu v oblasti současných informačních technologií užívaných s cílem podpořit rozvoj regionů.
- Na základě vybraných charakteristik provést analýzu vhodných IoT řešení.
- Analyzovat konflikt v oblasti sběru dat z těchto zařízení ve vztahu k GDPR.
- Provedení pilotního ověření ve vybrané lokalitě.

Teoretická část je založena na studiu a analýze odborných a vědeckých zdrojů z oblasti internetu věcí, především z oblasti jejich instalace a využití pro podporu regionálního rozvoje, sběru dat a jejich následné anonymizaci ve vztahu k GDPR. Na základě syntézy poznatků teoretické části a vyhodnocení výsledků praktické části budou formulovány závěry práce.

3. Teoretická východiska

3.1 Internet věcí

Internet věcí lze definovat jako: „*Sít' fyzických zařízení, vozidel, domácích spotřebičů a dalších zařízení, která jsou vybavena elektronikou, softwarem, senzory/čidly, a hlavně sít'ovou konektivitou. Která umožňuje těmto zařízením se navzájem propojit a vyměňovat si data.*“. Jedná se o rychle rostoucí síť, v polovině roku 2022 je aktivních více než 14,4 miliard zařízení, s odhadem na 27 miliard aktivních zařízení v roce 2025 (1)

Internet věcí nabízí poskytování služeb, či sběru dat a jejich následného vyhodnocení, které již probíhá na vzdáleném serveru. Myšlenka celého ekosystému IoT spočívá v plné automatizaci a poskytování dat a služeb bez potřeby pravidelného zásahu uživatele, uživatel by měl pouze provést počáteční nastavení nebo případnou kalibraci zařízení. (2)

3.1.1 Koncepce Smart

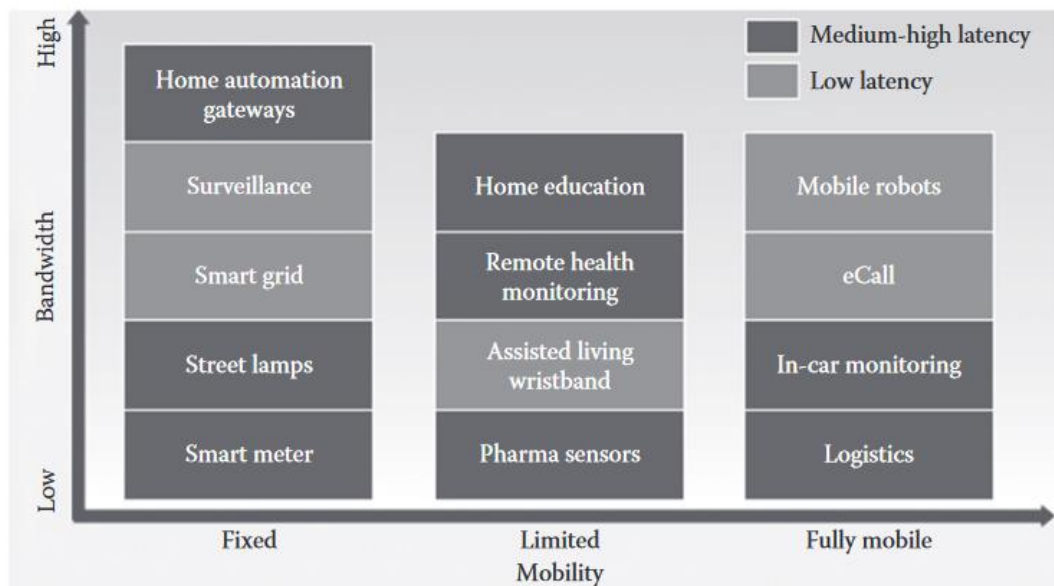
Zařízení, které spadá do kategorie internetu věcí, bývá velmi často také označováno jako „Smart“, tedy Chytré zařízení. Z běžných věcí vznikají zařízení Smart, jako chytré hodinky, chytré domácí spotřebiče, chytré lavičky, nebo chytré odpadkové koše. Existují ale také Smart řešení, jako například: Smart City, Smart Region, Smart House. Internet věcí právě propojuje Smart zařízení, nebo dělá z běžných zařízení, zařízení Smart. Zatímco termíny Smart City, Smart Region, Smart Village určují koncept, promyšlený plán a spíše základnu pro podporu dílčích projektů s využitím informačních technologií za podpory dlouhodobé strategie veřejné správy, případně strategie občana při stavbě domu. (3)

3.1.2 Konektivita

Funkční řešení IoT vyžaduje sít'ovou konektivitu. Otázka druhu připojení je závislá na několika proměnných. Je potřeba znát potřebnou latenci (odezvu internetového připojení), šířku pásma (datovou propustnost při spojení mezi zařízeními), prostředí umístění zařízení (otázka fixního spojení vs mobilního spojení) a znalost energetické náročnosti, která je závislá na druhu připojeného zařízení. Také je potřeba zhodnotit potřebu neustálého připojení, nebo intervalové připojování a odpojování od sítě za účelem úspory energie.

Graf na obrázku 1 znázorňuje požadavky na latenci a šířku pásma dle různých typů zařízení a služeb internetu věcí. (4)

Obr. 1: Ukázka vhodné konektivity v rámci různorodosti zařízení a služeb (4)



3.1.2.1 LPWAN

Velmi využívané v oblasti internetu věcí jsou rozsáhlé sítě s nízkým příkonem známé jako LPWAN. Tyto sítě nabízejí připojení pomocí radiových signálů s dlouhým dosahem při nízké spotřebě energie. Datová propustnost omezuje použití této technologie pouze pro zařízení, která odesílají jednoduché informace, jako například: chytré elektroměry, teploměry, parkovací místa nebo GPS lokátory. Další vlastností LPWAN sítí jsou nízké náklady na jejich využívání.

Mezi nejpoužívanější LPWAN sítě patří SigFox, Weightless, Nwave, Ingenu, LoRa, NB-IoT. (4)

Sigfox

Sigfox je velmi populární síť vyvíjená francouzskou společností, která paradoxně zbankrotovala v roce 2022, kvůli nedostatkům čipů a nenastání očekávaného nástupu IoT zařízení, avšak v České republice provoz stále pokračuje. (5)

Tato síť umožňuje přenést impulsy balíčků dat o velikosti 12 bajtů pomocí radiového pásma, přenosů může být odesláno maximálně 140 denně, což vychází na jednu za 10 minut, díky tomuto nestálému připojení dokáže zařízení fungovat až desítky let bez výměny baterie.

Nevýhodou této technologie je že vyžaduje přítomnost operátora, který využívá v Evropě radiové pásmo 868 MHz (V USA 915 a Asii 433Mhz). SigFox nabízí dosah 30-50 km v závislosti na prostředí. (6)

Nwave

Nwave je síťové řešení britské společnosti Nwave Technologies, které vzniklo za účelem dálkového odpočtu elektroměrů a vodoměrů, chytrého parkování a zemědělství. Nwave umožňuje přenosovou rychlost až 100b/s, s dosahem 7-10 km. Uživatelská zpráva je do 20 bajtů. Tato technologie byla zkoušena ve Velké Británii a Dánsku. (7)

Weightless

Tato síť byla vyvíjena od roku 2012 neziskovou organizací Weightless Special Interest Group, která vytvořila otevřené specifikace a certifikace. První představenou technologií byla v dubnu 2013 Weightless-W, která využívá tzv. „whitespace“ v televizním pásmu 400 až 800 MHz. Přenosová rychlost Weightless-W dosahuje až 10 Mb/s s dosahem ve městě až 5km a životností baterie 3 až 5 let. Využití Weightless-W se zatím vztahovalo převážně na Velkou Británii. (8)

V roce 2015 vznikla technologie Weightless-N, která vychází z Nwave. Umožňuje přenos pouze jednosměrně od koncových zařízení s přenosovou rychlostí 100b/s se stejným dosahem a životností baterie jako u technologie Weightless-W. (8)

V červenci 2015 vznikla specifikace Weightless-P, která už umožňuje obousměrnou komunikaci s přenosovou rychlostí 200b/s s dosahem přes 2km a životností baterie 3 až 8 let. (8)

Ingenu

Ingenu používá technologii RPMA (Random phase multiple access). Tato technologie funguje na nelicencovaném celosvětově dostupném 2,4 GHz pásmu, lze jej tedy snadno nasadit kdekoli na světě. RPMA poskytuje rychlost stahování 31 kb/s a odesílání 15,6 kb/s, tedy jedná se o oboustranný přenos, signály této technologie umí pronikat hluboko do budov a podzemí. (9)

LoRa

Síť LoRa byla vyvinuta společnostmi Semtech, IBM research a Actility. LoRa je označení pro standart sítě, zatímco LoRaWAN je označení pro celý komunikační protokol a architekturu celé sítě. Jedná se o otevřený ekosystém, tedy existuje mnoho softwaru a dodavatelů. Aby bylo možné tento standart využívat je potřeba spustit software serveru, který vyžaduje předplatné, navíc Semtech je jediným dodavatelem, který vyrábí potřebné čipy, a tedy dost ovlivňuje cenu a rozsah výroby.

LoRaWAN umožňuje komunikovat oběma směry s teoretickým dosahem až 20 km a s dosahem 2 km v zastavěném prostředí. Výdrž baterií je až 10 let. Stejně jako síť SigFox i LoRaWAN komunikuje v nelicencovaném pásmu 868 MHz. Datová propustnost je až 50 kb/s. Každé zařízení vyžaduje certifikaci, což nutí výrobce řešit i bezpečnostní rizika. V České republice síť budují České Radiokomunikace, které již vystavěli 1450 vysílačů LoRa. Zároveň CRA vydává i certifikace. (10) (11) (12)

NB-IoT

NB-IoT je úzkopásmová datová síť, která využívá infrastruktury mobilních operátorů. V České republice za touto technologií stojí mobilní operátoři jako například Vodafone. Nemusejí vytvářet novou infrastrukturu, ale pouze upraví software na stávající infrastrukturu, taková úprava vyhradí část pásma pro IoT. Zařízení, které podporují NB-IoT. Zařízení musí obsahovat SIM kartu, podobně jako zařízení v síti LTE. Nabízí datovou propustnost až 200 000 bit/s, s dosahem 20km. Vysílače LTE českých operátorů jsou pokryté téměř po celé České republice a komunikovat by tedy mělo jít všude kde je dostupná LTE síť. V porovnání s ostatními technologiemi LPWAN je nejnáročnější na spotřebu energie. (12)

IQRF

IQRF umožňuje komunikaci v nelicencovaném radiovém pásmu 868 MHz, vysílání nabízí rychlost až 20 kb/s a jednotlivé pakety mají velikost až 64 bajtů. Tato technologie vznikla v České republice, vyvíjí ji společnost MICRORISC se sídlem v Jičíně od roku 2004. Komunikace funguje na principu brány, kterou lze postavit na vývojových sadách s malým radiovým modulem. Výhodou této technologie je podpora MESH NETWORKING, tedy propojení každého s každým, kdy každé zařízení v dosahu přepoše přijatou zprávu dál, není nutnost stavět vysílače s dlouhým dosahem, ale pouze mít v dosahu každého zařízení,

zařízení další. Navíc lze díky protokolu IQMESH na jedno vysílání získat informace od všech zařízení, což snižuje dlouhodobě energetickou náročnost. (13)

3.1.2.2 Mobilní síť

Mobilní síť nabízí spolehlivou širokopásmovou komunikaci. Nevýhodou jsou velmi vysoké provozní náklady a nároky na napájení. Mobilní síť nejsou vhodné pro menší senzorové zařízení, která jsou napájena baterií, vhodné jsou naopak například k připojení automobilů (pro služby infotainmentu, informace o dopravě a pokročilé asistenční systémy), případně pro streamování videa, nebo různé hlasové komunikační aplikace. (14)

Aktuálně se využívají v rámci mobilních sítí 3G, 4G a 5G standardy. V tabulce 1 lze sledovat jejich postupný vývoj. S nástupem novějších generací dochází k zvýšení datové propustnosti a snížení latence.

Tab. 1: Porovnání mobilních sítí od 3. do 5. generace. (15)

	3G	4G	5G
Uvedení na trh	2004	2006	2019
Teoretická rychlost	2 Mbit/s	200 Mbit/s	1 Gbit/s
Latence	100-500 ms	20-30 ms	pod 10 ms
Průměrná rychlost	144 kb/s	25 Mbit/s	200-400 Mbit/s

3.1.2.3 WPAN síť

WPAN je bezdrátová počítačová síť používaná pro přenos mezi jednotlivými zařízeními. Bezdrátová komunikace probíhá maximálně v rámci desítek metrů. Přenos probíhá v režimu P2P, tedy není potřeba třetího zařízení pro řízení komunikace mezi příjemcem a odesílatelem. (16)

Nejpoužívanější protokoly WPAN sítě v rámci IoT jsou ZigBee, Bluetooth a NFC.

Zigbee

Zigbee je nízkoenergetický komunikační protokol k používání sítí topologie MESH. Za účelem vývoje této sítě byla vytvořena v roce 2002 ZigBee aliance, která sdružuje desítky různých společností, například Philips, Siemens, Motorola, Samsung, Amazon, Bosch, Xiaomi. Hlavní atributy ZigBee sítě je spolehlivost, nenáročnost na infrastrukturu a nízká spotřeba energie, přenosová rychlost je přibližně 10 až 100m v závislosti na prostředí.

Jedná se o otevřený standard, který komunikuje v nelicencovaných pásmech 868 MHz, 902-928 MHz a 2,4 GHz. (17)

Bluetooth – BLE

Bluetooth je standard pro bezdrátovou komunikaci, komunikující v rámci P2P spojení. V dnešní době tento standard obsahuje téměř každé zařízení. Bluetooth 5 generace zvládá rychlost až 2 Mb/s a teoretický dosah až 400m.

BLE(Bluetooth low energy) vznikl v rámci Bluetooth 4.0, využívá radiové spojení na krátkou vzdálenost s minimálním výkonem a funguje po dlouhou dobu. Jeho dosah je přibližně 100m. BLE pracuje s výkonem přibližně od 0,01 mW a 10mw.

Bluetooth Beacon je malé bezdrátové zařízení (maják), které vysílá signál jedinečného identifikátoru, pokud má uživatel zapnuté Bluetooth tak obdrží notifikaci, která ho může upozornit na nějakou zajímavost, nebo mu pomoci se lépe orientovat v rušných a velkých prostorech. (18)

NFC

NFC síť komunikuje na vzdálenost do několika cm. Tato technologie spočívá v přiblížení dvou zařízení pro obousměrnou komunikaci. Technologie vychází ze staršího standardu RFID, který k přenosu informace využívá elektromagnetickou indukci, tento způsob umožňuje použití pasivního zařízení – nálepky, štítku atd. V dnešní době se NFC využívá při čtení karet, či bezkontaktním placení. Data mohou být odesílána rychlostí až 424 kb/s. Výhodou této sítě je že ji podporuje většina smartphone zařízení. (19)

3.1.2.4 LAN

LAN síť je označení pro lokální síť, která pokrývá malý prostor, například rodinný dům, kancelář, nebo také firemní síť s tisíci zařízeními. Tato síť je řízena centrálním prvkem – routerem.

Ethernet

Ethernet je označení pro přenos dat pomocí fyzického média. Pro přenos se využívá převážně kroucená dvojlinka, nebo optické kabely, dříve se používal i koaxiální kabel (ten se již dnes pro malou propustnost dat nevyužívá). Tato technologie poskytuje velmi vysokou spolehlivost, nízkou odezvu a velmi vysokou datovou propustnost,

avšak je náročnější na stavbu infrastruktury. Data musí být navíc po určité vzdálenosti posilována. Pro přenos dat pomocí kroucené dvojlinky k dosažení maximální rychlosti dané kategorie musí být v určité vzdálenosti použit aktivní prvek sítě, avšak trasa může mít maximálně 100m. Nejnovější kategorie Cat8 nabízí datovou propustnost až 40 Gb/s na vzdálenost 30m. Nejrozšířenější je dnes Cat5e, která dosahuje 1Gbit na vzdálenosti 100m a Cat6, která nabídne rychlost až 10Gbit na 37m. (20)

Wi-Fi

Wi-Fi je dnes nejvyužívanější bezdrátová síť, která využívá pásma 2,4 a 5 GHz. Všechny moderní zařízení jako počítače, notebooky, chytré televize, telefony, jsou vybaveny podporou Wifi. Wifi na rozdíl od ethernetu není náročná na stavbu infrastruktury. Tato síť je schopna dosahovat velkých rychlostí, avšak s velkým odběrem energie, proto není vhodná pro malá IoT zařízení.

Síť Wi-Fi se stále vyvíjí a dochází k zaváděním nových standardů, v tabulce 2 lze vyčíst standardy a jejich datovou propustnost.

Tab. 2: Porovnání standardů Wi-Fi (21)

Název	Standard	Pásma	Propustnost
Wi-Fi 1	802.11b	2,4 GHz	11 Mb/s
Wi-Fi 2	802.11a	5 GHz	54 Mb/s
Wi-Fi 3	802.11g	2,4 GHz	54 Mb/s
Wi-Fi 4	802.11n	2,4 + 5 GHz	600 Mb/s
Wi-Fi 5	802.11ac	5 GHz	3,5 Gb/s
Wi-Fi 6	802.11ax	2,4 + 5 GHz	9,6 Gb/s
Wi-Fi 6E	802.11ax	2,4 + 5 + 6 GHz	9,6 Gb/s
Wi-Fi 7	802.11be	2,4 + 5 + 6 GHz	46,1 Gb/s

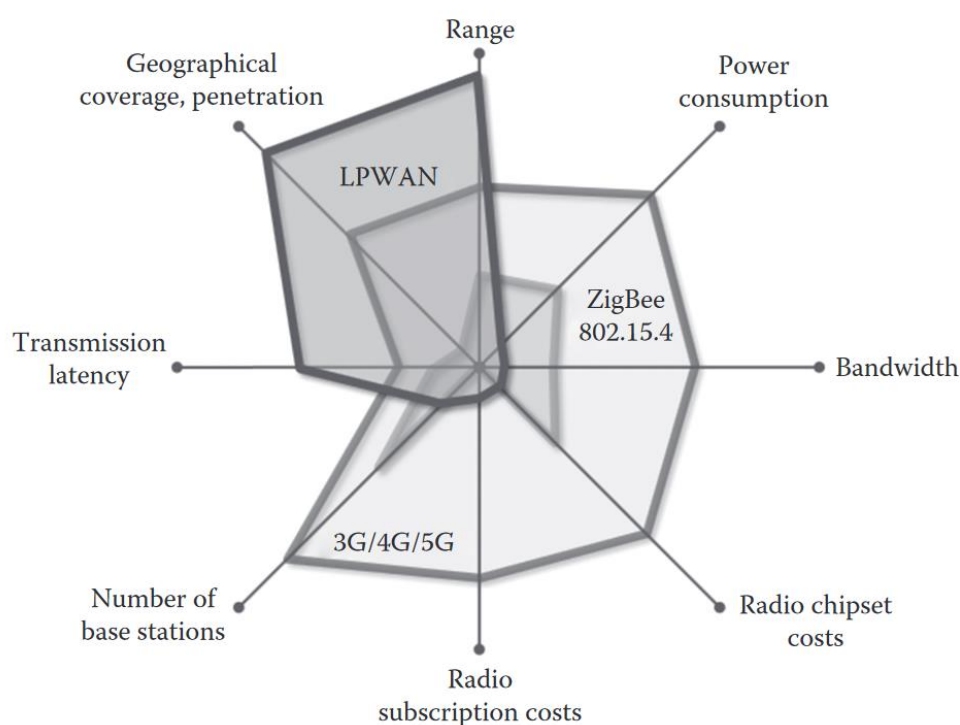
Wi-Fi HaLow je bezdrátová síť vyvinuta pro použití v IoT označována jako 802.11ah. Na rozdíl od klasické wifi využívá kmitočty okolo 900 MHz (v Evropě 868 MHz). Tato síť je zkonstruována pro velký dosah s malým energetickým odběrem. Datová propustnost

se pohybuje od 150kb/s do 80Mb/s dosahem několika stovek metrů až 1km. HaLow síť lze uplatnit i pro přenos obrazu z bezpečnostních kamer, či jiného streamu. (22) (23)

3.1.2.5 Porovnání

Každá technologie má svoje využití v daném odvětví. A je tedy nutné při vývoji IoT zařízení definovat nároky na síť, navíc není vyloučeno sítě kombinovat v rámci jedné velké infrastruktury. V grafu na obrázku 2 lze sledovat porovnání bezdrátových technologií v závislosti na parametrech, které jsou v oblasti IoT velmi důležité. Zatímco LPWAN sítě mají velmi dobrý dosah a dobrou propustnost přes objekty jako například zdi a jiné možné předměty, tak mobilní sítě vynikají v datové propustnosti, avšak jsou nákladnější a vykazují velkou spotřebu elektrické energie. U ZigBee sítí lze sledovat nižší dosah a poměrně nízkou spotřebu a náklady na pořízení. (24)

Obr. 2: Porovnání vlastností bezdrátových technologií (24)



3.1.3 Napájení

Jedním z klíčových otázek ve světě internetu věcí je správa napájení, tedy jak zajistit energetický zdroj pro miliardy zařízení, které jsou součástí internetu věcí. Je tedy potřeba

optimalizovat spotřebu elektrické energie u zařízení IoT. Například omezit vysílání na určité časové intervaly během dne, nebo použít vhodnou síť pro přenos dat a určit kdy a jak má zařízení operovat, tedy jak často je třeba sbírat data, jak dlouho se data sbírají a kolik to spotřebuje energie a samozřejmě jak aktuální data potřebujeme.

Zdroj zařízení může být omezený zdroj, který bude potřeba uživatelsky měnit, nebo zdroj, který může energii generovat. Také lze zařízení připojit k elektrické síti, avšak to vyžaduje v mnoha státech značná povolení, plány a stavbu infrastruktury, navíc při představě zapojení miliard takových zařízení do elektrické sítě je tato myšlenka neproveditelná a velmi nákladná. Zařízení také nejsou vždy umístěna v dosahu energetické sítě, a tedy vyvíjejí zařízení velmi často využívají vlastní zdroj energie.

Zařízení jsou obvykle napájena bateriemi, nebo akumulátory s možností generování energie z okolních zdrojů. Při volbě napájení baterií záleží na výdrži zařízení, u malých zařízení při předpokladu výdrže baterie jednotky nebo desítky let je baterie nevyměnitelná, a tedy životnost zařízení je omezená s životností baterie. Zatímco při vyšší spotřebě je zařízení navrženo tak, aby baterie byla vyměnitelná. Toto řešení vyměnitelných baterií je efektivní pro malé systémy zařízení v internetu věcí, ale pro velké systémy IoT je toto řešení neefektivní kvůli nákladům na údržbu a pravidelné výměně miliard kusů baterií. Řešení této problematiky je Energy harvesting. (25)

3.1.3.1 Energy harvesting

Energy Harvesting je metoda získávání elektrické energie z okolních zdrojů pomocí prvků jako solární články, piezoelektrické a termoelektrické generátory, atd. které vytvářejí elektrickou energii ze světla, vibrací, tepelné energie, nebo pomocí rádiové frekvence. Tyto zdroje lze použít převážně díky nízké spotřebě energie zařízení.

Existují různé způsoby sběru energie. Harvest and use metoda generuje dostatečnou energii a v reálném čase ji zařízení ihned spotřebovává. Pokud vygenerovaná energie není dostatečná pro chod zařízení, bude zařízení v nečinném stavu. Zatímco Harvest-Store-Use metoda napájí zařízení a když je vygenerované energie více tak akumuluje energii pro budoucí použití. Alternativně lze také energii akumulovat tak dlouho, dokud ji nebude dostatek pro provoz systému. (25)

3.1.3.2 Zdroje pro získávání energie

Zdroje pro získávání energie mohou být buď enviromentální zdroje jako je sluneční energie, vítr atd. Nebo zdroje jako například teplotní rozdíly, energie získávaná z pohybu, nebo vibrací.

Sluneční energie

Sluneční energie je nejúčinnějším zdrojem energie pro zařízení IoT. Solární energie se získává pomocí fotovoltaických článků, které využívají fotoelektrický jev, který působením fotonů na různé materiály vzniká elektrický proud. Fotovoltaický článek se používá v lokalitě, kde je zaručená dostupnost světla. (25)

Tepelná energie

Tepelná energie transformuje teplo, nebo rozdíl teplot na energii. Jevy používané pro získávání energie jsou termoelektrické a pyroelektrické. Termoelektrická metoda přímo přeměňuje rozdíl teplot na využitelnou energii. Pyroelektrická metoda generuje elektrickou energii, když dochází ke změně teploty. Používá pyroelektrický krystal, který generuje energii při zahřátí nebo ochlazení. Účinnosti přeměny této energie jsou velmi nízké. (25)

Mechanická energie

Mechanická energie se získává z pohybu, vibrací a tlaku. Získávání energie probíhá pomocí piezoelektrického, elektrostatického nebo elektromagnetického zdroje. Elektrostatické zdroje převádí vibrace na elektrickou energii. Piezoelektrické zdroje přímo převádí kinetickou energii na energii elektrickou pomocí deformace krystalu. Elektromagnetické zdroje vytváří elektrickou energii při vzniku pohybu mezi vodivou cívkou a zmagnetizovaným tělesem. energii lze vytvářet i pomocí lidského těla, například pomocí pohybu prstu. (25) (26)

Získávání energie pomocí radiových signálů

Elektrickou energii lze vytvořit i pomocí elektromagnetických signálů, které se nacházejí v okolí zařízení. Například pomocí výkonných 5G sítí v okolí lze vytvořit malé množství energie kolem 6 mW na vzdálenost 180m od vysílače, pomocí speciálního typu antény zvané rectenna, ta převádí elektromagnetickou energii na stejnosměrný proud. (27)

Tab. 3: Srovnání zdrojů generující energii. (25)

Zdroj	Zařízení pro převod	Výkon	Výhody	Nevýhody
Solární energie	Fotovoltaický panel	15 - 100 mW/cm ²	K dispozici během dne, vysoký výkon	Není k dispozici v noci, malá efektivita během zatažených dnů, nutnost výhledu na oblohu
Větrná elektřina	Anemometr	1200 mWh/den	K dispozici na otevřených prostorách	Nepoužitelný v uzavřených objektech
Pohyb prstu	Piezoelektrický zdroj	2.1mW	K dispozici kdykoliv je potřeba	Energie je generována jen když dochází k pohybu prstu
Vibrace	Elektromagnetická indukce	0.2 mW/cm ²	Dostupný zdroj energie	Malé množství vygenerované energie
Tepelná energie	Termočlánek	50 mW/cm ²	Spolehlivý, nízké úroky na údržbu	Nízká účinnost
Radiový zdroj	Rectenna	1 μW/cm ²	Velký počet elektromagnetické energie	Nízká hustota výkonu

V tabulce 3 lze sledovat jednotlivé zdroje energie a jejich výkon v závislosti na velikosti zdroje nebo čase. Každý zdroj elektrické energie přináší různé výhody a nevýhody, tedy je nutné při navrhování IoT zařízení zvážit volbu zdroje.

3.2 Příklady integrace IoT

Prvky IoT již fungují v rámci veřejných zařízení a služeb, které díky integraci IoT zařízení se stávají efektivnějšími, a tedy prospěšnějšími pro uživatele daných zařízení a služeb.

3.2.1 Chytré letiště

Letiště procházejí neustálým vývojem, aby byla schopna uspokojit stále rostoucí a neustále se měnící požadavky cestujících v letecké dopravě. Dnešní letiště se potýkají s kritickými problémy v oblasti efektivnosti, které jsou způsobeny tím, že technologie a procesy, které jsou v nich zavedeny, nestačí na zvládnutí stále rostoucích toků cestujících což následně vede ke zhoršení kvality služeb pro cestující. Některé z nejčastějších problémů, kterým cestující čelí, jsou následující:

- Problémy se zavazadly: Chybějící, ztracená nebo špatně manipulovaná zavazadla, zpoždění při výdeji zavazadel
- Zpoždění při odbavení: Zpoždění při odbavení u vchodu na letiště a u odbavovacích přepážek, zejména na letištích při cestování v období dovolených.
- Řízení poruch: Nepříjemnosti pro cestující způsobené zpožděním a zrušením letů.

Letiště se v dnešní době rozdělují na 3 úrovně podle technologické vyspělosti. (28)

3.2.1.1 Airport 1.0

Letiště 1.0 byli převážně letiště v 80. letech, které pouze zajišťovali bezpečnost cestujících a letadel. Důraz byl tedy kladen pouze na bezpečnostní aspekty a žádná další pozornost nebyla věnovaná zařízením, které by cestujícím zlepšila pohodlí a efektivnost během cestování. Letištní procesy byly minimálně automatizované, a tedy bylo zapotřebí mnoho zaměstnanců. Navíc bylo potřeba vyplňovat mnoho formulářů což mělo za následek mnoho chyb kvůli ručnímu zpracování dat. (28)

3.2.1.2 Airport 2.0

Na letištích 2.0 již je zavedeno mnoho infrastruktury využívající IT, kdy jednotlivé sektory mezi sebou komunikují. Je zavedeno bezdrátové širokopásmové připojení (Wi-Fi, podpora mobilních sítí) a jsou vytvořeny aplikace na mobilní zařízení pro cestující, které pomáhají cestujícím zlepšit zážitek z cestování.

Existuje mnoho aplikací, které poskytují podrobné informace cestujícímu o letišti, jako podrobnosti služeb, stavy letů a navigace na letištích, aktuální časové pásmo a cílové časové pásmo. Na letištích se také nacházejí interaktivní dotykové displeje, které obsahují interaktivní mapy. (28)

3.2.1.3 Airport 3.0

Letiště 3.0 dále rozvíjí technologie využívané v konceptu letiště 2.0, klíčové jádro konceptu letiště 3.0 je IoT. IoT umožňuje analyzovat velké množství dat a tím zlepšit efektivitu celého letiště. Více než 75 % letišť plánuje poskytovat služby cestujícím prostřednictvím chytrých telefonů. Což umožní cestujícím poskytovat personalizované nabídky podle jejich požadavků, využívání mobilních telefonů umožní také lépe sledovat polohu cestujících čímž se snadno předejde dlouhým frontám, díky posílení personálu v kritické části letiště. Využití lokalizační technologie v chytrých telefonech tedy umožní letišťům předvídat a odhadovat čas, který cestující stráví v různých zónách letiště. Jednou dalších inovací je možnost se samoobslužně odbavit pomocí aplikace na mobilním zařízení, webu, nebo na samoobslužném kiosku. (28)

Na letištích 3.0 dochází také k využívání beacon technologie (majáků) pomocí technologie Bluetooth BLE, která umožní kontaktovat cestujícího s chytrým telefonem až na vzdálenost 70m, tyto majáky lze využít pro lepší navigaci uživatele, například jej navigovat ke správnému nástupišti. Dále tato technologie může cestujícího upozornit na různé služby či slevové akce, které letiště nabízí, případně cestujícímu poskytnout informace o jeho letu, nebo ho informovat kde bude vydáváno jejich zavazadlo s přibližným časem kdy zavazadlo dorazí.

Velký posun na letištích 3.0 se týká NFC technologií, kdy místo palubní letenky stačí nosit mobilní zařízení s NFC tokenem, který veškeré informace o letence již obsahuje. To umožní snazší pohyb cestujících pomocí NFC snímačů rozmístěných po letišti, které cestujícího navedou na správný terminál, tedy dojde k rychlejšímu odbavení cestujícího. Využívání NFC letenek také umožní dynamicky měnit letenku v závislosti na neočekávaných změnách na letišti, tím se také usnadní efektivita přesunu lidí. NFC technologie se také využívají k placení po celém areálu letiště, což umožní cestujícímu nedisponovat hotovostí, a tedy mít lepší správu a zabezpečení nad jeho financemi. (28)

Další změna probíhá u logistiky zavazadel, kdy zavazadlo místo čárového kódu obdrží RFID identifikátor. To snižuje šanci ztráty, nebo odcizení zavazadla, vzhledem k tomu, že lze na rozdíl od čárového kódu RFID identifikátor číst na dálku pomocí RFID čteček. Díky tomu jsou zavazadla nepřetržitě sledována od místa vstupu až po jejich naložení do příslušného zavazadlového prostoru. Použití této technologie zlepšuje, jak spokojenost cestujících, protože se méně budou ztrácet zavazadla, ale také sníží náklady letiště na úhradu ztracených, nebo odcizených zavazadel. (28)

3.2.2 IoT ve zdravotnictví

Závislost zdravotnictví na internetu věcí se neustále zvyšuje, převážně kvůli potřebě sbírání a analyzování velkého množství dat a jejich ukládání na cloud. Internet věcí může zdravotnictví poskytnout:

- Zajištění rychlého přístupu ke zdravotní péči.
- Zvýšení kvality zdravotnického zařízení.
- Zkrácení doby potřebné k získání kvalitní zdravotní péče.

Použití internetu věcí také řeší nedostatek zdravotních pracovníků po celém světě, díky digitalizaci a sběru dat lze rychleji určovat diagnózu a zvolením správné léčby zkrátit čas pacienta ve zdravotním zařízení. Navíc není potřeba vyplňovat tolik formulářů v rámci propojení systémů, a tedy lze opět omezit chyby, ke kterým dochází při ručním vyplňování dat. Chytré systémy mohou také díky přístupům k datům pacienta naplánovat pravidelné kontroly, případně pacienta pomocí například mobilního zařízení včas upozornit na vhodnou kontrolu. (29)

3.2.2.1 Klinická péče

Mnoho chronicky nemocných pacientů vyžaduje neustále sledování životně důležitých tělesných parametrů. Za normálních okolností jsou tyto pacienti umístěni na jednotkách intenzivní péče v nemocnicích. IoT technologie nabízí neinvazivní monitorování pomocí senzorů, které shromažďují komplexní fyziologické informace týkající se různých životně tělesných parametrů. Údaje nashromážděné pomocí těchto senzorů jsou odesílány pomocí bran a bezdrátových sítí blízkým příbuzným a ošetřovatelům, kteří mohou přijmout vhodná opatření k ošetření pacienta a včas zareagovat na případný zhoršení stavu pacienta. Tato technika internetu věcí nahrazuje tradiční nepřetržité monitorování v nemocnicích

zdravotnickými pracovníky a poskytuje automatizovanou zdravotní péči doma chronicky nemocným pacientům s poměrně nízkými náklady. Pomocí IoT technologií lze dále u chronicky nemocných pacientů zajistit na dálku tyto zařízení a služby: (29)

- Chytrý dávkovač léků
- Senzor detekce pádu
- Senzor času stráveného v klidu
- Měření doby a kvality spánku
- Sledovací zařízení

3.2.2.2 Monitorování na dálku

Lidé, kteří žijí v odlehlých oblastech, nebo lidé kteří nechtějí trávit čas po zdravotních zařízeních mohou být monitorováni na dálku. Senzory, které jsou propojeny pomocí internetu věcí, umožní monitorování zdravotního stavu a nashromáždí data, pomocí kterých lze pomocí komplexních algoritmů pro analýzu dat určovat různé diagnózy a konzultovat data s lékaři. Kromě sledování životně tělesných parametrů se sleduje také pohyb a aktivity. Pomocí monitorování lze také určit fyzickou kondici člověka a například mobilní aplikace, nebo web může uživateli sestavit plán, jak zlepšit jeho zdravotní stav. Navíc tyto data lze sdílet s vlastním lékařem a předejít tak včas možným zdravotním problémům. Různé typy snímačů a zařízení, které lze v tomto sektoru použít, jsou následující: (29)

- Snímače hmotnosti
- Monitory aktivity
- Monitory srdečního tepu a tlaku
- Monitory na cvičicích nástrojích (Běžecský pás atd.)

3.2.3 Další IoT prvky v regionech

Existuje mnoho dalších konceptů využití IoT, které napomáhají v regionálním rozvoji, například chytrá města, která využívají infrastruktury chytrých sítí ke zlepšení kvality života ve městě, zejména v oblasti řízení spotřeby energie, lepší koordinace veřejných zdrojů, zefektivnění veřejných služeb a udržitelnosti životního prostředí. Obyvatelé měst mohou lépe hospodařit se svojí spotřebou elektrické energie, nebo vody z vodovodního řádu pomocí chytrých elektroměrů. Lze snadno pomocí chytrého telefonu určit stav nepřítomnosti v domě, a tak vypnout světla, nebo nepotřebné spotřebiče a regulovat i teplotu pro vytápění,

nebo chlazení po dobu nepřítomnosti. Zlepšení kvality života ve městech napomáhají také chytré parkoviště, nebo chytré veřejné služby jako například chytrý odvážení komunálního odpadu, nebo vylepšení služeb obchodníků, kteří mohou díky velkému objemu shromažďovaných a zpracovávaných dat vylepšit nabídku produktů, které nabízejí a lépe optimalizovat nabídku pro jednotlivce. Pouze zavedení infrastruktury pro IoT zařízení pomůže ke zlepšení služeb, které IoT může nabídnout. (30)

3.2.3.1 IoT Elektroměr / vodoměr

Již dochází k postupnému přechodu od klasických analogových, nebo nechytrých digitálních měřičů spotřeby vody, nebo elektřiny k měřičům které jsou schopny svojí naměřenou hodnotu v pravidelných intervalech odesílat. Tyto chytré měřiče ušetří náklady společností, protože už nebudou muset posílat zaměstnance to terénu, aby naměřená data ručně zapsali. Tím se navíc předejde možnosti chyby lidského faktoru.

Chytrý vodoměr také může pomoci detekovat únik vody včas, díky živým datům a znalostem průměrné spotřeby v daných sektorech. K odesílání dat se většinou využívají LPWAN sítě jako například LoRaWAN, díky využití LPWAN sítí lze tyto měřiče provozovat více než 10 let na baterii. (31)

Spotřebitelé mohou také lépe hospodařit se spotřebou energie, nebo vody díky aplikacím, které jim zobrazí data o jejich spotřebě.

3.2.3.2 Chytré parkoviště

Řidič může hledat parkovací místo v průměru až 22 minut, což pro něj znamená větší spotřebu paliva a pro město zase vyšší provoz a samozřejmě vyšší emise. Senzory volného místa na parkovišti mohou tomuto problému předejít, kdy pomocí integrace do navigačních aplikací, nebo chytrých značek může řidič přímo jet k volnému místu a ušetřit čas. (32)

Tyto zařízení mají v sobě integrovanou baterii a používají LPWAN sítě. Dále chytré čidlo na parkovišti může také komunikovat s vozidlem a zjistit zda-li je vozidlo oprávněno stát na daném parkovišti, případně kontaktovat potřebné orgány, pokud oprávnění vozidlo nemá. (33)

3.2.3.3 Využití IoT v rámci služeb obchodů

Obchodníci mohou díky datům nasbíraných pomocí IoT lépe optimalizovat nabídku služeb, ale také zlepšit jejich kvalitu. Použití bezdrátových digitálních nápisů, nebo bezdrátových

beaconů u zboží umožňuje dynamicky měnit ceny a slevy bez nutnosti pracného obcházení zaměstnanci, a tak si lépe udržet a uspokojit věrné zákazníky obchodu. Výdejní automaty a samoobslužné pokladny pomáhají snížit náklady obchodů, díky nižšímu počtu zaměstnanců, a tedy sníženým nákladům na mzdy. (30)

3.2.3.4 IoT v komunálních službách

Odvoz odpadů lze zefektivnit instalováním ultrazvukových senzorů do kontejnerů, které budou komunikovat v rámci IoT sítí. Pomocí nasbíraných dat lze předpovídat naplněnost kontejnerů a zamezit jejich cyklickému vyvážení, kdy nemusí být pokaždé plné, tedy optimalizovat svozové trasy, aby se vyváželi pouze kontejnery plné. Tím se dají ušetřit provozní náklady díky snížení počtu svozových aut včetně zaměstnanců. V rámci optimalizované trasy se bude v svozové oblasti objevovat méně svozových aut, což ocení převážně obyvatelé oblastí, protože bude docházet k menšímu přetížení komunikací, což se projeví na zlepšení kvality života v oblasti.

Díky propojení v rámci aplikací mohou stav kontejneru sledovat i samotný občané a ušetřit si tak zbytečnou cestu k plnému kontejneru, nebo nalézt aktuálně volný kontejner. Pomocí aplikací lze také hlásit poškození kontejneru, a navíc chytrý kontejner může v případě požáru automaticky kontaktovat nejbližší požární stanici.

Umístěním RFID nebo QR technologie na odpadní kontejner může pomoci k identifikaci majitele kontejneru, adresu jejího původního uložení v případě krádeže, nebo informovat o harmonogramu svozu takového kontejneru. (34)

3.2.3.5 Použití senzorů v zemědělství

Pomocí různých senzorů lze zvýšit efektivnost farmy a zemědělských podniků. Lze měřit teplotu a vlhkost, jak už ve skladovacích zařízeních ale i přímo v porostech, ale také lze sledovat například odvlhčení listů. Na základě těchto senzorů lze v reálném čase sledovat a vyhodnocovat podmínky a předcházet škodám na úrodě způsobených škůdci a chorobami, nebo nedostatkem vláhy. Tyto senzory opět využívají LPWAN sítě kvůli jejich nízké spotřebě a dobrému pokrytí. (35)

3.2.4 Problémy při instalaci IoT

Integrace IoT zařízení a systémů do různých institucí přivádí mnoho problémů, které je třeba pro efektivní využívání IoT systémů vyřešit. Mnoho institucí má již zavedené databáze

a systémy, které nemusí být kompatibilní s IoT infrastrukturou. Také je třeba řešit otázku sběru dat se souhlasem uživatelů k jejich sběru soukromých informací. (36)

3.2.4.1 Rozmanitost zařízení

Ke správnému shromažďování a odesílání dat pomocí sítě do databáze je potřeba dodržovat standardy mezi zařízeními a bránami, a také bránami a databázemi. Vzhledem k tomu, že existuje mnoho výrobců, tak mohou vzniknout potíže během kombinace různých zařízení. Proto existuje mnoho certifikací, avšak stále mnoho produktů od různých výrobců tyto certifikace nenabízí. Dále je potřeba pracovat s již zavedenými databázemi a daty, které je potřeba propojit s moderními IoT zařízeními. Tyto problémy s kompatibilitou mezi zařízeními vedou k zvýšeným nákladům na integraci systémů. (36)

3.2.4.2 Nedostatečně naddimenzovaná infrastruktura IoT

K postupné instalaci stále více zařízení do systému internetu věcí, se neustále bude zvyšovat objem dat, která se budou přijímat, ukládat a analyzovat. Vzhledem k rozlišnosti typu přebíraných dat, je potřeba dostatečně naddimenzovat infrastrukturu na základě odlišnosti oblasti využití, aby další růst systému mohl být plynulý bez větších investic. Integrace IoT do již zavedené síťové infrastruktury může přinést problém, který později vyvrcholí nutností infrastrukturu přetvořit a tím vzniknou potíže, které by při prvotní integraci nenastaly (Nutnost vypnout IoT síť po dobu údržby, lidé už bez ní nebudou schopni pracovat jako před jejím zavedením). (36)

3.2.4.3 Rychlý vývoj aplikací a technologií

Vzhledem k neustálému posunu technologií roste také zájem uživatelů o nové služby, tudíž je potřeba neustále systémy vylepšovat což vyžaduje poměrně vysoké finance. Pokud by instituce zanechala systémy stávající, mohlo by se stát, že za několik let by uživatelé již nebyli schopni systémy používat (Zánik technologií například na mobilním zařízení jako je NFC, Bluetooth, Wi-Fi a začátek využívání jiných a lepších technologií). (36)

3.2.4.4 Ochrana osobních údajů

Data, které jsou shromažďována pomocí systémů, musí být dostatečně chráněny před jejich únikem a poškozením. Instituce musí mít také souhlas uživatele s nakládáním jeho osobních dat, které například díky integraci a digitalizaci starších systému nemusí mít v dostatečné

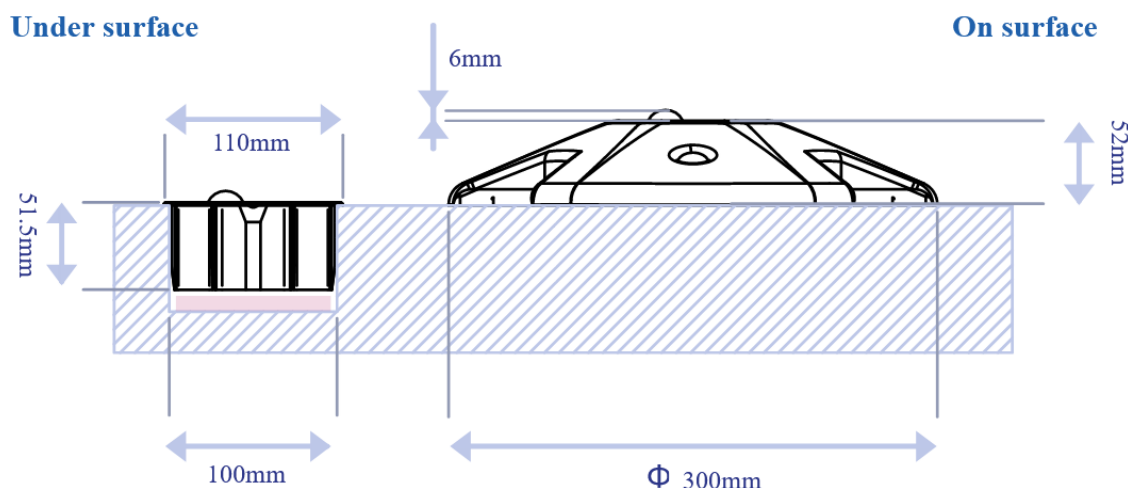
právní podobě. Je potřeba dodržovat zásady a postupy, které zajistí, že do informačních systému a databází se dostanou pouze oprávněné osoby a aplikace budou mít přístup pouze k žádoucím informacím. (36)

3.2.4.5 Problematika instalace zařízení

Instalace senzoru, nebo jiného zařízení pro sběr dat je poměrně komplexní otázka vzhledem časté nutnosti jejich integrace do již hotových areálů a budov. Je nutné se potýkat s otázkami vhodného umístění zařízení, aby zařízení efektivně fungovalo, ale zároveň nenarušovalo architektonický design okolí. Lze také zařízení instalovat pouze provizorně povrchově bez větších zásahů a později během rekonstrukce zařízení přímo integrovat pro nejefektivnější použití.

Na obrázku 3 lze sledovat odlišnosti instalace IoT zařízení. Jedná se konkrétně o parkovací senzor. Zařízení na obrázku vlevo je plně integrováno do vozovky, taková instalace přináší vyšší náklady, avšak nabízí lepší estetický dojem. Zařízení vpravo je pouze přivrtáno na vozovku, taková instalace může být značně rychlejší, bez nutnosti větších omezení provozu a zároveň méně nákladná, taková instalace může být vhodná při dočasném použití.

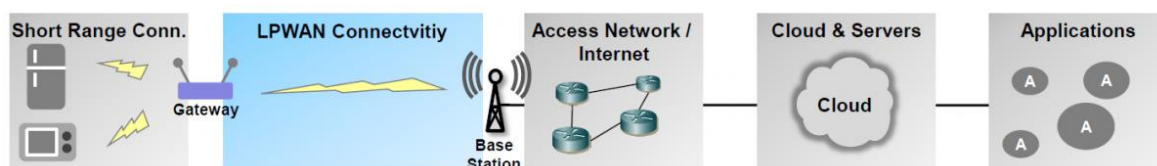
Obr. 3: Rozdíl instalace parkovacího senzoru. (33)



3.3 Sběr Dat

IoT zařízení sbírají obrovské množství dat, a tedy je potřeba data ukládat tak aby byli dobře přístupná a zabezpečená. Proto jsou data převážně ukládána na cloud, nebo vzdálený server. Cloud může ukládat ale i zpracovat data a následně je poskytnout aplikacím pro prezentaci dat. (37)

Obr. 4: Proces získávání, přenosu a zpracování dat (37)



Na obrázku 4 lze sledovat celý proces poskytování služeb IoT zařízení. Nejdříve dochází k prvotnímu sběru dat a jejich následného přesunu k bráně, která propojuje více zařízení v okolí. Následně jsou data přeneseny přes síť (v tomto případě LPWAN síť). LPWAN síť se přes síť internet připojí ke vzdálenému serveru (cloudu), který následně uloží/vyhodnotí posbíraná data a poskytne je k dalšímu použití pro koncové aplikace.

V oblasti IoT při sběru dat musí docházet k ochraně osobních údajů, na tuto ochranu se vztahuje přímo nařízení GDPR. V rámci ochrany osobních údajů musí být tedy úložiště dobře zabezpečené. (37)

3.3.1 Cloud Computing

Cloud Computing označuje model výpočetní techniky, kdy jsou zpoplatněné služby založené na informačních technologiích zpřístupněny uživatelům. Služby zahrnují softwarové aplikace, platformy pro vytváření aplikací, úložný prostor, nebo celou infrastrukturu hardwaru. Cloud Computing je efektivní cesta, jak zavádět nové technologie bez nutnosti velkých kapitálových výdajů za vytváření vlastní infrastruktury, proto firmy dnes místo vlastní serverové infrastruktury volí tuto cestu. Cloud Computing také přináší riziko, společnosti, které používají Cloud Computing nemají data pevně ve svých rukou, a tedy existují rizika odcizení citlivých dat. Existují tři podoby distribučních modelů: IaaS, PaaS a SaaS. (38)

IaaS (Infrastruktura jako služba) je poskytování infrastruktury, na které probíhá virtualizace serveru. Hlavní benefit této služby je, že se o veškeré problémy s hardwarem se stará

poskytovatel, není tedy potřeba řešit zastaralý, nebo opotřebovaný hardware. PaaS(Platforma jako služba) je poskytování kompletních prostředků pro podporu celého cyklu tvorby poskytování aplikací a služeb, bez nutnosti instalování softwaru a SaaS(Software jako služba) je poskytování přístupu k softwaru, kdy je software hostován provozovatelem. (37)

3.3.2 Konflikt sběru dat ve vztahu k GDPR

GDPR je soubor pravidel na ochranu dat klientů, zaměstnanců, dodavatelů, nebo zákazníků tedy fyzických osob. GDPR se týká všech firem, institucí, jednotlivců, ale i online služeb, které zpracovávají data uživatelů. GDPR také zavádí astronomické pokuty za porušování pravidel ochrany osobních údajů. Hlavním cílem GDPR je chránit digitální práva občanů EU. (39)

GDPR přináší velkou zátěž při zpracování dat, musí být dokumentováno, že jsou zpracována pouze ta data, která jsou ke konkrétnímu účelu nezbytná. Fyzické osoby mají také v rámci GDPR právo být důkladně informovány o zpracování jejich údajů a také právo vznést námitku proti zpracování, kvůli které správce musí data dané fyzické osoby přestat nadále zpracovávat a pokud si to fyzická osoba přeje tak je i smazat. Fyzická osoba má také právo si vyžádat svoje zpracovávaná data ve strukturovaném, strojově čitelném formátu. Správce dat má také povinnost informovat o úniku dat do 72 hodin od okamžiku, kdy se o incidentu dozvěděl, v některých případech má také povinnost kontaktovat přímo osobu a subjekty, kterých se únik týkal. (40)

Mezi osobní údaje patří jméno, pohlaví, věk, datum narození, osobní stav, IP adresa, fotografický záznam, ale také e-mailová adresa, telefonní číslo, nebo různé identifikační údaje vydané státem. Dále existují další kategorie jako etnický původ, politický názor, zdravotní stav, sexuální orientace a trestní delikty, kterých se fyzická osoba dopustila. Mezi zpracování osobních údajů patří také genetické a biometrické údaje. Naopak z působnosti GDPR jsou vyloučeny anonymizované údaje, tedy údaje o zemřelých osobách, nebo údaje získané v rámci čistě osobní povahy, které nemají obchodní charakter, také údaje, které jsou zpracovávány pro osobní potřebu a nejsou nijak sdíleny. Anonymizované údaje jsou taky taková data, která ani nepřímou nemohou identifikovat fyzickou osobu a nemohou být s ní nijak spojitelná (41)

IoT síť tedy při sběru dat musí buď data anonymizovat, a tedy se vyhnout právním souhlasům fyzických osob, anebo posbírat souhlasy od každé osoby, což může být komplexní problém, tyto souhlasy lze snadno posbírat například v areálech, kde vstup bude podmíněn právě souhlasem GDPR. Při sběru velkého množství dat bude, ale stále nutné vytvořit automatizované rozhraní, které fyzickým osobám poskytne jejich zpracované údaje a nabídne jim možnost žádosti o smazání a zastavení zpracování dat.

3.3.2.1 Anonymizace dat

Anonymizace je praktické řešení pro zachování soukromí uživatelů při zveřejňování dat. Mnoho institucí již dnes anonymizuje svá data, s cílem ochránit soukromí uživatelů a nedostat se tedy do právních komplikací. Anonymní údaje ale musí zůstat stále pro instituci užitečné. Existuje mnoho technik anonymizace. Platí, že čím více jsou data anonymizovaná, tím nižší mají vypovídající hodnotu. (42)

Odstranění přímo identifikovatelných dat

Na počátku anonymizace je potřeba z databáze dat odstranit veškeré informace, které mohou někoho přímo identifikovat, tedy jsou odstraněny data jako jméno, emailová adresa, mobilní číslo, nebo identifikační údaje vydané státem. Po odstranění citlivých informací je vhodné potlačit nulové hodnoty, tedy nenechávat prázdné sloupce po informacích. Potlačení nulové hodnoty je důležité, aby neexistoval žádný důkaz o tom, že daná hodnota byla vůbec někdy zaznamenána. (42)

Tab. 4: Příklad dat telefonické společnosti (upravený příklad podle zdroje (44))

Jméno	Příjmení	Telefon	Věk	Tarif	Měsíční cena za služby
Jan	Novák	711 102 566	16	Internet+	399
Jiří	Josef	601 505 111	25	Internet free	999
Jan	Pavel	723 008 001	56	Volej zdarma	220
Matyáš	Horník	805 555 684	55	Internet+	399

Tab. 5: Data po odstranění přímo identifikovatelných dat. (upravený příklad podle zdroje (44))

Věk	Tarif	Měsíční cena za služby
16	Internet+	399
25	Internet free	999
56	Volej zdarma	220
55	Internet+	399

Generalizace dat

Generalizace dat, tedy zobecnění dat spočívá v zjednodušení dat, tedy transformace dat na méně specifické, ale stále vypovídající informace. Například hodnota věku 25 let bude zobecněna pomocí intervalu $<25;30>$ nebo <30 . Jednotlivá informace může totiž stále vést k identifikaci osoby na základě dalších externích dat, jakmile ale má více jedinců stejnou hodnotu nelze už je na základě této informace jednoznačně identifikovat. (42)

Tab. 6: Data po generalizaci dat. (upravený příklad podle zdroje (44))

Věk	Tarif	Měsíční cena za služby
20>	Internet+	399
(20;30)	Internet free	999
>50	Volej zdarma	220
>50	Internet+	399

Permutace dat

Při permutaci dat se záznamy rozdělí do několika skupin, kdy jsou data v každé skupině promíchány. Tato metoda vede k odstranění vazeb mezi jednotlivými sloupci a tím může soubor dat vést k nepřesné analýze. (42)

Tab. 7: Přehled dat po provedení permutace věku (upravený příklad podle zdroje (44))

Věk	Tarif	Měsíční cena za služby
25	Internet+	399
56	Internet free	999
55	Volej zdarma	220
16	Internet+	399

Přidání šumu k datům

Přidání šumu k datům znamená upravit data tak, aby se odchýlili od původních hodnot, ale stále byli relevantní. K původním datům se tedy přičte nová náhodná hodnota, která původní hodnotu změní tak, aby nemohla identifikovat osobu, ale aby stále hodnota byla vypovídající.

Tab. 8: Data s vygenerovanou hodnotou šumu, která neovlivní použitelnost dat (upravený příklad podle zdroje (44))

Věk	Tarif	Měsíční cena za služby	Náhodně vygenerovaná hodnota od 20 do 99 kč
16	Internet+	399	35
25	Internet free	999	41
56	Volej zdarma	220	24
55	Internet+	399	98

Tab. 9: Data s již přidaným šumem. (upravený příklad podle zdroje (44))

Věk	Tarif	Cena po přidání šumu
16	Internet+	434
25	Internet free	1040
56	Volej zdarma	244
55	Internet+	497

3.3.2.2 Pseudonymizace dat

Zatímco anonymizace dat je nevratný proces bez možnosti identifikace osoby, pseudonymizace data anonymizuje metodou takovou že lze data opět vrátit do původní podoby. Pseudonymizace není metodou anonymizace, a tedy se na ní stále vztahuje GDPR, ale může být dobrým způsobem zabezpečení dat, nebo metodou sdílení pouze část dat s různými aplikacemi.

Citlivá data jsou nahrazena identifikátorem, který odkazuje na jiný soubor dat, který je uložen na bezpečnějším místě a měl by být dobře zabezpečen. Existuje více metod pseudonymizace: tokenizace, maskování nebo zašifrování dat. (43)

Tokenizace dat

Tokenizace používá nezávislý algoritmus pro generování tokenů a přiřazuje je záznamům. Tokeny mohou být například náhodně generovaná čísla.

Tab. 10: Příklad z tabulky 5 po pseudonymizaci tokenem (upravený příklad podle zdroje (44))

Token	Věk	Tarif	Měsíční cena za služby
72197	16	Internet+	399
49477	25	Internet free	999
41301	56	Volej zdarma	220
46411	55	Internet+	399

Tab. 11: Klíč k tabulce 10 (upravený příklad podle zdroje (44))

Token	Jméno	Příjmení	Telefon
72197	Jan	Novák	711 102 566
49477	Jiří	Josef	601 505 111
41301	Jan	Pavel	723 008 001
46411	Matyáš	Horník	805 555 684

Maskovaná a zašifrovaná citlivá data

Maskování dat nahrazuje staré hodnoty citlivých atributů náhodnými hodnotami tak aby zachovala formát a sémantiku hodnot. Taková data jsou tedy nepoznatelná od původních dat, ale neidentifikují žádnou fyzickou osobu. Původní data jsou ale stále bezpečně uloženy pro potenciální pozdější použití. Pseudonymy lze také vytvořit pomocí šifrování identifikačních údajů pomocí tajného klíče. Je tedy důležité si šifrovací klíč bezpečně uložit. Šifrování dat pomocí tajného klíče je nejbezpečnější způsob pseudonymizace. (44)

4. Vlastní práce

V této části práce je provedena analýza vhodných IoT řešení vzhledem k užití v dané lokalitě, tedy analýza bezdrátových sítí a koncového zařízení pro sběr dat. Dále je provedeno pilotní ověření ve vybrané lokalitě Lázeňské lesy Karlovy Vary, kde cílem instalací IoT systémů je zajistit alternativní způsoby, jak získávat informace o počtu návštěvníků. Je provedena analýza konfliktů v oblasti sběru dat ve vztahu k GDPR, včetně analýzy posbíraných dat a jejich vyhodnocení s ohledem na charakter technologie sběru dat.

4.1 Analýza IoT řešení

Pro každý vznikající IoT projekt je potřeba důkladně zhodnotit jednotlivé požadované parametry pro správný chod systému v souladu s umístěním zařízení. Při tvorbě IoT systému, je vhodné již na začátku zvolit nejoptimálnější technologii ať už z hlediska konektivity, či zdrojů napájení.

4.1.1 Analýza konektivity

Vhodné řešení konektivity určuje převážně umístění zařízení potažmo ke vztahu k financím. Vzhledem k tomu, že lze využívat LPWAN, Wi-Fi, WPAN, či mobilní sítě v rámci tvorby IoT systému, je vhodné analyzovat jednotlivé sítě na základě SWOT tabulky. Každá níže analyzovaná technologie má svoje využití v daném odvětví. A je tedy nutné při vývoji IoT zařízení definovat nároky a požadavky na síť. Síť lze také kombinovat v rámci jedné velké IoT infrastruktury. Je nutné sledovat kromě silných stránek sítě i stránky slabé, zejména u sítí, kde je nutná funkce operátora (tedy potřeby třetí strany).

4.1.1.1 LPWAN síť

Tab. 12: SWOT Analýza LPWAN sítí

Silné stránky (S)	Slabé stránky (W)
Nízká spotřeba energie	Malá šířka pásma
Připojení velkého množství zařízení	Potřeba operátora
Nízké pořizovací náklady	Častá závislost na nevlastní infrastruktuře
Vysoký průnik signálu zdi a suterény budov	Vhodné pouze pro zařízení, které odesílají malé množství dat
Příležitosti (O)	Ohrožení (T)
Vznik nových IoT zařízení díky vlastnostem LPWAN sítí	Zánik společnosti, která vyvíjí síť, následující postupný úpadek sítě.
Možnosti propojit miliardy IoT zařízení	Riziko zdražení služeb operátora

Na základě vyhotovení SWOT tabulky (tabulka 12) pro LPWAN síť, lze vyhodnotit, že užití takové sítě je vhodné zejména pro zařízení, které odesílají malé množství dat a zároveň nevyžadují velkou spotřebu energie. Na základě použití této sítě lze totiž sestavovat taková zařízení, která budou schopna fungovat dlouhodobě na základě vlastního omezeného zdroje elektrické energie. Tyto sítě mohou být závislé na existenci operátora, který své služby má zpoplatněné, je tedy nutné počítat s možností zdražení služeb, a tedy zvýšení nákladů na provoz takové IoT infrastruktury. Existuje také riziko zániku společnosti, která síť vytvořila, nebo vyvíjí, tak jak se tomu stalo u společnosti SigFox, tedy je riziko, že při neexistující společnosti, která by síť dále vyvíjela by mohlo dojít k nalezení bezpečnostních nedostatků a postupnému zániku sítě, což by neslo další náklady při migraci IoT systému na síť jinou. Na druhou stranu, toto riziko nesou skoro všechny uzavřené sítě, které nejsou open source, a tedy toto riziko by nemělo být tak zásadním faktorem při volbě sítě. Tedy závěrem lze analýzu shrnout tak, že LPWAN sítě jsou vhodné pro nenáročná zařízení, která mohou pracovat na základě svého vlastního malého zdroje energie, převážně pro sběr okolních dat k jejich následnému zpracování na vzdáleném serveru. Tyto sítě jsou také vhodné pro provoz mobilních zařízení pro krátkodobý lokální sběr dat, vzhledem k dobré propustnosti skrze zastavěné oblasti (zdi), lze zařízení

komunikující na základě LPWAN sítí přemísťovat bez zvýšeného rizika špatného až žádného signálu v bodě umístění.

4.1.1.2 Mobilní síť

Tab. 13: SWOT Analýza Mobilních sítí

Silné stránky (S)	Slabé stránky (W)
Velmi velká šířka pásma	Vyšší spotřeba energie
Velmi dobré pokrytí v ČR	Nutnost platit operátorovi za služby
Nízké pořizovací náklady	Vyšší poplatky operátorovi
Vhodné pro přenos streamu videí	Špatný průnik signálu přes zdi a suterény budov
Příležitosti (O)	Ohrožení (T)
Zefektivnění služeb díky velkému množství přenesených dat	Riziko zdražení služeb operátora
Zlepšování infrastruktury a datových propustností na základě snahy operátora poskytnout lidem co nejlepší internetové služby	Přetížení sítě v obydlených oblastech, riziko kolísání datové propustnosti a latence v síti

V rámci analýzy mobilních sítí v tabulce 13 lze určit závěry, že užití mobilních sítí může být vhodné pro provoz jednoho až nízkého vyššího počtu zařízení, vzhledem k nákladnosti této služby by využívání této sítě pro provoz tisíců zařízení pro sběr dat mohlo být příliš nákladné. Mobilní síť nabízí obrovskou datovou propustnost a poměrně nízkou přenosovou latenci v porovnání s ostatními sítěmi, tudíž jejich použití je vhodné pro přenosy velkého množství dat (Například přenosu videozáznamů z kamer). Vzhledem k tomu, že tyto sítě nejsou primárně určeny pro IOT systémy, lze sledovat příležitost jejich dalšímu rozvoji nezávisle na tom, jestli IoT sítě budou nadále hojně využívány, tedy lze pozorovat nižší riziko zániku těchto sítí na základě neuchycení na trhu. Tyto sítě je vhodné provozovat na zařízeních u kterých bude předpoklad umístění mimo budovy, tedy na venkovních prostředí vzhledem k jejich špatné propustnosti skrze zdi. Dále je nutno při provozu těchto sítí předpokládat vyšší spotřebu energie, tudíž je zařízení provozující tyto sítě vhodno opatřit větším zdrojem energie, popřípadě možností dobíjení akumulátoru na základě dostupných

okolních zdrojů (teplo, světlo, vítr), ideálně připojit zařízení do elektrické sítě. Na základě této analýzy lze určit, že užití mobilních sítí je vhodné pro IoT systémy, u kterých je potřeba velká datová propustnost a je předpoklad, že budou užity ve venkovním prostředí.

4.1.1.3 LAN síť

Tab. 14: SWOT Analýza LAN sítí

Silné stránky (S)	Slabé stránky (W)
Velmi vysoká šířka pásma sítě	Vysoké náklady na vznik infrastruktury sítě
Zabezpečení	Vysoké náklady na změnu infrastruktury sítě
Stabilní připojení	Rozsah omezen pouze na oblasti budov a areály
Žádné poplatky za provoz sítě – Neexistence operátora (třetí strany)	
Příležitosti (O)	Ohrožení (T)
Zlepšení dostupnosti internetu v rámci stavby IoT infrastruktury.	Zvýšení ceny metalických vodičů

Dle vyhotovené SWOT analýzy v tabulce 14 lze určit závěry, že užití LAN sítí při tvorbě IoT systému může být vhodné tehdy pokud LAN síť v dané budově, či areálu již existuje anebo pokud se bude zároveň paralelně využívat pro běžné potřeby přístupu k síti. Vzhledem k vyšší nákladnosti k sestavení této sítě oproti ostatním možným druhům konektivity v IoT, není vhodné navrhovat LAN síť pro malá IoT zařízení pro sběr běžných dat. LAN síť lze určit jako nejbezpečnější oproti ostatním analyzovaným sítím za předpokladu, že bude celá LAN síť vyhotovena z fyzických vodičů. Potenciální útočník by musel mít fyzický přístup k vodičům, aby mohlo dojít k úniku dat. Protože v rámci této sítě není potřeba žádného operátora, tedy třetí strany, je tato síť více důvěryhodná z hlediska bezpečnosti a zároveň nepřináší žádné budoucí poplatky za provoz této sítě. Na základě této analýzy lze definovat závěr, že LAN sítě jsou vhodné pro takové IoT zařízení, které potřebují stabilní a velmi velkou datovou propustnost, nebo pro zařízení, která sbírají citlivá data a bylo by nežádoucí riskovat jejich únik.

4.1.1.4 WPAN síť

Tab. 15: SWOT Analýza WPAN sítí

Silné stránky (S)	Slabé stránky (W)
Podpora chytrých telefonů	Malá šířka pásma
Snadné propojení zařízení	Malý rozsah sítě
Možnost používání i pasivních zařízení	Použití pouze pro specifické zařízení
Zlepšení efektivity služeb podniků	Schopnost uživatelů využívat tyto sítě
Příležitosti (O)	Ohrožení (T)
Vznik specifických IoT zařízení, které pomůžou regionálnímu rozvoji	Konec podpory mobilních zařízení(NFC, Bluetooth)
Funkce WPAN sítí mohou zvýšit obecné povědomí o IoT sítích	

Podle analýzy ve SWOT tabulce 15 lze určit závěry, že užití WPAN sítí je vhodné pro zařízení, která mohou poskytovat přístup a data chytrým telefonům uživatelů, případně propojovat nechytrá zařízení s IoT systémem. U WPAN sítí nelze provozovat přenos dat mezi IoT systémy na velké vzdálenosti, tudíž jejich užití bude převážně přenos a poskytování dat koncovým zařízeními. WPAN sítě jsou vhodné zejména k přenosu informací, reklamních akcí nebo ovládání různých zařízení. Silnou stránkou WPAN sítí může být zlepšení efektivity provozu velkých areálů ve veřejném ale i soukromém sektoru, zejména v oblasti přesunu lidí, či výroby a skladování produktů a zboží, zejména díky schopnostem navigace ale i kompatibility s většinou chytrých telefonů. WPAN sítě jsou vhodné také pro užití v domácnosti, při komunikaci s nechytrými zařízeními, při ovládání světel, nebo automatizaci teploty dle přítomnosti uživatele. Silnou stránkou těchto sítí je snadné propojení zařízení, kdy není mnohdy nutné stahovat speciální programy a aplikace, ale pouze využít již aplikovaný software výrobcem zařízení, propojení v rámci této sítě je rychlé, což přináší výhody zejména při užití LPWAN sítí během placení. Užití LPWAN sítí ovšem spoléhá se součinností uživatelů, což je slabá stránka těchto sítí, zejména kvůli nedostatečným schopnostem uživatelů tyto sítě užívat, tedy je nutno stále paralelně využívat i jiné toky poskytování informací, zejména při navigaci, či poskytování reklamních akcí a plateb.

4.2 Pilotní ověření ve vybrané lokalitě

V této kapitole je analyzována instalace IoT systému v lokalitě Lázeňské lesy Karlovy Vary. Cílem je analýza použitých technologií na základě porovnání naměřených výsledků pomocí vybraných technologií. Dále bude analyzován postup sběru dat a systém jejich zpracování. Na základě těchto analýz jsou definovány závěry pilotního ověření.

4.2.1 Použité technologie a jejich analýza

Jelikož je IoT systém nainstalován a již poskytuje data pro zpracování, tak v této podkapitole bude zhodnocena vhodnost použití hardware a technologie pro přenos dat.

4.2.1.1 Popis IoT hardwaru

Při instalaci IoT systému v lokalitě Lázeňské lesy Karlovy Vary byli použity konkrétně 3 zařízení AgroNode. AgroNode jsou zařízení pro záznam dat, které jsou určeny pro použití v zemědělství, jsou vybaveny akumulátorem a solárním panelem, které zařízení dobíjí. Zařízení nabízí rozhraní pro připojení senzorů pro sběr dat. Zařízení AgroNode tedy zastává funkci brány v rámci procesu sbírání jejich dat a jejich následného použití, konkrétně se stará o napájení senzoru a přenosu dat ze senzoru do svých pamětí a následného odeslání dat při procesu odeslání dat v rámci sítě. Zařízení je vybaveno modulem SigFox a přes tuto síť přenáší posbíraná data na datový server.

Každé zařízení měří jiné veličiny pomocí senzorů a to konkrétně:

- Teplotu a vlhkost
- Rychlost proudění a směr proudění větru
- Sluneční svit

Teplota a vlhkost je měřena pomocí senzoru Decagon VP-4, tento senzor sleduje teplotu vzduchu, relativní vlhkost, barometrický tlak a tlak páry. Senzor je propojen se zařízením AgroNode pomocí portu SDI12. Aby senzor VP-4 nemohl být ovlivněn slunečním zářením a následně poskytovat chybné údaje o naměřených teplotách je vybaven radiačním štítem. Radiační štít ochraňuje čidlo před zdrojem tepla a deště, ale zároveň umožňuje proudění vzduchu.

Rychlost proudění a směr větru měří ultrazvukový anemometr Atmos 22. Tento anemometr nemá žádné pohyblivé části, a tudíž nemůže dojít k riziku opotřebení nebo k jinému

mechanickému poškození zařízení. Zařízení rovněž komunikuje s centrální jednotkou AgroNode pomocí SDI-12.

Dobu trvání slunečního svitu měří snímač SD9 MPS. Tento senzor komunikuje s jednotkou AgroNode pomocí portu RS485. Senzor je vybaven vyhříváním pro eliminaci námrazy během chladnějších období, je tedy schopno pracovat během provozních podmínek od -50°C do +85°C.

4.2.1.2 Analýza IoT hardware

Na základě analýzy zařízení AgroNode lze konstatovat, že nabízí kompletní řešení problematiky sbírání dat a jejich přenosu při použití v oblasti Lázeňských lesů v Karlových Varech. Zařízení je modulární, nabízí možnosti konektivity přes GSM, LoRa, SigFox IQRF a NB-IoT sítě, tedy zařízení snižuje možná rizika spojené s náklady na změnu použité sítě pro přenos dat. Na základě analýzy LPWAN sítí z tabulky 12 je patrné že může dojít k zániku sítě, či k zvýšení poplatků operátora, zařízení tedy nabízí možnost změnit druh sítě na základě změny modulu, a tedy není nutné měnit celé zařízení jako takové. AgroNode také disponuje 4 kompatibilními vstupními porty které jsou fyzicky umístěny na dvou fyzických svorkovnicích, jedná se konkrétně o sběrnice SDI12, 1WIRE, RS485, I2C. Konkrétní použitá sběrnice se volí připojením svorkovnice na správné místo, lze tedy současně sbírat data ze 2 různých čidel, to nabízí větší volnost při nákupu senzorů, a tedy možné snížení vstupních nákladů na základě lepší nabídky na trhu.

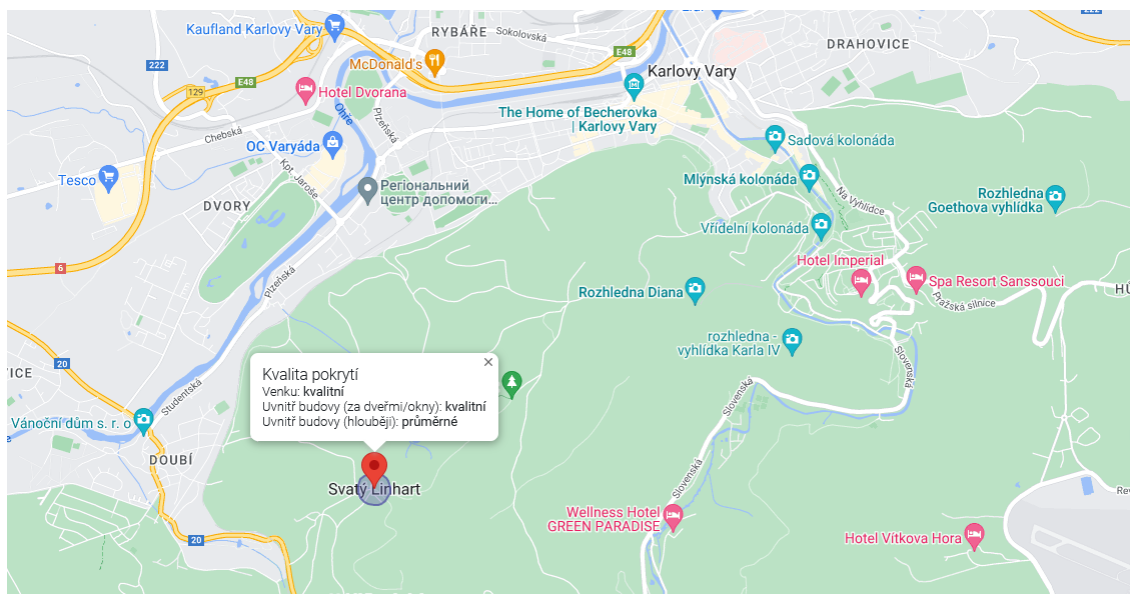
4.2.1.3 Konektivita v oblasti Lázeňských lesů

Na základě analýzy pokrytí v této oblasti budou dosažené závěry formulovány do tabulky 16.

Tab. 16: Porovnání pokrytí konektivity v oblasti Lázeňských lesů v Karlových Varech

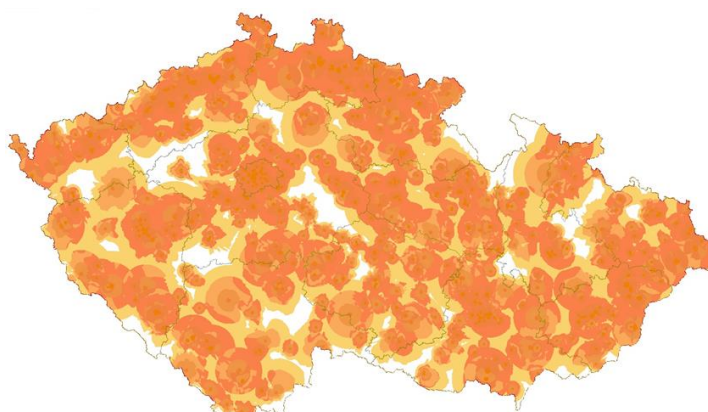
Druh připojení	SigFox	LoRaWan	NB-IoT
Pokrytí venku	Kvalitní	Mělo by být	Kvalitní
Pokrytí uvnitř budovy	Kvalitní / Průměrné	Mělo by být	Kvalitní
Klíčové vlastnosti	Frekvence intervalů odesílání jednou za 10 minut	Obousměrná komunikace	Rychlost až 27 kbit/s, vyšší spotřeba energie.

Obr. 5: Pokrytí sítě SigFox v oblasti Lázeňských lesů v Karlových Varech (screenshot z webu <https://coverage.sigfox.cz/>)

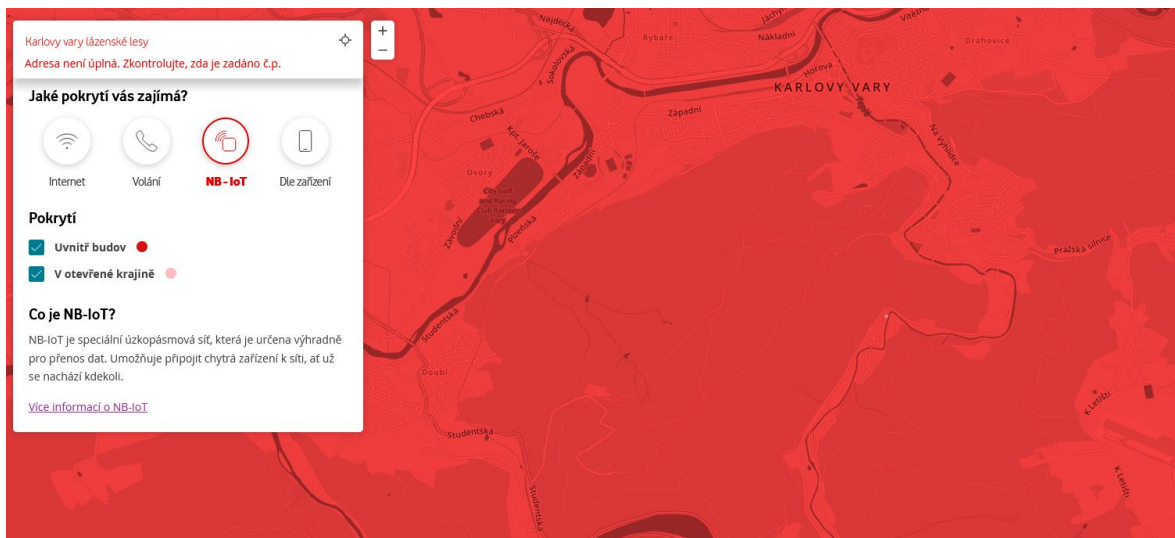


Dle provedené analýzy jsou porovnávány sítě z tabulky 16, které podporuje zařízení AgroNode v oblasti Lázeňských lesů v Karlových Varech dostupné. U Sítě LoRaWAN nelze konstatovat jednoznačně pokrytí v dané oblasti, na základě nedostupnosti podrobné mapy pokrytí. České telekomunikace poskytují pouze obecnou mapu pokrytí, kde je patrné, že Karlovy vary pokryté jsou, avšak mohlo by docházet k „hluchým“ místům, tedy místům, kde by pokrytí nebylo žádné a IoT zařízení by muselo být umístěno s ohledem na kvalitu připojení. Tedy by bylo nutné primárně určovat umístění zařízení na základě připojení, nikoliv na základě vhodnosti umístění z hlediska optimálního měření senzorů, či estetického dojmu. Tudíž použití sítě LoRaWAN by bylo nevhodné, pokud by nedošlo k hlubší analýze prostředí na základě proměření kvality signálu, či konzultace s operátorem.

Obr. 6: Mapa pokrytí sítě LoRaWAN v České republice (Vlastní screenshot z webu(11))



Obr. 7: Pokrytí sítě SigFox v oblasti Lázeňských lesů v Karlových Varech (screenshot z webu <https://www.vodafone.cz/mapa-pokryti/>)



Na základě vlastností zvolených sítí pro analýzu v oblasti Lázeňských lesů v Karlových Varech lze určit závěr, že zvolená síť SigFox se může na základě analýzy dle tabulky 16 jevit jako optimální. Ačkoliv síť SigFox nabízí interval spojení pouze v průměrném rozmezí jednou za 10 minut, v tomto případě tato vlastnost nijak nebude vadit při měření dat. Vzhledem k tomu, že zařízení AgroNode si nasbírané informace uchová po celou dobu, než dojde k odeslání dat, tak o žádné „výpadky“ v datech nebude docházet, zároveň lze konstatovat, že pro nakládání s daty v tomto případě není nutné mít živá data ohledně návštěvnosti. NB-IoT síť by se mohla jevit jako vhodná, ale vzhledem k tomu, že zařízení běží na vlastní zdroj energie, je vhodné cílit k co nejnížší spotřebě.

4.2.2 Sběr dat

Data ze zařízení AgroNode přicházejí na datový server v podobě, která je znázorněna na obrázku 8. Tedy jsou evidovány hodnoty jako konec času změření a začátek změření dané hodnoty, dále se evidují hodnoty mac adresy zachyceného zařízení, na které se může vztahovat GDPR a adresa mac adresy vlastního zařízení, které tuto hodnotu změřilo, na vlastní zařízení se pochopitelně GDPR nevztahuje.

Obr. 8: Ukázka nezpracovaných dat se znehodnocením identifikovatelných dat ke vztahu k GDPR (vlastní screenshot z poskytnutých dat)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	time,"networkid","ipv4","ssid","os","clientMac","latestTime","latestNearestApMac","latestNearestApRssi","ipv6","manufacturer"													
2	2022-10-05 20:25:17,N_620933798623719864,null,null,null,38									2022-10-05 20:25:17,8:f8:9e:28:ff:f8:66,-85,null,INGENICO	TERMINALS	SAS		
3	2022-10-05 20:26:05,N_620933798623719864,null,null,null,e8									2022-10-05 20:26:05,f8:9e:28:ff:f8:66,-91,null,Intel				
4	2022-10-05 20:28:20,N_620933798623719864,null,null,null,e8									2022-10-05 20:28:20,f8:9e:28:ff:f8:66,-91,null,Intel				
5	2022-10-05 20:29:49,N_620933798623719864,null,null,null,e8									2022-10-05 20:29:49,f8:9e:28:ff:f8:66,-92,null,Intel				
6	2022-10-05 20:29:49,N_620933798623719864,null,null,null,38									2022-10-05 20:29:49,f8:9e:28:ff:f8:66,-85,null,INGENICO	TERMINALS	SAS		
7	2022-10-05 20:32:05,N_620933798623719864,null,null,null,e8									2022-10-05 20:32:05,f8:9e:28:ff:f8:66,-92,null,Intel				
8	2022-10-05 20:34:22,N_620933798623719864,null,null,null,e8									2022-10-05 20:34:22,f8:9e:28:ff:f8:66,-86,null,Intel				
9	2022-10-05 20:35:57,N_620933798623719864,null,null,null,e8									2022-10-05 20:35:57,f8:9e:28:ff:f8:66,-90,null,Intel				
10	2022-10-05 20:35:57,N_620933798623719864,null,null,null,38									2022-10-05 20:35:57,f8:9e:28:ff:f8:66,-81,null,INGENICO	TERMINALS	SAS		
11	2022-10-05 20:37:25,N_620933798623719864,null,null,null,38									2022-10-05 20:37:25,f8:9e:28:ff:f8:66,-85,null,INGENICO	TERMINALS	SAS		
12	2022-10-05 20:38:07,N_620933798623719864,null,null,null,e8									2022-10-05 20:38:07,f8:9e:28:ff:f8:66,-90,null,Intel				
13	2022-10-05 20:40:15,N_620933798623719864,null,null,null,e8									2022-10-05 20:40:15,f8:9e:28:ff:f8:66,-90,null,Intel				
14	2022-10-05 20:42:20,N_620933798623719864,null,null,null,e8									2022-10-05 20:42:20,f8:9e:28:ff:f8:66,-91,null,Intel				
15	2022-10-05 20:42:20,N_620933798623719864,null,null,null,38									2022-10-05 20:42:20,f8:9e:28:ff:f8:66,-86,null,INGENICO	TERMINALS	SAS		
16	2022-10-05 20:44:31,N_620933798623719864,null,null,null,e8									2022-10-05 20:44:31,f8:9e:28:ff:f8:66,-90,null,Intel				
17	2022-10-05 20:47:29,N_620933798623719864,null,null,null,38									2022-10-05 20:47:29,f8:9e:28:ff:f8:66,-85,null,INGENICO	TERMINALS	SAS		
18	2022-10-05 20:48:14,N_620933798623719864,null,null,null,e8									2022-10-05 20:48:14,f8:9e:28:ff:f8:66,-91,null,Intel				
19	2022-10-05 20:49:47,N_620933798623719864,null,null,null,e8									2022-10-05 20:49:47,f8:9e:28:ff:f8:66,-86,null,Intel				
20	2022-10-05 20:51:02,N_620933798623719864,null,null,null,38									2022-10-05 20:51:02,f8:9e:28:ff:f8:66,-80,null,INGENICO	TERMINALS	SAS		
21	2022-10-05 20:51:54,N_620933798623719864,null,null,null,e8									2022-10-05 20:51:54,f8:9e:28:ff:f8:66,-91,null,Intel				
22	2022-10-05 20:53:10,N_620933798623719864,null,null,null,38									2022-10-05 20:53:10,f8:9e:28:ff:f8:66,-88,null,INGENICO	TERMINALS	SAS		
23	2022-10-05 20:54:05,N_620933798623719864,null,null,null,e8									2022-10-05 20:54:05,f8:9e:28:ff:f8:66,-86,null,Intel				
24	2022-10-05 20:57:04,N_620933798623719864,null,null,null,38									2022-10-05 20:57:04,f8:9e:28:ff:f8:66,-86,null,INGENICO	TERMINALS	SAS		
25	2022-10-05 21:00:11,N_620933798623719864,null,null,null,e8									2022-10-05 21:00:11,f8:9e:28:ff:f8:66,-92,null,Intel				
26	2022-10-05 21:02:32,N_620933798623719864,null,null,null,38									2022-10-05 21:02:32,f8:9e:28:ff:f8:66,-86,null,INGENICO	TERMINALS	SAS		
27	2022-10-05 21:03:12,N_620933798623719864,null,null,null,38									2022-10-05 21:03:12,f8:9e:28:ff:f8:66,-86,null,INGENICO	TERMINALS	SAS		
28	2022-10-05 21:04:39,N_620933798623719864,null,null,null,e8									2022-10-05 21:04:39,f8:9e:28:ff:f8:66,-92,null,Intel				
29	2022-10-05 21:06:32,N_620933798623719864,null,null,null,38									2022-10-05 21:06:32,f8:9e:28:ff:f8:66,-86,null,INGENICO	TERMINALS	SAS		
30	2022-10-05 21:06:48,N_620933798623719864,null,null,null,e8									2022-10-05 21:06:48,f8:9e:28:ff:f8:66,-91,null,Intel				
31	2022-10-05 21:07:31,N_620933798623719864,null,null,null,38									2022-10-05 21:07:31,f8:9e:28:ff:f8:66,-82,null,INGENICO	TERMINALS	SAS		
32	2022-10-05 21:08:56,N_620933798623719864,null,null,null,e8									2022-10-05 21:08:56,f8:9e:28:ff:f8:66,-90,null,Intel				
33	2022-10-05 21:10:21,N_620933798623719864,null,null,null,e8									2022-10-05 21:10:21,f8:9e:28:ff:f8:66,-91,null,Intel				
34	2022-10-05 21:11:53,N_620933798623719864,null,null,null,e8									2022-10-05 21:11:53,f8:9e:28:ff:f8:66,-92,null,Intel				
35	2022-10-05 21:12:41,N_620933798623719864,null,null,null,38									2022-10-05 21:12:41,f8:9e:28:ff:f8:66,-85,null,INGENICO	TERMINALS	SAS		
36	2022-10-05 21:13:01,N_620933798623719864,null,null,null,38									2022-10-05 21:13:01,f8:9e:28:ff:f8:66,-88,null,INGENICO	TERMINALS	SAS		
37	2022-10-05 21:14:12,N_620933798623719864,null,null,null,e8									2022-10-05 21:14:12,f8:9e:28:ff:f8:66,-91,null,Intel				
38	2022-10-05 21:17:07,N_620933798623719864,null,null,null,38									2022-10-05 21:17:07,f8:9e:28:ff:f8:66,-85,null,INGENICO	TERMINALS	SAS		
39	2022-10-05 21:18:34,N_620933798623719864,null,null,null,e8									2022-10-05 21:18:34,f8:9e:28:ff:f8:66,-91,null,Intel				
40	2022-10-05 21:19:33,N_620933798623719864,null,null,null,38									2022-10-05 21:19:33,f8:9e:28:ff:f8:66,-88,null,INGENICO	TERMINALS	SAS		
41	2022-10-05 21:22:11,N_620933798623719864,null,null,null,50									2022-10-05 21:22:11,f8:9e:28:ff:f8:66,-89,null,HP				
42	2022-10-05 21:22:11,N_620933798623719864,null,null,null,e8									2022-10-05 21:22:11,f8:9e:28:ff:f8:66,-91,null,Intel				
43	2022-10-05 21:22:56,N_620933798623719864,null,null,null,38									2022-10-05 21:22:56,f8:9e:28:ff:f8:66,-85,null,INGENICO	TERMINALS	SAS		
44	2022-10-05 21:23:52,N_620933798623719864,null,null,null,38									2022-10-05 21:23:52,f8:9e:28:ff:f8:66,-89,null,INGENICO	TERMINALS	SAS		
45	2022-10-05 21:24:33,N_620933798623719864,null,null,null,e8									2022-10-05 21:24:33,f8:9e:28:ff:f8:66,-91,null,Intel				
46	2022-10-05 21:25:54,N_620933798623719864,null,null,null,e8									2022-10-05 21:25:54,f8:9e:28:ff:f8:66,-92,null,Intel				

4.2.2.1 Pseudonymizace MAC adresy

MAC adresa nemusí být nutně zatížena zákonem o GDPR, pokud přímo neukazuje na subjekt v kombinaci s ostatními informacemi. MAC adresa je zatížena zákonem o GDPR v případě, pokud jsou evidovány data, která by pomohla určit vlastníka zařízení, například přihlašovací údaje, včetně kontaktu uživatele. MAC adresa jako taková pouze jednoznačně odlišuje unikátnost jednotlivých zařízení, což je nutné pro pozdější zpracování o přesném počtu návštěvníků, včetně jejich četnosti návštěv. Je ale vhodné stejně MAC adresu v databázi upravit tak, aby její podoba stále umožňovala identifikovat unikátní zařízení, ale aby nebylo možné zpětně přes tuto hodnotu identifikovat zařízení.

Na základě poskytnutých dat, která byla posbírána pomocí IoT systému v lokalitě Lázeňské lesy Karlovy Vary, bylo navrženo v rámci praktické části bakalářské práce uložená data o MAC adrese cizích zařízení pseudonymizovat pomocí kryptografických hashovacích funkcí, například pomocí funkce SHA-1.

Tab. 17: Pseudonymizace MAC adresy pomocí hashovací funkce SHA-1

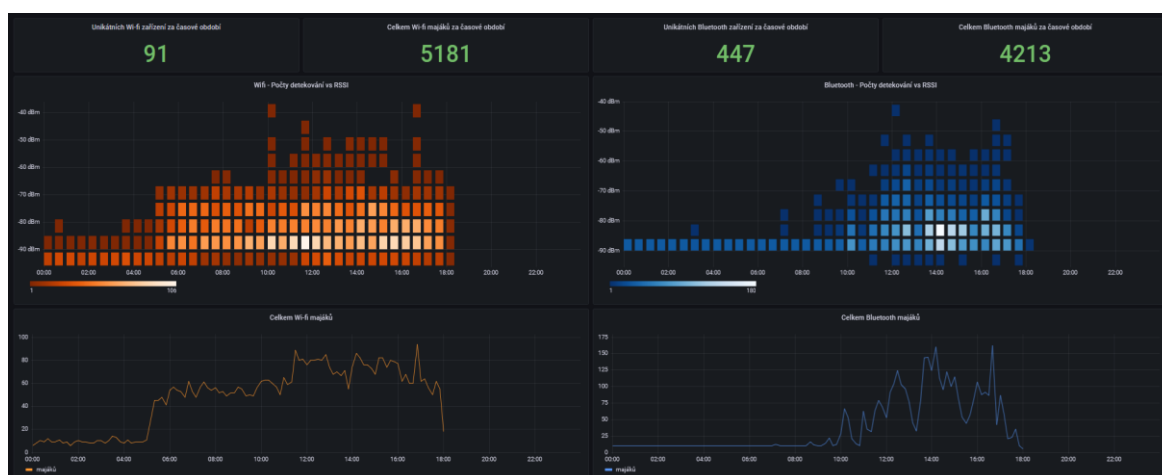
MAC adresa v originální podobě	MAC adresa v pseudonymizované podobě
2E:DA:C9:A9:F5:76	aeaa1250c26f1dce95d3572039f23875a6985c3e
22:CA:54:51:24:30	c2e42d34abb1e2dcaed90c7b0ad579d14e850f20
0E:F8:AF:70:2B:44	7b84396147d3424adf1b99d8c94b6ae01a2a1200
72:CE:A5:E9:0E:37	43353d9f971b2bd86db966cb1cff5e7a567d5f57

V tabulce 17 lze sledovat stále unikátnost pseudonymizovaných MAC adres, ovšem po jejich zašifrování tyto data nemohou identifikovat zařízení uživatele. Potenciální útočník by mohl data sice rozšifrovat, například pomocí použití takzvané hrubé síly anebo „rainbow tables“ tedy tabulky s hodnotami, které již někdo zašifroval. Ovšem k existenci až 281 bilionů různých MAC adres bude snaha takové data rozšifrovat poměrně složitá.

4.2.3 Zpracování dat přes rozhraní Grafana

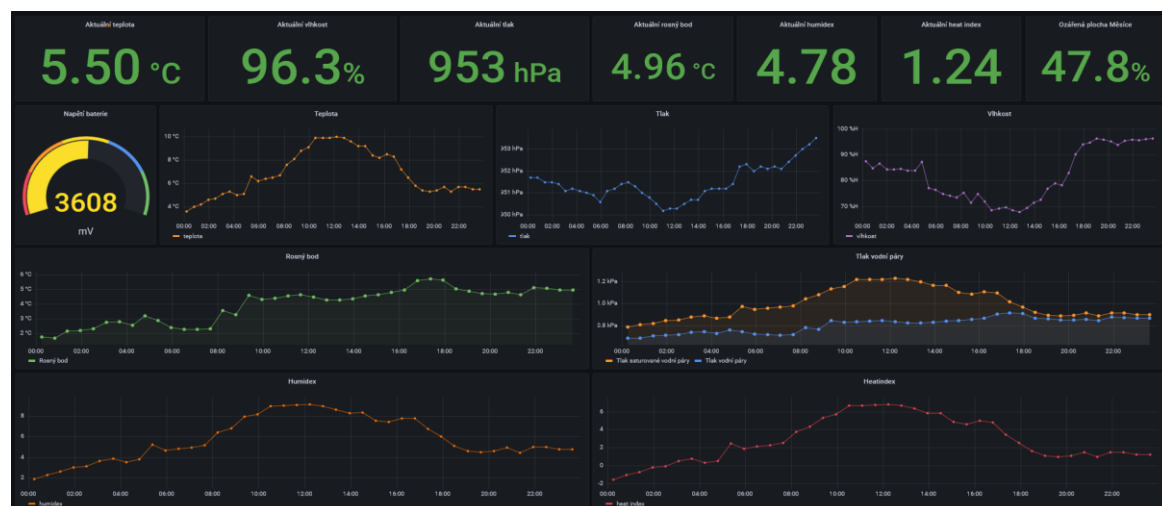
Data, která jsou sbírána IoT systémem v oblasti Lázeňských lesů v Karlových Varech jsou zpracovávána a zobrazována pomocí softwaru Grafana.

Obr. 9: Snímek obrazovky, sledovaných dat za uplynulých 24 hodin z data 29.12.2022 00:00:00 až 29.12.2022 23:59:59. (Screenshot z rozhraní Grafana na základě poskytnutého přístupu).



Na obrázku č.9 lze sledovat sledování počtu zařízení na základě dvou technologií, technologie Bluetooth a technologie Wi-Fi. Na grafech výše lze sledovat četnost návštěv v časovém rozmezí v závislosti na RSSI, tedy na hodnocení kvality příjmu signálu. Na grafech níže se sleduje počet zaznamenaných zařízení, ovšem dochází k zaznamenávání stejných zařízení během každého měření, které probíhá, tudíž grafy znázorňují pouze celkový počet zaznamenaných zařízení v daném časovém rozmezí bez ohledu na jejich duplicitu.

Obr. 10: Snímek obrazovky, sledovaných dat za uplynulých 24 hodin z data 29.12.2022 00:00:00 až 29.12.2022 23:59:59. (Screenshot z rozhraní Grafana).



Na obrázku č.10 lze sledovat naměřené hodnoty, které se týkají počasí v oblasti lázeňských lesů. Na základě tohoto měření lze sledovat četnost návštěv Lázeňských lesů v Karlových Varech v závislosti na počasí. Jsou sledovány faktory jako aktuální teplota, vlhkost, tlak, humidex, heat index (pocitová teplota).

4.2.4 Rozdíly naměřených hodnot v závislosti na technologii

V rámci sledování počtu návštěvníků dochází k použití dvou technologií. Sledování unikátních zařízení přes technologii Wi-Fi a Bluetooth. V závislosti na těchto technologiích dochází k rozdílu měření hodnot.

Tab. 18: Výpis dat za jednotlivá období v rozmezí 24 hodin

Datum	Počet unikátních zařízení Wifi	Počet unikátních zařízení Bluetooth
31.12.2023 00:00:00 – 31.12.2023 23:59:59	116	622
1.1.2023 00:00:00 - 1.1.2023 23:59:59	130	635
2.1.2023 00:00:00 - 2.1.2023 23:59:59	140	343
3.1.2023 00:00:00 - 3.1.2023 23:59:59	34	144
4.1.2023 00:00:00 - 4.1.2023 23:59:59	41	150

Z tabulky č. 18 je patrné že naměřené hodnoty jsou rozdílné. Lze usoudit, že naměřené hodnoty Wi-Fi jsou závislé převážně na chytrých telefonech, které v současné době lidé používají ke komunikaci k domácím bezdrátovým sítím právě přes tuto síť. Naopak technologie Bluetooth je více využívána v rámci komunikace s periferiemi mobilních zařízení, které návštěvník může mít rovněž sebou. Tedy jeho digitální stopa může být zaznamenána hned vícekrát. Zároveň lze předpokládat, že mnoho uživatelů má síť Wi-Fi na svém mobilním zařízení vypnutou, ať už z důvodů chytrých polohových funkcí zařízení anebo z důvodů nepotřeby této sítě, naopak uživatelé považují síť Bluetooth

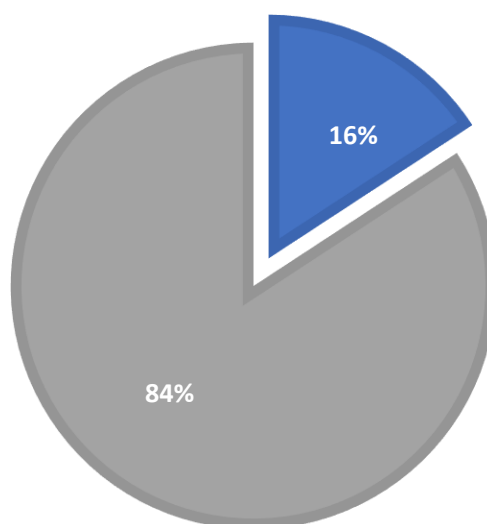
za žádoucí nechat zapnutou kvůli bezstarostné komunikaci mezi periferiemi (Například chytré hodinky, sportovní chytré náramky, Bluetooth komunikace s automobily, kterými se mohli dopravit k lázeňským lesům).

Tento trend lze sledovat i dlouhodobě v grafu 1, který jasně ukazuje dlouhodobou dominanci většího množství zaznamenaných zařízení Bluetooth. Lze tedy konstatovat, že Bluetooth bude lépe zaznamenat návštěvníka na základě charakteru technologie, ovšem zase může a bude zkreslovat na základě vícečetného zaznamenání jednoho účastníka, naopak technologie Wi-Fi na základě charakteru technologie nebude duplicitně zaznamenávat jednoho uživatele vícekrát a skutečný počet návštěvníků nebude nižší než unikátní počet Wi-Fi zařízení. Zvolené technologie budou zaznamenávat návštěvníky pouze na základě zařízení, které budou nosit u sebe. Což se může jevit jako problematické už jen kvůli předpokladu, že návštěvníci by museli mít na zařízeních, které nosí u sebe povolené nutné technologie.

Graf 1: Celkový počet všech zaznamenaných zařízení v podílu mezi technologiemi

**CELKOVÝ POČET NAMĚŘENÝCH ZAŘÍZENÍ OD
5.10.2022 DO 6.1.2023**

■ Unikátních Wi-fi zařízení 5444 ■ Unikátních Bluetooth zařízení 29029



4.2.5 Statické zařízení v dosahu, které ovlivňují výsledky měření

Tab. 19: Počet naměřených zařízení v době „klidu“

Datum	Počet unikátních zařízení Wifi	Počet unikátních zařízení Bluetooth
3.12.2022 00:00:00 - 3.12.2022 03:00:00	4	2
4.12.2022 00:00:00 - 4.12.2022 03:00:00	4	1
5.12.2022 00:00:00 - 5.12.2022 03:00:00	5	1
5.12.2022 00:00:00 - 5.12.2022 03:00:00	4	1
6.12.2022 00:00:00 - 6.12.2022 03:00:00	4	1
7.12.2022 00:00:00 - 7.12.2022 03:00:00	5	1

Skutečný počet naměřených zařízení návštěvníků je také zkreslen o statické zařízení v okolí, které jsou zaznamenávány neustále, tyto zařízení jsou zaznamenány v tabulce 19. Lze sledovat v čase od 00:00:00 do 03:00:00 skutečnost, že v okolí se nachází 4 statické Wi-Fi zařízení a minimálně 1 Bluetooth zařízení. Jedno ze 4 statických zařízení se povedlo na základě poskytnutých informací z prostředí Grafana identifikovat (viz. obrázek 11) jako platební terminál od společnosti Ingenico, lze tedy předpokládat že není obsluhou nikdy vypínáno, a tedy je stále zaznamenáváno do dat o unikátních počtu zařízení. Z tabulky 19 lze také vysledovat 5.12 odchylku u unikátních zařízení Wi-Fi, dle dat toto 5. zařízení bylo zaznamenáno s poměrně slabým signálem a lze tedy předpokládat že se mohlo jednat o individuální zaznamenání, zařízení tedy není konstantně zaznamenáváno na každém měření, mohlo se jednat o návštěvníka anebo o vzdálené zařízení, které bylo díky vhodným podmínkám změřeno s ohledem na charakter technologie Wi-Fi.

Na základě tabulky 19 lze tedy konstatovat že změřená zařízení za cílem získání informace o počtu návštěvníků jsou vždy zkruslena minimálně o 4 konstantní zařízení Wi-Fi a minimálně 1 zařízení Bluetooth.

Obr. 11: Detekovaný platební terminál jako statické zařízení v okolí měření (Zdroj: screenshot z prostředí Grafana)

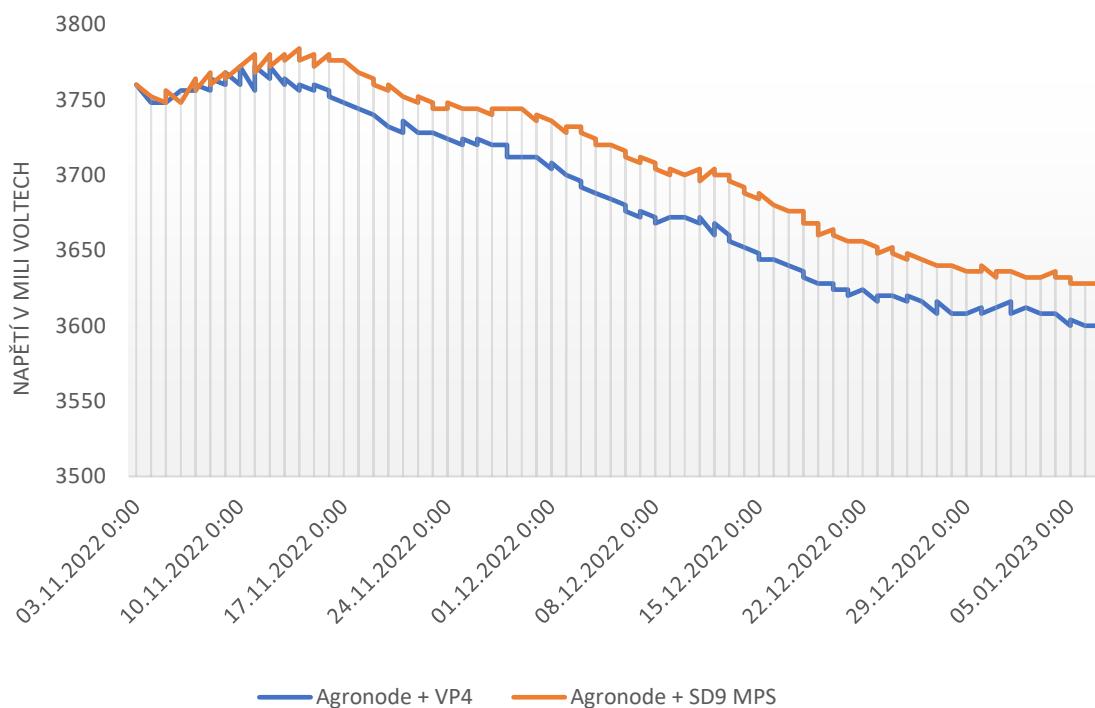
Wifi				
MAC adresa	Výrobce	Prvotní výskyt ↓	Poslední výskyt	Počet výskytů
38:ef:e3:39:75:41	INGENICO TERMINALS SAS	2022-12-04 00:37:57.000	2022-12-04 00:37:57	1

Na základě této analýzy lze vyvést závěry, že zvolené technologie na alternativní zajištění počtu návštěvníků nelze považovat za přesné, lze je použít k přibližnému odhadu počtu návštěvníků. K takovému odhadu počtu návštěvníků by bylo ale nejdříve nutné zanalyzovat přibližný skutečný počet návštěvníků k daným naměřeným hodnotám v časovém rozmezí, aby následně bylo možné poměrově přepočítávat odhadovaný počet návštěvníků. Zároveň jsou data zkruslena o staticky umístěná zařízení v okolí senzoru, tedy o 4 zařízení Wi-Fi a 1 zařízení Bluetooth. Pro optimalizaci naměřených dat by bylo vhodné na základě znalosti MAC adres statických zařízení tyto zařízení z měření vyloučit.

4.2.6 Napětí baterií v závislosti na počasí

Na základě sběru dat jsou k dispozici také informace o napětí jednotlivých baterií v zařízeních AgroNode. Tyto data lze sledovat v grafu 2.

Graf 2: Vývoj stavu napětí baterií v čase u dvou sledovaných zařízení AgroNode



V závislosti na čase lze v grafu 2 sledovat postupný dlouhodobý pokles napětí. Dochází, ale i ke krátkodobým nárůstům napětí, které lze přisoudit k vlastnosti zařízení AgroNode, které mají nainstalovaný solární panel. Vzhledem k tomu, že zařízení AgroNode začali být plnohodnotně využívány až v listopadu roku 2022, nelze momentálně sledovat jejich dlouhodobý trend stavu baterie vzhledem k aktuálnímu ročnímu období. Lze přisoudit, že během první poloviny listopadu byl dostatek slunečního světla, aby zařízení dokázalo elektrickou energii více akumulovat, a tedy docházelo k zvýšení napětí na bateriích v obou zařízeních. S nástupem zimy a postupnému zkracování dne začalo napětí v obou zařízeních postupně klesat. Aktuální hodnota napětí v tuto dobu je stále provozu schopná, dle manuálu výrobce začne být kritická hodnota pro provoz zařízení kolem 3,4 V. Nelze jednoznačně usoudit na základě dat, zdali bude zařízení celoročně provozuschopné bez zásahu třetí osoby, která by zařízení nabíla.

V období mezi 1.12.2022 a 1.1.2023 lze sledovat průměrný pokles napětí o 92mV, ale v období od 1.11.2022 až 1.12.2022 lze sledovat průměrný pokles napětí o 44mV, tedy pokles napětí nebude nikdy konstantní vzhledem k tomu, že solární panel stále vyrobí určitě množství energie, které sice nedokáže současný zdroj energie dobít, či zachovat na aktuální hodnotě napětí, ale dokáže alespoň snížit spotřebu energie ze zdroje.

Vzhledem k postupnému dlouhodobému poklesu napětí v bateriích by bylo vhodné upravit zařízení tak, aby nebylo možné zejména během zimních období dospět do stavu kritického vybití baterie. Jako jedno z možných řešení by mohlo být lepší umístění zařízení s přímým výhledem na oblohu, aby přímý sluneční svit nebyl nijak stíněn. Také jako další možnost řešení tohoto problému by bylo možné připojit další solární panel, nebo vyměnit stávající za větší, který by poskytl více elektrické energie, popřípadě by také bylo možné zvětšit současný zdroj energie tak, aby vydržel celou zimu.

Závěrem lze konstatovat, že zařízení AgroNode dokáže vydržet poměrně dlouhou dobu bez nutné obsluhy, vzhledem k vlastnímu zdroji napájení, ovšem v kritických obdobích kvůli špatným podmínkám počasí lze sledovat postupný pokles napětí, který by mohl dosáhnout až kritické hodnoty, kdy by zařízení nebylo schopné provozu. Tento problém by šel vyřešit zvětšením zdroje elektrické energie anebo lepším umístěním zařízení v prostředí instalace.

5. Zhodnocení a doporučení

Na základě pilotního ověření IoT systému v lokalitě Lázeňské lesy Karlovy Vary bylo zanalyzováno hned několik dílčích částí:

- Použitý Hardware včetně technologie konektivity SigFox
- Sběr dat s ohledem na vztah k GDPR
- Porovnání technologií Wi-Fi a Bluetooth pro sledování počtu návštěvníků
- Nepřesnost měření na základě statických zařízení v okolí
- Sledování stavu baterií při dlouhodobém užití

U každé z této části byli zhodnoceny výsledky a případná doporučení.

5.1 Použitý hardware včetně sítě technologie SigFox

Použití brány AgroNode bylo zhodnoceno jako velmi vhodné, zejména díky její kompatibilitě s více vstupními rozhraními SDI12, 1WIRE, RS485, I2C, které zvyšují možný výběr senzorů, a tedy potencionální snížení vstupních nákladů. Dále brána AgroNode podporuje také poměrně velké množství dostupných IoT sítí, což opět může zlepšit volbu sítě s ohledem na náklady s tím spojené. Užití sítě SigFox je vhodné, na základě analýzy dostupnosti IoT sítí v dané lokalitě je formulován závěr tak, že síť SigFox je optimální pro provoz v lokalitě Lázeňské lesy Karlovy Vary. Zejména díky její dostupnosti, ale také kvůli charakteru této sítě.

5.2 Sběr dat s ohledem na vztah k GDPR

Na základě analýzy posbíraných dat bylo zhodnoceno, že na data se v tuto chvíli sice GDPR nevztahuje, ale dochází ke sběru MAC adresy zařízení návštěvníků, která by mohla s pozdějším sběrem dalších dat přímo identifikovat fyzické osoby. Proto bylo navrženo doporučení MAC adresy pseudonymizovat pomocí kryptografických hashovacích funkcí například SHA-1. Po pseudonymizaci nebude již MAC adresa přímo identifikovat unikátní zařízení, ale data o MAC adresách stále budou vhodně moci rozlišit unikátní zařízení v rámci měření. Toto doporučení je navrženo v tabulce 20.

Tab. 20: Návrh možné pseudonymizace MAC adres

MAC adresa v originální podobě	MAC adresa v pseudonymizované podobě
2E:DA:C9:A9:F5:76	aeaa1250c26f1dce95d3572039f23875a6985c3e
22:CA:54:51:24:30	c2e42d34abb1e2dcaed90c7b0ad579d14e850f20
0E:F8:AF:70:2B:44	7b84396147d3424adf1b99d8c94b6ae01a2a1200
72:CE:A5:E9:0E:37	43353d9f971b2bd86db966cb1cff5e7a567d5f57

5.3 Porovnání technologií pro sledování počtu návštěvníků

Při porovnávání naměřených výsledků pomocí technologie Bluetooth a Wi-Fi bylo dosaženo závěru, že naměřené hodnoty jsou rozdílné. Tento rozdíl naměřených hodnot je dán charakterem technologií a zejména aktuálním trendem, kdy návštěvníci nosí s sebou hned několik zařízení s povolenou Bluetooth technologií. Při měření unikátních Bluetooth zařízení ovšem není vyloučeno zaevidování návštěvníka hned vícekrát.

Dále bylo zaznamenáno, že se v okolí měření nachází celkově 4 statická Wi-Fi zařízení a 1 Bluetooth zařízení, bylo doporučeno z celkového počtu zaznamenaných unikátních zařízení přestat evidovat taková zařízení, která jsou staticky umístěna v okolí zařízení, a tedy logicky nejsou majetkem žádného návštěvníka, tudíž vytváří odchylku ve výsledku měření.

5.4 Sledování stavu baterie

Při sledování stavu baterie, která napájí zařízení AgroNode bylo zhodnoceno, že v dlouhodobém trendu klesá její stav napětí. To může být dáno zejména zimním počasím, které se negativně projevuje na zisk energie ze solárního panelu. Na základě posbíraných dat nelze usoudit, zdali zdroj energie zařízení do příchodu přívetivějšího počasí dokáže fungovat a nedojde k dosažení kritické hranice napětí. Na základě tohoto potencionálního problému bylo doporučeno vylepšit zisk energie ze solárního panelu buď lepším umístěním zařízení s ohledem na dobrý výhled na oblohu anebo poskytnout zařízení zdroj energie s vyšší kapacitou.

6. Závěr

Na základě pilotního ověření provedeného na již fungujícím IoT systému v lokalitě Lázeňských lesů Karlovy Vary, kde cílem tohoto systému je získat alternativní způsob počítání počtu návštěvníků byly v rámci analýzy vyvedeny tyto stěžejní výsledky: Použitá síť SigFox je optimální, na základě její velmi dobré dostupnosti v lokalitě, ale také díky jejím vlastnostem ohledně nízké spotřeby energie. Naměřené hodnoty pomocí technologií Bluetooth a Wi-Fi jsou rozdílné, což je dáno charakterem a aktuálním trendem využívání těchto sítí. Výsledky unikátního počtu zařízení jsou také zkresleny o statická zařízení v okolí, která nejsou jednoznačně zařízení návštěvníků. Na MAC adresy zařízení návštěvníků se může vztahovat zákon o GDPR, kvůli možnému riziku identifikace návštěvníka v rámci kombinace více posbíraných dat, a tedy je vhodné tyto MAC adresy pseudonymizovat tak, aby jejich unikátnost pro účely měření byla zachována a zároveň aby zařízení již nebylo možné zpětně identifikovat. Zdroj energie zařízení vykazuje dlouhodobě klesající trend ve vztahu k napětí, převážně kvůli nízkému zisku energie ze solárního panelu zařízení během zimních období. Je také provedena analýza sítí konektivity pro IoT systémy, ze které vyplívá, že analyzované síť mají své užití a jejich optimálnost určuje prostředí a charakter zařízení.

Jsou vyvozeny následující doporučení:

- Vyloučit nežádoucí statická zařízení z měření unikátního počtu zařízení na základě znalosti jejich MAC adresy.
- Provedení pseudonymizace MAC adres zařízení návštěvníků pomocí kryptografických hashovacích funkcí.
- Vylepšit zisk energie lepším umístěním solárního panelu zařízení, popřípadě zvětšit plochu solárního panelu zařízení a vylepšit akumulátor zařízení, aby zařízení bylo schopné dlouhodobého provozu během období s nízkým ziskem energie ze solárního panelu.

7. Seznam použitých zdrojů

7.1 Odborné publikace

3. CHMELÁŘOVÁ, Magdalena, Helena KOLIBOVÁ a Věra JUŘÍČKOVÁ. *Internet věcí a chytrá města v regionální perspektivě*. Opava: Slezská univerzita v Opavě : Fakulta veřejných politik v Opavě, 2019. str. 7. ISBN 978-80-7510-358-1.

4. RAJ, Pethuru a Anupama C. RAMAN. *The Internet of things: enabling technologies, platforms, and use cases*. Boca Raton : RC Press/Taylor & Francis Group, 2017. stránky 53-56. ISBN 978-1498761284.

18. RAJ, Pethuru a Anupama C. RAMAN. *The Internet of things: enabling technologies, platforms, and use cases*. Boca Raton : CRC Press/Taylor & Francis Group, 2017. str. 71. ISBN 978-1498761284.

24. RAJ, Pethuru a Anupama C. RAMAN. *The Internet of things: enabling technologies, platforms, and use cases*. Boca Raton : CRC Press/Taylor & Francis Group, 2017. str. 55. ISBN 978-1498761284.

25. Garg, N. Garg a R. *Energy harvesting in IoT devices: A survey*. International Conference on Intelligent Sustainable Systems (ICISS) : s.n., 2017. DOI: 10.1109/ISS1.2017.8389371.

26. Anwesa Mohanty, Suraj Parida, Rabindra Kumar Behera. *Vibration energy harvesting: A review*. Rourkela, India : National Institute of Technology, 2019. DOI: 10.1142/S2010135X19300019.

28. RAJ, Pethuru a Anupama C. RAMAN. *The Internet of things: enabling technologies, platforms, and use cases*. Boca Raton : CRC Press/Taylor & Francis Group, 2017. stránky 249-272. ISBN 978-1498761284.

29. RAJ, Pethuru a Anupama C. RAMAN. *The Internet of things: enabling technologies, platforms, and use cases*. Boca Raton : CRC Press/Taylor & Francis Group, 2017. stránky 273-292. ISBN 978-1498761284.

30. RAJ, Pethuru a Anupama C. RAMAN. *The Internet of things: enabling technologies, platforms, and use cases*. Boca Raton : CRC Press/Taylor & Francis Group, 2017. str. 235. ISBN 978-1498761284.

36. RAJ, Pethuru a Anupama C. RAMAN. *The Internet of things: enabling technologies, platforms, and use cases.* Boca Raton : CRC Press/Taylor & Francis Group, 2017. stránky 279-280. ISBN 978-1498761284.

38. RAJ, Pethuru a Anupama C. RAMAN. *The Internet of things: enabling technologies, platforms, and use cases.* Boca Raton : CRC Press/Taylor & Francis Group, 2017. str. 296. ISBN 978-1498761284.

42. ABDUL MAJEED, SUNGCHANG LEE. *Anonymization Techniques for Privacy Preserving.* Kojang : IEEE, 2020. DOI: 10.1109/ACCESS.2020.3045700.

45. RAJ, Pethuru a Anupama C. RAMAN. *The Internet of things: enabling technologies, platforms, and use cases.* Boca Raton : CRC Press/Taylor & Francis Group, 2017, str. 42. ISBN 978-1498761284.

7.2 Internetové zdroje

1. **IoTPORT.** Co to je IoT? *IoTPORT*. [Online] 27. Leden 2020. <https://www.iotport.cz/iot-novinky/ostatni-clanky-o-iot/co-to-je-iot>.
2. **Gillis, Alexander S.** What is the internet of things (IoT)? <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>. [Online] 2022. [Citace: 9. 7 2022.] <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>.
5. **Sedlák, Jan.** Síť internetu věcí Sigfox míří do bankrotu, v Česku má provoz fungovat i nadále. *Lupa.cz*. [Online] 31. 1 2022. [Citace: 12. 7 2022.] <https://www.lupa.cz/aktuality/sit-internetu-veci-sigfox-miri-do-bankrotu-v-cesku-ma-provoz-fungovat-i-nadale/>.
6. **David Polesný.** Zkusili jsme Sigfox, síť pro internet věcí. *mobilmania.zive.cz*. [Online] [Citace: 12. 7 2022.] <https://mobilmania.zive.cz/clanky/zkusili-jsme-sigfox-sit-pro-internet-veci/sc-3-a-1334151/default.aspx>.
7. **Síťové technologie LPWAN pro Internet věcí – 6. díl.** *Network News*. [Online] [Citace: 12. 7 2022.] <https://cz.iot-nn.com/blog/2017/09/07/sitove-technologie-lpwan-pro-internet-veci-6-dil/>.
8. **Síťové technologie LPWAN pro Internet věcí – 5. díl.** *NetworkNews*. [Online]. [Citace: 12. 7 2022.] <https://cz.iot-nn.com/blog/2017/06/27/sitove-technologie-lpwan-pro-internet-veci-5-dil/>.
9. **Ingenu. Technology - Ingenu.** [Online] <https://www.ingenu.com/technology>.
10. **Jan Sedlák.** IoT síť se nám rozjela. Tržby jsou ve vyšších desítkách milionů, uvádí České Radiokomunikace. *Lupa.cz*. [Online] 9. 6 2022. [Citace: 12. 7 2022.] <https://www.lupa.cz/clanky/iot-sit-se-nam-rozjela-trzby-jsou-ve-vyssich-desitkach-milionu-uvadi-ceske-radiokomunikace/>.
11. **LoRaWAN - připojení do sítě IoT.** *IoTPORT.cz*. [Online] [Citace: 12. 7 2022.] <https://www.iotport.cz/lorawan-sit-pro-iot>.
12. **LoRaWAN, Sigfox nebo NB-IoT?** Srovnání 3 významných typů IoT sítí. *IoTPort.cz*. [Online] 3. 10 2020. [Citace: 12. 7 2022.] <https://www.iotport.cz/iot-novinky/lorawan/lorawan-sigfox-nebo-nb-iot-srovnani-3-vyznamnych-typu-iot-siti>.

13. **Pech, Jiří.** IoT technologie: IQRF (2/5). *eman*. [Online] 17. 1 2019. [Citace: 14. 7 2022.] <https://www.eman.cz/blog/iot-technologie-iqrf-2-5/>.
14. **Best Uses of Wireless IoT Communication Technology.** *Industry today*. [Online] 13. 12 2018. [Citace: 14. 7 2022.] <https://industrytoday.com/best-uses-of-wireless-iot-communication-technology/>.
15. **5G vs 4G: Jaké jsou rozdíly, jak je na tom ČR s pokrytím a jsou opravdu rychlosti 10× vyšší?** *inSmart*. [Online] 29. 7 2020. [Citace: 14. 7 2022.] <https://insmart.cz/5g-vs-4g-vse-o-sitich-budoucnosti/>.
16. **Jena, Satyabrata.** Overview of Wireless Personal Area Network (WPAN). *GeeksforGeeks.org*. [Online] 17 3 2021. [Cited: 17 7 2022.] <https://www.geeksforgeeks.org/overview-of-wireless-personal-area-network-wpan/>.
17. **Co je to Zigbee technologie, proč je důležitá pro smart domácnost a jaké Xiaomi produkty ji podporují?** *xiaomiplanet.cz*. [Online] 22. 11 2020. [Citace: 17. 7 2022.] <https://www.xiaomiplanet.cz/ZigBee-technologie/>.
19. **Kilián, Karel.** Co je NFC a k čemu je dobré ho použít? *svetandroida.cz*. [Online] 25. 6 2022. [Citace: 17. 7 2022.] <https://www.svetandroida.cz/co-je-nfc-k-cemu-je-dobre-ho-pouzit/>.
20. **Awati, Rahul.** Categories of twisted-pair cabling systems . *TechTarget*. [Online] 2 2022. [Cited: 18 7 2022.] <https://www.techtarget.com/searchdatacenter/definition/Categories-of-twisted-pair-cabling-systems>.
21. **Lukáš Václavík.** Éra Wi-Fi 7 pomalu začíná. Rychlosti přenosu přiblíží k 50 Gb/s. *zive.cz*. [Online] 8. 6 2021. [Citace: 18. 7 2022.] <https://www.zive.cz/clanky/era-wi-fi-7-pomaluzacina-rychlosti-prenosu-priblizi-k-50-gb/s/sc-3-a-210574/default.aspx>.
22. **Wi-Fi má nového sourozence. Přivítejte HaLow optimalizované pro IoT.** *zive.cz*. [Online] 25. 11 2021. [Citace: 18. 7 2022.] <https://www.zive.cz/clanky/wi-fi-ma-noveho-sourozence-privitejte-halow-optimalizovane-pro-iot/sc-3-a-213581/default.aspx>.
23. **Čížek, Jakub.** Wi-Fi pro internet věcí se bude jmenovat HaLow. [Online] 12. 1 2016. [Citace: 18. 7 2022.] <https://www.zive.cz/bleskovky/wi-fi-pro-internet-veci-se-bude-jmenovat-halow/sc-4-a-181025/default.aspx>.

27. **Aline Eid, Jimmy G. D. Hester, Manos M. Tentzeris.** *nature.com. 5G as a wireless power grid.* [Online] 2021. 1 12. [Citace: 21. 7 2022.] <https://www.nature.com/articles/s41598-020-79500-x>.
31. **IoTport.cz.** *Zařízení pro dálkový odečet vodoměrů .* [Online] [Citace: 25. 7 2022.] <https://www.iotport.cz/iot-reseni/odecty-a-spotreba/zarizeni-pro-dalkovy-odecet-vodomeru-wmr04-l>.
32. **Parkování nejen ve městě.** *IoTport.cz.* [Online] [Citace: 25. 7 2022.] <https://www.iotport.cz/iot-reseni/mesto-kraj-region-ves/parkovani-v-centru-rican>.
33. **IoT Parking Sensor Standard.** *fleximodo.com.* [Online] [Citace: 25. 7 2022.] <https://www.fleximodo.com/solution-iot-parking-sensor/>.
34. **IoT a chytrý management odpadu .** *IoTPort.cz.* [Online] 28. 4 2020. [Citace: 2. 8 2022.] <https://www.iotport.cz/iot-a-chytry-management-odpadu>.
35. **IoTport.cz.** *Agdata zemědělské senzory.* [Online] [Citace: 25. 7 2022.] <https://www.iotport.cz/iot-reseni/agro-a-environment/zemedelske-senzory>.
37. **Velký přehled cloudů pro IoT – 1. část .** *IoT-portal.cz.* [Online] 2. 23 2017. [Citace: 26. 7 2022.] <https://www.iot-portal.cz/2017/02/23/velky-prehled-cloudu-pro-iot-1-cast/>.
39. **Škorníčková, Mgr. Eva.** <https://www.gdpr.cz/gdpr/co-je-gdpr/>. *GDPR.cz.* [Online] [Citace: 27. 7 2022.] <https://www.gdpr.cz/gdpr/co-je-gdpr/>.
40. **Škorníčková, Mgr. Eva.** Jaké zásadní změny GDPR přinese. *gdpr.cz.* [Online] [Citace: 27. 7 2022.] <https://www.gdpr.cz/gdpr/zmeny/>.
41. **Škorníčková, Mgr. Eva.** *GDPR.cz. Co považuje GDPR za osobní údaje.* [Online] [Citace: 27. 7 2022.] <https://www.gdpr.cz/gdpr/osobni-udaje/>.
43. **Škorníčková, Mgr. Eva.** Anonymizace a pseudonymizace jsou dvě rozdílná slova. *GDPR.CZ.* [Online] 20. 9 2017. [Citace: 29. 7 2022.] <https://www.gdpr.cz/blog/anonymizace-a-pseudonymizace-jsou-dve-rozdilna-slova/>.
44. **Popović, Josipa. bizdatax.com.** *Anonymization and Pseudonymization in the context of GDPR.* [Online] 18 11 2020. [Cited: 29 7 2022.] <https://bizdatax.com/anonymization-and-pseudonymization-in-the-context-of-gdpr/#>.

8. Seznam obrázků, tabulek, grafů a zkratk

8.1 Seznam obrázků

Obr. 1: Ukázka vhodné konektivity v rámci různorodosti zařízení a služeb (4)	15
Obr. 2: Porovnání vlastností bezdrátových technologií (24)	21
Obr. 3: Rozdíl instalace parkovacího senzoru. (33).....	32
Obr. 4: Proces získávání, přenosu a zpracování dat (37)	33
Obr. 5: Pokrytí sítě SigFox v oblasti Lázeňských lesů v Karlových Varech(screenshot z webu https://coverage.sigfox.cz/)	47
Obr. 6: Mapa pokrytí sítě LoRaWAN v České republice (Vlastní screenshot z webu(11))	47
Obr. 7: Pokrytí sítě SigFox v oblasti Lázeňských lesů v Karlových Varech(screenshot z webu https://www.vodafone.cz/mapa-pokryti/)	48
Obr. 8: Ukázka nezpracovaných dat se znehodnocením identifikovatelných dat ke vztahu k GDPR (vlastní screenshot z poskytnutých dat).....	49
Obr. 9: Snímek obrazovky, sledovaných dat za uplynulých 24 hodin z data 29.12.2022 00:00:00 až 29.12.2022 23:59:59. (Screenshot z rozhraní Grafana na základě poskytnutého přístupu).	51
Obr. 10: Snímek obrazovky, sledovaných dat za uplynulých 24 hodin z data 29.12.2022 00:00:00 až 29.12.2022 23:59:59. (Screenshot z rozhraní Grafana).	51
Obr. 11: Detekovaný platební terminál jako statické zařízení v okolí měření (Zdroj: vlastní screenshot z prostředí Grafana).....	55

8.2 Seznam tabulek

Tab. 1: Porovnání mobilních sítí od 3. do 5. generace. (15).....	18
Tab. 2: Porovnání standardů Wi-Fi (21).....	20
Tab. 3: Srovnání zdrojů generující energii. (25).....	24
Tab. 4: Příklad dat telefonické společnosti (upravený příklad podle zdroje (44))	35
Tab. 5: Data po odstranění přímo identifikovatelných dat. (upravený příklad podle zdroje (44))	36
Tab. 6: Data po generalizaci dat. (upravený příklad podle zdroje (44)).....	36
Tab. 7: Přehled dat po provedení permutace věku (upravený příklad podle zdroje (44)) ...	37
Tab. 8: Data s vygenerovanou hodnotou šumu, která neovlivní použitelnost dat(upravený příklad podle zdroje (44))	37
Tab. 9: Data s již přidaným šumem. (upravený příklad podle zdroje (44)).....	37
Tab. 10: Příklad z tabulky 5 po pseudonymizaci tokenem (upravený příklad podle zdroje (44))	38
Tab. 11: Klíč k tabulce 10 (upravený příklad podle zdroje (44))	38
Tab. 12: SWOT Analýza LPWAN sítí	41
Tab. 13: SWOT Analýza Mobilních sítí	42
Tab. 14: SWOT Analýza LAN sítí	43
Tab. 15: SWOT Analýza WPAN sítí.....	44
Tab. 16: Porovnání pokrytí konektivity v oblasti Lázeňských lesů v Karlových Varech ...	46
Tab. 17: Pseudonymizace MAC adresy pomocí hashovací funkce SHA-1	50
Tab. 18: Výpis dat za jednotlivá období v rozmezí 24 hodin	52
Tab. 19: Počet naměřených zařízení v době „klidu“	54
Tab. 20: Návrh možné pseudonymizace MAC adres	59

8.3 Seznam grafů

Graf 1: Celkový počet všech zaznamenaných zařízení v podílu mezi technologiemi.....	53
Graf 2: Vývoj stavu napětí baterií v čase u dvou sledovaných zařízení AgroNode	56

8.4 Seznam použitých zkratek

IoT	Internet of Things (Internet věcí)
GDPR	General Data Protection Regulation (Nařízení o ochraně osobních údajů)
P2P	Peer-to-Peer (klient-klient počítačová síť)
IaaS	Infrastructure as a service (Integrace jako služba)
PaaS	Platform as a Service (Platforma jako služba)
SaaS	Software as a service (Software jako služba)
LPWAN	Low-power wide-area network (Nízkoenergetická rozlehlá síť)
GPS	Global Positioning System (Globální polohový systém)
NB-IOT	Narrowband Internet of Things (Úzkopásmové připojení internetu věcí)
USA	United States of America (Spojené státy americké)
IBM	International Business Machines Corporation
CRA	České Radiokomunikace
SIM	Subscriber Identity Module (Modul identity účastníka)
LTE	Long Term Evolution (Dlouhodobý vývoj)
WPAN	Wireless Personal Area Network (Bezdrátová osobní síť)
BLE	Bluetooth Low Energy
NFC	Near Field Communication
RFID	Radio Frequency Identification
LAN	Local Area Network (Lokální počítačová síť)
Cat5e	Category 5 Enhanced
Cat6	Category 6
IT	Information technology (Informační technologie)
WAN	Wide Area Network (Rozlehlá počítačová síť)
QR	Quick Response
EU	Evropská unie

IP	Internet protocol
SWOT	Strengths (Silné stránky), Weaknesses (Slabé stránky), Opportunities (Příležitosti), Threats (Hrozby)
MAC	Media Access Control
SHA-1	Secure Hash Algorithm 1
RSSI	Received Signal Strength Indication

