Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Bakalářská práce

Analýza a vyhodnocení vybraných technologií IoT vhodných pro domácí automatizaci

Albert Suchopár

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Albert Suchopár

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Analýza a vyhodnocení vybraných technologií IoT vhodných pro domácí automatizaci

Název anglicky

Analysis and evaluation of selected IoT technologies suitable for home automation

---

Cíle práce

Práce zpracovává vhodně zvolené technologie a prostředky tzv. „internetu věcí", definuje jejich fyzikální a technické parametry a na základě těchto zjištění stanovuje podmínky pro jejich využiti v různých oblastech domácí automatizace.

Metodika

1. Úvod
2. Cíl práce
3. Metodika
4. Stanovení podmínek pro výběr technologií a diskuse těchto podmínek
5. Výběr technologií a jejich technické specifikace
6. Analýza aplikačních možnosti jednotlivých technologií

Doporučený rozsah práce

30 až 40 stran textu včetně obrázků, grafů a tabulek

Klíčová slova

IoT, počítačová komunikace, počítačové protokoly, aplikace

Doporučené zdroje informací

BURIAN, P: Internet inteligentních aktivit, Grada 2014, e-kniha
Internetové zdroje, např. https://www.e15.cz/magazin/prumysl-prochazi-zmenou-jako-nikdy-predtim-rika-autor-knihy-o-internetu-veci-1333263

James F. Kurose, Keith W. Ross: Počítačové sítě, CPress, 2014, 3. vydání
Maciej Kranz: Budování internetu věcí, New York Times, 2017

Předběžný termín obhajoby

2021/2022 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 3. 2. 2021

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 2. 2021

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 04. 11. 2021

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci „Analýza a vyhodnocení vybraných technologií IoT vhodných pro domácí automatizaci" 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 Praze dne: ……. ……..

Albert Suchopár

Poděkování

Děkuji svému vedoucímu práce Ing. Zdeňkovi Votrubovi, Ph.D. za výběr tématu, za ochotu a možnost pracovat pod jeho vedením. Během zpracování tohoto tématu jsem získal mnoho nových znalostí. Chtěl bych také poděkovat své rodině za podporu, trpělivost a motivaci. V neposlední řadě velké díky patří mému kamarádovi Adamovi za jeho velkolepý výkon při korektuře této práce.

Analýza a vyhodnocení vybraných technologií IoT vhodných pro domácí automatizaci

Abstrakt

Tématem bakalářské práce je analýza technologií využívaných v tzv. internetu věcí z hlediska možnosti jeho využití v domácí automatizaci. Na začátku práce se autor zabývá definicí internetu věcí a základním popisem jeho fungování. Dále jsou probrány jednotlivé komunikační technologie a cloudové platformy. Na to navazují zhodnocení jejich aplikačních možností v domácí automatizaci a srovnání finanční náročnosti nasazení IoT technologií oproti běžným způsobům domácí automatizace. Na závěr je nastíněn budoucí vývoj internetu věcí a doporučení vhodných technologií IoT pro realizaci automatizované domácnosti.

Klíčová slova: *IoT, počítačová komunikace, počítačové protokoly, aplikace*

Analysis and evaluation of selected IoT technologies suitable for home automation

Abstract

The topic of this dissertation is an analysis of technologies used in the so-called Internet of Things in terms of the possibilities of use in home automation. The beginnig of the thesis deals with the definition of the Internet of Things and a basic description of its functioning. The individual communication technologies and cloud platforms are also discussed. This is followed by an evaluation of their application possibilities in home automation and a comparison of the financial demands of the deployment of IoT technologies compared to conventional methods of home automation. The end of the thesis outlines future development of the Internet of Things and suitable IoT technologies for the implementation of an automated home.

Keywords: *IoT, computer communication, computer protocols, applications*

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

IoT – Internet of Things

IPv4 – Internet Protocol version 4, internetový protokol verze 4

IPv6 – Internet Protocol version 6, internetový protokol verze 6

OSI – Open Systems Interconnection model, Open Systems Interconnection model

ISM - Industrial, Scientific and Medical

EIRP – Equivalent isotropically radiated power, ekvivalentní izotropně vyzářený výkon

LPWAN – Low-power wide-area network, nízkoenergetická síť dlouhého dosahu

PAC – porting authorisation code, autorizační kód pro přenesení

LoRA – Long Range, dlouhý dosah

NB-IoT- Narrowband Internet of Things

3GPP – The 3rd Generation Partnership Project, Partnerský projekt třetí generace

GSM – Groupe Spécial Mobile

LTE – 3GPP Long-Term Evolution, dlouhodobý vývoj 3GPP

P2P – peer-to-peer, klient-klienr

BLE – Bluetooth Low Energy

TWT – Target Wake Time, cílový čas buzení

RFID – Radio Frequency Identification, identifikace na rádiové frekvenci

NFC – Near field communication, blízkopolní komunikace

SDK – Software development kit, sada vývojových nástrojů

NAS – Network Attached Storage, datové úložiště na síti

1 Úvod

Jedním z největších historických milníků z hlediska komunikace bylo vytvoření globální sítě nazývané internet. Ta je bezesporu největší počítačovou sítí na světě a denně propojuje uživatele napříč kontinenty. Dosud byla vnímána pouze jako virtuální nehmotné prostředí. Rozšíření internetu věcí však může změnit dosavadní vnímání internetu.

Internet věcí (IoT) je fenoménem dnešní doby a marketingovým hitem mnoha prodejců spotřební elektroniky, nicméně uvědomit si význam tohoto pojmu a zjistit, jak jej uchopit, se zdá být kvůli přemíře informací stále složitější. Internet věcí je rozsáhlá oblast, a proto jej často každý autor může definovat odlišně. Prvotní myšlenkou IoT byla snaha o propojení „věcí" (senzorů, spotřebičů, regulátorů, nositelné elektroniky atd.) v jeden funkční celek, a tedy vytvoření ekosystému pro vícero typů zařízení. Tento koncept otevírá nepřeberné množství možností ve všech aktuálních i budoucích oborech. Díky tomu je IoT zajímavou oblastí nabízející množství příležitostí pro firmy i pro jednotlivce.

Proto není divu, že je stále obtížnější nalézt oblast, kde by internet věcí nenašel své uplatnění a nebyl tak součástí mnoha inovací. Výstižným příkladem je často zmiňovaný průmysl 4.0, kde internet věcí hraje podstatnou roli v procesu digitalizace, propojování a automatizování veškerých výrobní úkonů a služeb. Tato práce se však zmařuje především na internet věcí v nekomerčních podmínkách. Konkrétně v domácnosti, kde je schopná ulehčit každodenní život díky automatizaci všedních úkonů.

Automatizace v domácnosti je přítomna již delší dobu v podobě klasických spotřebičů jako je myčka, pračka či vysavač. Internet věcí však přináší další krok ve způsobu automatizace a obecně mění představu o moderní domácnosti. Díky IoT lze udělat z hrstky různorodých spotřebičů jeden organismus, který analyzuje všechny své úkony a využívá informace ze všech svých částí se záměrem zefektivnit svoje fungování a tím mimo jiné docílit časové a energetické úspory.

2 Cíl práce

Cílem práce je objasnit aktuální možnosti a fungování internetu věcí, specifikovat základní vlastnosti vybraných technologií tvořících tento koncept a zhodnotit jejich aplikační možnosti v domácí automatizaci. Dále zvážit finanční náročnost běžné technologie a internetu věcí při nasazení v domácí automatizaci a na závěr učinit, kromě pohledu na budoucí vývoj oboru, i doporučení vhodných technologií pro realizaci automatizované domácnosti.

3 Metodika

V první řadě bylo potřeba si uvědomit význam a způsob fungování internetu věcí, především díky literární rešerši ověřených zdrojů. Po prozkoumání problematiky byly vybrány podstatné technologie tvořící internet věcí. Tyto technologie byly dále zkoumány, skrze získaná data o jejich četnosti použití; byly vybrány ty nejběžněji využívané na trhu. Byly posouzeny jejich základní vlastnosti a v závislosti na tom i jejich aplikační možnosti pro domácí automatizaci. Dalším krokem bylo finanční zhodnocení a porovnání automatizace domácnosti prostřednictvím běžných způsobů a IoT. Následně byly prozkoumány možnosti budoucího vývoje internetu věcí a jeho nasazení v domácnostech. Na závěr byly shrnuty poznatky ze všech kapitol a byly doporučeny vhodné technologie pro domácí automatizaci.

4 Principy technologie internetu věcí a domácí automatizace

V první řadě je nutné pochopit problematiku a přibližný způsob fungování internetu věcí. Při té příležitosti budou zmíněny i jeho podstatné funkce a limity technologie. Je třeba si též uvědomit co přináší automatizace, ujasnit si význam pojmu automatizovaná domácnost a jaké další její varianty mohou existovat.

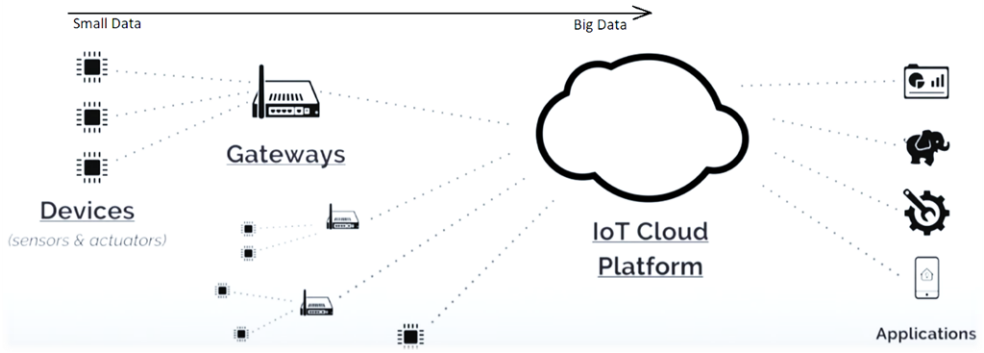
4.1 Internet věcí

Termín internet věcí nelze jednoznačně specifikovat, jelikož existuje nepřeberné množství různých definic. Jak už bylo řečeno na úvod, každý autor definuje internet věcí mírně odlišně. Dalo by se říct, že vizí internetu věcí je vytvářet z „hloupých" objektů objekty „chytré". Například společnost IBM vysvětluje pojem internet věcí jako koncept rozsáhlé sítě vzájemně propojených věcí a lidí, které shromažďují a sdílejí data o svém stavu a prostředí kolem nich. (1)

Je důležité zmínit, že koncept internetu věcí nespočívá pouze ve výměně dat mezi fyzickými objekty, ale i mezi virtuálními objekty prostřednictvím internetu. Díky tomuto spojení je IoT efektivním nástrojem pro shromažďování a analyzování dat s následnou optimalizací celkového provozu.

4.1.1 Architektura IoT

Z hlediska vzniku, přenosu a zpracování dat v sítích internetu věcí lze popsat typickou topologii třemi základními prvky – viz Obr. 1. Prvním prvkem je koncové zařízení. Jedná se především o senzory či akční členy, které produkují nebo přijímají data. Druhým prvkem je místo, které odděluje síť zařízení od globální sítě, což může představovat router, síťová brána, centrální jednotka nebo hub. Tato zařízení mimo jiné spojují i koncová zařízení s cloudovým clusterem. Ten tvoří poslední prvek a je místem, kde běží služby, které zpracovávají, analyzují a ukládají hotové informace. Tyto informace mohou následně využívat různé aplikace. (2), (3)



Obr. 1 Typická topologie internetu věcí (4)

Koncová zařízení generují malé množství dat, typicky v jednotkách bajtů. Jedná se obvykle o údaje teploty, vlhkosti či lokace. Data, se kterými se zde pracuje, mají typicky malé objemy, proto se nazývají Small Data Tato data se odesílají různými drátovými či bezdrátovými protokoly skrze síťovou bránu a internetu do cloudu. Tam se Small Data z různých datových toků shromažďují a stávají se z nich velká nestrukturovaná data nazývaná též jako Big Data. Protože v cloudu se data dlouhodobě ukládají, lze je nyní dále systematizovat a analyzovat. Výsledky tohoto procesu mohou být následně vizualizovány prostřednictvím grafu či tabulky v různých aplikacích. (2), (3)

Internet věcí však nezahrnuje pouze přenos a čtení informací z koncových zařízení, ale také jejich vzdálenou správu. Různé IoT platformy umožňují zápis dat na periferní zařízení, která následně vykonají cílenou činnost. Za tímto účelem bývá v platformách internetu věcí implementována tzv. virtuální reprezentace periferních zařízení, která umožňuje zaznamenávat veškeré informace o změně stavu koncových zařízeních a v závislosti na to i aktualizovat jejich aktuální stav. (2), (3)

4.1.2 Funkce a výzvy IoT

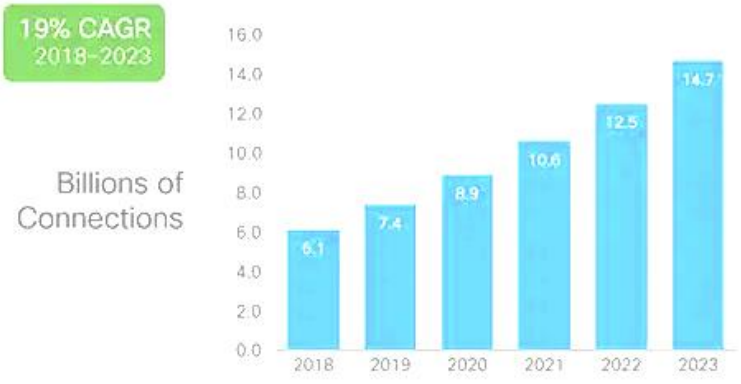
V internetu věcí dochází k nárůstu počtu chytrých a propojených objektů s nimiž jsou spojené i různé inovativní příležitosti. Každý objekt, který je součástí IoT, má atributy, díky kterým je jedinečný a odlišný od ostatních. Schopnost objektu měnit svoji povahu je jednou ze základních vlastností, díky kterým lze odlišit chytrý objekt od ostatních objektů. O inteligentním objektu lze hovořit, jako o aktivním objektu, který je schopen pracovat autonomně, může tvořit síť, je rekonfigurovatelný a má vlastní kontrolu nad svými zdroji. Některé hlavní funkce a výzvy spojené s IoT jsou popsány níže:

Heterogenita

V IoT se vyskytují různé typy zařízení, které se vzájemně ovlivňují a vytvářejí síť. Tato zařízení jsou heterogenní co do velikosti, tvaru a funkčnosti. Lze si pod tím představit malá zařízení fungující jako senzory zabudované v oblečení či obrovské stroje pracující v průmyslových linkách. Tato zařízení mají různorodé možnosti použití z hlediska komunikace a výpočtů. Společné fungování a interakce takovýchto zařízení v IoT je zásadní překážkou, kterou je třeba řešit. Ta zahrnuje vzájemnou interakci mezi zařízeními IoT, síťovou bránou a cloudem, kde se využívají různé komunikační protokoly a kde se může vyskytnout i problém s datovým formátem jednotlivých zařízení. Proto je nutné brát ohled na efektivní tvorbu architektury sítě a vybírat vhodné komunikační protokoly s ohledem na heterogenitu sítě. (5)

Škálovatelnost

IoT je mohutná síť s velkým množstvím objektů připojených ke globální informační infrastruktuře. Počet připojených zařízení se každý rok zvyšuje, což vede k problému se škálovatelností v IoT. Pro správnou komunikaci je podstatnou podmínkou jedinečnost odesílatele a příjemce, spolu s identifikací vhodné cesty nebo kanálu. Aby bylo možné identifikovat jedinečného odesílatele a příjemce, měla by koncovým zařízením být poskytnuta jedinečná globální identita. Dosud používané adresování IPv4 (32bitové adresování) nabízí pouhých 4 294 967 296 jedinečných adres. Tento počet adres není dlouhodobě adekvátní, jestliže budeme vycházet z prognózy, že počet IoT zařízeních v následujících letech několikanásobně převýší světovou populaci, jak je uvedeno níže v Obr. 2. Růst počtu zařízení povede též k vyšší zátěži komunikačních kanálů, což celkově sníží kvalitu komunikace. Proto je do budoucna potřeba zajistit dostatečně naddimenzované komunikační sítě a způsob adresování, které poskytne dostatečné množství adres s jedinečnou identifikací. (5)



Obr. 2 Graf predikce globálního růstu IoT (6)

Výměna dat

Již dnes jsou a budou lidé závislí na okamžitému přístupu k datům. Aby IoT uspokojilo tyto potřeby neomezeného přístupu k datům, bude se stále frekventovaněji využívat bezdrátová technologie. Ta umožní vzájemně propojovat izolované živé a neživé objekty. Díky této schopnosti poskytne komukoliv a čemukoliv okamžitý přístup k téměř veškerým lidským znalostem. Nezbytnou podmínkou pro bezdrátovou komunikaci je dostupnost spektra. Bezdrátové spektrum funguje jako médium pro přenos rádiových signálů. Můžeme tedy říci, že dostupnost spektra hraje důležitou roli v udržení funkční sítě. Problémem, který se dnes v bezdrátové komunikaci vyskytuje, je právě nedostupnost volného spektra, které omezuje růst oboru internetu věcí. (5)

Spotřeba energie

Zařízení, která jsou součástí sítě IoT se mohou lišit v závislosti na své aktivitě. Některá koncová zařízení fungují pouze v případě potřeby a některá mohou podle požadavků aplikace přepínat mezi aktivním režimem a režimem spánku. Koncová zařízení mohou využívat externí zdroj napájení či mohou být soběstačná a používat k napájení baterie. V případě externího napájení nejsou komunikace ani výpočty dat překážkou. Jestliže jsou však zařízení napájena z baterie, je nutné vymýšlet řešení, která mají za cíl optimalizovat spotřebu energie i třeba na úkor výkonu. (5)

Schopnost samoorganizace

IoT je pouhou sítí, o které lze říct, že je směsí statické sítě a decentralizované sítě bez pevně dané infrastruktury, tj. síť ad hoc. Zásadním rozdílem mezi oběma sítěmi je stabilita pozice jednotlivých zařízení. Ve statické síti se umístění fyzických objektů moc často nemění, což umožňuje vytvoření stabilní sítě. V případě sítě IoT se však mohou jednotlivé objekty neustále měnit. Proto vznikla síť schopná autonomního plánování, organizace a vlastní údržby. Síť internetu věcí je tedy síť ad hoc s inteligentní distribucí po celé síti. Věci zapojené do této sítě mohou neustále měnit svoji pozici a funkci. Krom toho jsou schopny pracovat autonomně tím, že reagují na širokou škálu různých situací bez vnějšího zásahu. Podle požadavků uživatele a aktuální situace se chytré uzly v IoT autonomně uspořádají do dočasné sítě ad hoc. Pomocí této přechodné sítě získávají chytré uzly schopnost sdílet svá data a provádět úkony ve vzájemné koordinaci. Výše uvedená situace zahrnuje též proces vyhledávání služeb a zařízení a automatickou konfiguraci používaných protokolů. (5)

Ochrana soukromí a zabezpečení

Podstatou internetu věcí je poskytnout konektivitu mezi koncovými zařízeními a internetem. Vzhledem k tomu, že se připojuje stále více zařízení, riziko potenciálního úniku dat či nakažení malwarem je stále reálnější. Vzhledem k tomu, že síť IoT by měla autonomně spojovat a organizovat své uzly, je vysoké riziko, že dojde k narušení bezpečnosti. Snahou o připojení cizího uzlu může dojít k infekci propojených zařízení škodlivým softwarem, a tak hrozí i únik nebo dokonce ztráta dat uložených na cloudu. Proto se v komunikačních protokolech sítí IoT klade velký důraz na zabezpečení. I přes to, že data jsou dnes relativně v bezpečí, je nutné při návrhu architektury a protokolů pro řešení IoT považovat zabezpečení za nejvyšší prioritu. (5), (7)

4.2 Automatizace domácnosti

Termín domácí automatizace má překvapivě dlouhou historii. Již na počátku 20. století tento pojem označoval způsob, jakým si lze ulehčit každodenní domácí povinnosti. V té době se prakticky všechny úklidové, opravářské či kuchyňské práce musely provádět vlastnoručně. Nicméně rozšíření elektrické sítě do více domácností odstartovalo boom v podobě prodeje strojů šetřících práci a čas. Mezi tyto stroje lze zařadit různé ohřívače vody, chladničky, šicí stroje, myčky, pračky a sušičky prádla. (8)

Technologické možnosti se během 20. století rok od roku rozšiřovaly a v závislosti na tom se změnila i představa moderní domácnosti a poprvé se objevila možnost setkat se s pojmem automatizovaná domácnost tak, jak ji chápeme i dnes. Její součástí jsou nyní spotřebiče ovládané automaticky, bez lidského zásahu, pomocí časovačů, senzorů a v neposlední řadě i počítačů. (8)

V důsledku další modernizace je dnes možné minimalizovat velikost počítačů a díky tomu je integrovat do objektů kolem nás a tím z nich udělat tzv. chytré věci, které jsou nedílnou součástí internetu věcí. Na rozdíl od běžné automatizace, chytré věci mají schopnost se adaptovat a přizpůsobovat své úkony v závislosti na získaných datech z dlouhodobého provozu. V ideálním případě by chytré věci měly být schopny fungovat autonomně bez zásahu uživatele. Po integraci těchto zařízení do domácnosti lze tvrdit, že jde o tzv. chytrou domácnost. (9)

Je nutné podotknout, že záleží čistě na uživateli, jestli využije plný potenciál konceptu chytré domácnosti. Chytrá domácnost je pokročilým nástrojem, který umožňuje automatizovat různé úkony, nicméně nemusí být nutně tímto způsobem využívána. Proto lze konstatovat, že chytrá domácnost není nutně automatizovaná domácnost. Stejně tak je možné tvrdit, že automatizovaná domácnost nemusí být chytrou domácností. (8), (9)

V tomto kontextu se tak dá narazit na termín „propojené objekty“ či „propojená domácnost“ (z angl. connected things), v jejichž případě zařízení mezi sebou pouze komunikují a jinak neplní žádné další pokročilé funkce. Typickým příkladem může být klasický vypínač na světlo propojený s internetem. Prostřednícím svého smartphonu světlo lze pouze zapnout a vypnout, ale nelze očekávat další funkce v podobě například analýzy četnosti rozsvícení světla. (10)

5 Výběr komunikačních technologií a jejich specifikace

Veškeré objekty v internetu věcí potřebují vzájemně komunikovat a sdílet mezi sebou informace. Tato komunikace může probíhat mezi dvěma a více zařízeními nebo mimo lokální síť s vnějším světem prostřednictvím globální sítě internet. Komunikace je možná pouze v případě, že zařízení má specifický modul určený pro drátovou či bezdrátovou komunikaci. Tento modul se řídí souborem pravidel obecně nazývaných protokoly pro sdílení informací v síti. Modul konkrétně využívá komunikační protokoly na nižší fyzické úrovni referenčního modelu OSI, které jsou zodpovědné pouze za samotný přenos dat. Nespecifikují však co konkrétní data reprezentují a jak s nimi nakládat. To zajišťují aplikační protokoly vyskytující se ve vyšších vrstvách modelu OSI. (5)

U každého typu komunikace lze nalézt určité výhody a nevýhody jeho používání. Obecně lze však říct, že neexistuje všestranně efektivní způsob komunikace, a proto je třeba vybírat vhodnou komunikační technologii na základě konkrétní situace a preferovaných vlastností přenášených dat.

Lze rozdělit způsob komunikace do dvou základních kategorie, tj. na přenos informací bezdrátově či prostřednictvím kabelu. Protože IoT sítě jsou především založené na větším počtu zařízení, použití kabelu jako komunikačního média je finančně náročnější a z hlediska užití i značně nepraktické. Obvykle se kabelové rozhraní (např. Ethernet nebo optická vlákna) používá jako fyzická vrstva pro připojení řídícího zařízení na internet. Existují však případy, kdy je užití kabelů preferované kvůli potřebě spolehlivé komunikace v pro signál nepříznivém prostředí. Převážně se jedná o průmyslová řešení, kde se často využívají různé varianty sériových linek. (11)

V případě bezdrátové komunikace, přenos probíhá převážně prostřednictvím rádiového záření, kdy každá technologie může využívat různé vlastnosti rádiových vln. Základní podmínkou pro přijetí a odeslání dat je přítomnost rádiových vln schopných cestovat na vzdálenost od vysílače k přijímači. Proto byla vyvinuta řada technologií s rozdílnými vlastnostmi. Mohou se například lišit vlnovou frekvencí, od které se následně odvíjí přenosová vzdálenost, energetická náročnost, šířka pásma či latence. (11)

Vlastnosti vlnových frekvencí při přenosu určuje řada pravidel vymezených telekomunikačními úřady po celém světě. V první řadě je nutné zmínit, že existují licencovaná a nelicencovaná frekvenční pásma. K vysílání v licencovaných pásmech je nutné získat určitá oprávnění od místního telekomunikačního úřadu, což může být časově a finančně náročný proces, který navíc nemusí vždy dopadnout pozitivně. Tato pásma využívají například mobilní operátoři, internetoví provideři, televize, rádiový rozhlas či slouží k různé prioritní komunikaci. Proto byla pro běžné uživatele vymezena nelicencovaná pásma, též nazývaná pásma ISM, na kterých lze vysílat bez nutného oprávnění. Komunikace v nelicencovaných frekvenčních pásmech nicméně s sebou nese řadu nevýhod. Kvůli tomu, že jej využívá značné množství zařízení, je často v městských oblastech pásmo ISM zaplněno, a tím dochází k vzájemnému rušení při vysílání. Aby se tomuto rušení alespoň částečně zamezilo, jsou vysílací zařízení limitována vysílacím výkonem, který se vyjadřuje prostřednictvím EIRP, ekvivalentně izotropního výkonu záření. Orientační vlnové frekvence pásem ISM a maximální vyzářené výkony jsou v Tab. 2 – mohou se lišit podle vysílacích norem příslušných států. (11)

Tab. 1 Frekvenční pásma ISM v MHz a maximální EIRP v mW (11)

FREKVENČNÍ PÁSMO [MHZ]	MAXIMÁLNÍ EIRP [MW]
13,5530 – 13,5670	100/500
40,66 – 40,70	100/500
433,05 – 434,79	50/100
863–870	25
2 400 – 2 500	500
5 725 – 5925	500
24 000 – 24 250	500
59 300 – 62 000	500/1000
122 020 – 123 000	500/1000
244 000 – 246 000	500/100

Signál s nižší vlnovou frekvencí se z pravidla lépe šíří a má větší dosah. Vezmeme-li však v potaz nastavené vysílací limity, v praxi toto pravidlo nemusí vždy platit. Proto se můžeme setkat s protokoly, které využívají stejné frekvence, ale mají diametrálně odlišné vzdálenosti přenosu. (11)

V následujících sekcích jsou stručně popsány komunikační protokoly zařazené do skupin podle jejich vlastností. Výběr byl proveden na základě analýzy četností použití jednotlivých komunikačních standardů získaných z portálu iot-analytics.com. Je podstatné zmínit, že konkrétně komunikační technologie se v tomto rychle vyvíjí, a proto je pravděpodobné, že v budoucnu níže popsané protokoly budou nahrazeny novými a dokonalejšími. (12, 13)

5.1 LPWAN

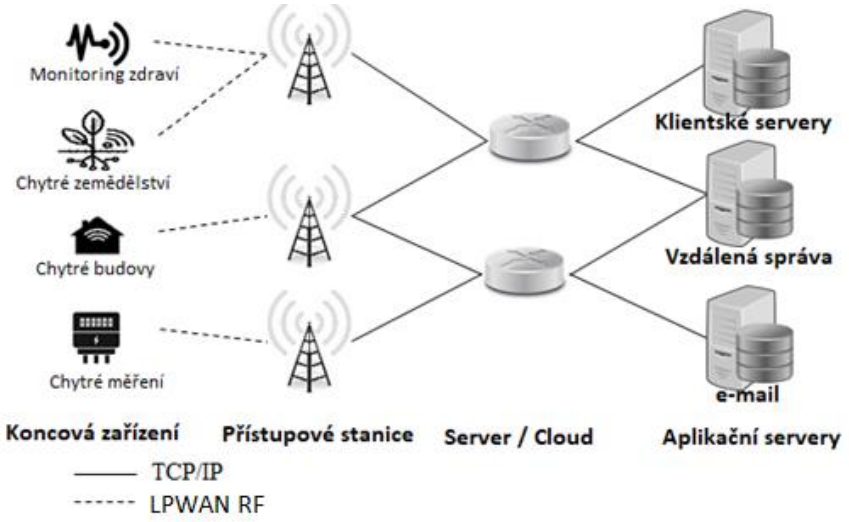
LPWAN je souhrnný název pro technologie umožňující přenos dat s vysokou energetickou účinností na dlouhé vzdálenosti za příznivou cenu. Pro tyto sítě, jak je vidět v Tab. 2, je typické přenášet malé objemy dat s nízkou přenosovou rychlostí v nepravidelných intervalech. Přenášet data lze na krátké vzdálenosti od desítek centimetrů a na dlouhé až do vzdálenosti 5 km v obytných oblastech a v otevřeném terénu až na 40 km. Sítě LPWAN typicky využívají rádiové frekvence v rozmezí 800–900 MHz. Díky nižší frekvenci lze vysílat s nižší energetickou náročností, a proto se koncová zařízení nemusí nutně zapojovat do elektrické sítě a vystačí si pouze s vyměnitelnou baterií. Obvykle největší vliv na výdrž baterie má právě způsob komunikace a její četnost. (14), (15)

Tab. 2 Vlastnosti technologií LPWAN (16, 17)

KOMUNIKAČNÍ PROTOKOL	FREKVENCE	ISM	VZDÁLENOST PŘENOSU	MAXIMÁLNÍ RYCHLOST PŘENOSU
SIGFOX	868 MHz (EU) 906 MHz (US)	ANO	50 km	1 kbps
LORA	169 MHz, 433 MHz, 868 MHz (EU) 915 MHz (US)	ANO	15 km	50 kbps
NB-IOT	1800 MHz, 900 MHz, 800 MHz (EU)	NE	15 km	20 kbps (uplink) 200 kbps (downlink)

WHITE-FI (IEEE 802.11AF)	470–790 MHz	NE	3 km	24 Mbps
HALOW (IEEE 802.11AF)	750–928 MHz	ANO	1 km	100 Mbps

Klasická architektura LPWAN vyžaduje bezdrátový přístup a možnost konektivity na internet a cloud. Základní funkcí LPWAN zařízení je shromažďování dat, jejich odesílání a reagování na příkazy ze sítě LPWAN. Shromážděná data se obvykle odesílají pomocí specifického rádiového spojení do nejbližší stanice odkud dále putují do sítě IoT – viz. Obr. 3. Nejčastější topologií koncových zařízení v sítích LPWAN je hvězda, kde spolu jednotlivá zařízení komunikují skrze jednu společnou stanici. Stanice zajišťují integritu rádiového spojení manipulací s přijatelnou bitovou chybovostí. Za řízení a provoz komunikace mezi zařízením a klientem zodpovídá cloud poskytovatele LPWAN. Ten konkrétně spravuje kanál pro výměnu informací mezi stanicí a sítí IoT a překlad mezi protokoly využívanými stanicí na jedné straně a na straně druhé samotnou sítí. (15)



Obr. 3 Architektura sítí LPWAN (18)

Z hlediska pokrytí a četnosti použití se v České republice vyskytují tři významné typy LPWAN. Sigfox od společnosti SimpleCell využívající infrastrukturu T-Mobile; LoRa poskytovaná společností Česká Radiokomunikace a NB-IoT provozována na sítích LTE a 5G mobilních operátorů Vodafone a O2. V následujících sekcích jsou i komunikační protokoly IEEE 802.11af a IEEE 802.11ah. Ty nejsou zatím moc používané, nicméně do budoucna se nabízejí jako potenciální technologie. (19)

5.1.1 Sigfox

Sigfox je patentovaná úzkopásmová LPWAN technologie využívající nízké modulační frekvence k dosažení vysoké přenosové vzdálenosti. Je hojně vysílána v Evropě a je pro ni typické, že využívá nelicencovaná pásma s frekvencí pod 1 GHz. K navázání spojení se sítí Sigfox je zapotřebí zařízení opatřit komunikačním modulem s unikátním 32bitovým identifikátorem SigfoxID, který je přiřazen ke konkrétnímu modemu při jeho výrobě. K registraci zařízení je též potřeba tzv. PAC kód, který je poskytnut při koupi a po použití je kód znovu vygenerován pro dalšího případného majitele. Z tohoto důvodu k zařízení má přístup vždy pouze jeden uživatel. Z hlediska zabezpečení jsou veškerá data šifrována a podepsána privátním klíčem. (15), (19)

Specifikem sítě Sigfox jsou její striktní omezení přenosu dat. Konkrétně se jedná o její přenosovou rychlost omezenou na pouhý 1 kbps, stanovení 144 zpráv jako maximum možných odeslaných zpráv za den, velikost uživatelské zprávy do 12 bajtů a limit vysílacího výkonu na 25 mW. Díky těmto limitům mají zařízení využívající Sigfox velmi malou spotřebu energie a příznivé pořizovací náklady. Komunikace je jednosměrná a od serveru ke koncovému zařízení se uskuteční pouze na vyžádání zařízení. (19), (16)

5.1.2 LoRA

Technologie fyzické vrstvy LoRa je stejně jako Sigfox v evropském nelicencovaném pásmu pod 1 GHz. Zásadním rozdílem je, že LoRa umožňuje obousměrnou komunikaci zprostředkovanou pomocí metody modulace rádiového rozprostřeného spektra umožňujícího rychlosti přenosu dat od 300 bps až po 50 kbps v závislosti na prostředí a nastavené šířce pásma. (15)

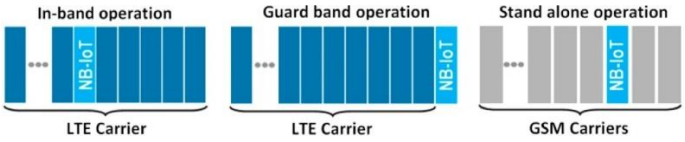
Komunikační protokol založený na LoRa s názvem LoRaWAN byl standardizován LoRa-Alliancí a slouží ke komunikaci mezi koncovými zařízeními a základovými stanicemi, které následně odesílají data prostřednictvím 3G či Ethernetu na cloud. Odtud mohou být dále zpracována vlastníkem zařízení. Výhodou technologie LoRa v porovnání se SigFox je její flexibilita. LoRa umožňuje nasazení lokálních sítí prostřednictvím LoRa gateway, které poskytují stejné možnosti bezdrátové sítě jako sítě od poskytovatelů připojení využívajících základové stanice. (19), (20)

Z hlediska zabezpečení se při komunikaci v síti využívá systém dvou šifrovaných klíčů 128bitovými šiframi. Přičemž jeden klíč vlastní provozovatel sítě a druhý koncový zákazník. Každé koncové zařízení by mělo podléhat certifikaci a v případě provozu sítě Českou Radiokomunikací je možné přihlásit výhradně certifikovaná zařízení. (19)

5.1.3 NB-IoT

NB-IoT je poměrně nová a ambiciózní technologie umožňující obousměrnou komunikaci. Byla standardizována organizací 3GPP v roce 2016. Její specifickou vlastností je, že dovede koexistovat na již vystavené infrastruktuře vysílacích stanic s pásmy GSM a LTE. Její alternativou je komunikační protokol LTE-M, který má podobné vlastnosti, ale dovede využít pouze pásma LTE. Faktem je, že samotná 3GPP doporučuje integrovat právě NB-IoT do všech stávajících sítí GSM i LTE. K jejímu nasazení do provozu postačí pouhá aktualizace softwaru ve stávajících základových stanicích. (15), (20)

Dalším důvodem pro nasazení NB-IoT je, že dovede fungovat v několika operačních režimech využívajících různé části pásma – viz. Obr. 4. V In-band režimu NB-IoT využívá minimálně jeden rádiový blok, tedy minimálně 200 KHz v rámci pásma, které právě využívá LTE. Režim Guard band umožňuje použít a vyplnit oddělující vrstvy mezi jednotlivými frekvenčními pásmy LTE a tím nezmenšuje jejich šířku pásma. Posledním je Stand alone režim, který umožňuje provozovat NB-IoT ve frekvenčním pásmu nevyužívaném LTE, ideálně v pásmu GSM, které má též šířku frekvence 200 KHz a postupně se od něj odstupuje. (20)



Obr. 4 Operační režimy sítě NB-IoT (20)

V případě koncového zařízení platí, že k jeho připojení do sítě NB-IoT je, kromě modemu, potřeba i SIM karta. Rychlost přenosu pro downlink je omezen na 200 kbps a pro uplink na 20 kbps. Maximální velikost jedné zprávy je 1600 bajtů. Pro vyšší výdrž a větší konektivitu stanovila 3GPP tři různé výkonnostní třídy (Power Class x). Power Class 3 nabízí výkon 23 dBm, Power class 5 má nižší výstupní výkon 20 dBm. Poslední a nově přidanou třídou je Power Class 6, která nabízí nejnižší výkon, a to pouhých 14 dBm. V závislosti na použité třídě se ovlivňuje odběr energie, dosah komunikace a v některých případech má vliv i na kompatibilitu zařízení. (21)

5.1.4 IEEE 802.11af

IEEE 802.11af je standard, který upravuje standard 802.11 známý též jako Wi-Fi, pro provoz v televizním pásmu tak, aby se zvýšil vysílací dosah a tím se vyřešil problém s přetížením vysílacího spektra a zvýšila se energetická úspora při vysílání. Tato verze konkrétně umožnuje přenášet data s maximální rychlostí až 24 Mbps na vzdálenost do 3 km. Nicméně v praxi tolik dat nepřenese, neboť vysílání trvá pouhé setiny sekundy. Protože IEEE 802.11af využívá licencovaná frekvenční pásma v rozmezí 470–790 MHz, která se nazývají mimo jiné bílým prostorem (z angl. White space), dostal označení White-Fi. Méně často se lze setkat i s označením superWiFi. Zajímavostí tohoto protokolu je, že dovede během přenosu dynamicky měnit kanál a tím snížit riziko kolize s jiným vysíláním. (22)

5.1.5 IEEE 802.11ah

Podobně jako u IEEE 802.11af je hlavním cílem standardu IEEE 802.11ah známého též jako HaLow nízká spotřeba energie pro koncová zařízení. Tento standard používá nelicencovaná frekvenční pásma pod 1 GHz, díky čemuž dovede přenášet data i skrz větší překážky stejně jako White-Fi. Taktéž podporuje připojení většího množství uzlů. Za účelem snížení doby přenosu a spotřeby energie během komunikace se přenáší krátké datové pakety. HaLow je schopnen přenášet data s rychlostí až 100 Mbps na vzdálenost do 1 km. I v tomto případě je však vysílací doba v setinách sekundy. Přístupové body užívající HaLow mohou teoreticky podporovat kromě pásem pod 1 GHz i pásma 2,4 a 5 GHz, což umožní připojovat i běžná zařízení využívající standardy Wi-Fi. (5)

5.2 Sítě krátkého dosahu

Sítě krátkého dosahu (SRN) jsou využívané v případech, kdy není zásadní velká přenosová vzdálenost. Jak si lze všimnout v Tab. 3, existuje poměrně velký rozdíl ve vlastnostech těchto standardů. Většina protokolů využívá frekvence v pásmech ISM a mají různou energetickou spotřebu. V závislosti na spotřebě energie se odvíjí i možnost napájení pomocí baterie. V případě technologií SRN je často využívaná hvězdicová, P2P či stromečková topologie. Existují však protokoly, které využívají topologii typu mesh. Ta má oproti klasickým topologiím řadu zajímavých vlastností, které mohou být pro IoT přínosem.

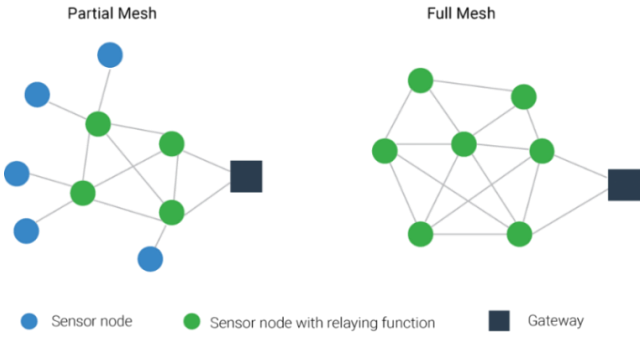
Tab. 3 Vlastnosti protokolů sítí krátkého dosahu (5, 11, 22, 23)

KOMUNIKAČNÍ PROTOKOL	KMITOČTOÉ PÁSMO	TOPOLOGIE SÍTĚ	MAXIMÁLNÍ VZDÁLENOST PŘENOSU	MAXIMÁLNÍ RYCHLOST PŘENOSU	STANDARD
ZIGBEE	868 MHz, 2,4 GHz	P2P, Mesh, Hvězda, Stromeček	10 – 100 m	167 kbps	IEEE 802.15.4
BLE	2,4 GHz	P2P, Hvězda	50 m	1–4 Mbps	IEEE 802.15.1
Z-WAVE	868 MHz	Mesh	100 m	100 kbps	-
6LOWPAN	868 MHz, 2,4 GHz	Mesh, Hvězda	10 – 100 m	250 kbps	IEEE 802.15.4
WI-FI 6	2,4 GHz, 5 GHz	P2P, Hvězda	10 – 100 m	604,4 Mbps (pro 1 kanál)	IEEE 802.11ax

Topologie mesh

Typickým znakem této sítě je její struktura, ve které je každý komponent přímo spojen se všemi ostatními komponenty v jedné síti. V praxi je bezdrátová síť typu mesh strukturou, která by měla umožňovat automatickou konfiguraci zařízeních pro spolehlivý přenos dat. (24)

Většinou se vyskytuje částečná mesh sítí, kde pouze zlomek zařízení plní funkci uzlového bodu (repeateru), přičemž zbytek zařízení funguje pouze jako koncový bod. Na Obr. 5 vlevo je schéma částečné mesh sítě, přičemž vpravo je úplná mesh síť, která plně odpovídá definici klasické mesh sítě. Součástí sítě je obvykle i zařízení plnící funkci síťové brány, která propojuje síť mesh s vnější sítí, např internetem. Toto zařízení je zpravidla připojeno na internet a proudí jím veškerá komunikace v síti. (24), (25)



Obr. 5 Schéma částečné a úplné topologie mesh (25)

5.2.1 ZigBee

ZigBee je síťový protokol založený v roce 2012 na standardu IEEE 802.15.4. Je využívaný více než 70 miliony zařízeními po celém světě především díky levnému a energeticky nenáročnému provozu. Pracuje v nelicencovaném frekvenčním pásmu pod 1 Ghz a 2,4 GHz s maximálním datovým přenosem 167 kbps a latencí do 150 ms. Udává se, že ZigBee může mít dosah až 100 m, ale záleží na použité frekvenci a prostředí. Z hlediska adresace může být teoreticky v jedné síti až 64 000 zařízení, ale z hlediska dlouhodobé únosnosti se doporučuje nepřekročovat počet 1024 zařízení v jedné síti. Spolu se síťovou topologií mesh lze utvořit i hvězdicovou, stromovou a peer-to-peer topologii. (22)

5.2.2 BLE

BLE je bezdrátová technologie využívající standardu IEEE 802.15.1, která je hojně používána v mobilních zařízeních. BLE bylo integrováno do Bluetooth 4.0 v roce 2009 a je až do součástí ve všech nových verzí. Velké množství operačních systémů, jako jsou Android, BlackBerry, IOS, Linux, macOS, Windows a další, podporují technologii BLE. Využívá nelicencované frekvenční pásmo 2,4 GHz s maximální rychlostí přenosu dat 4 Mbps na vzdálenost až 50 m. Obvyklá latence přenosu se pohybuje od 200 do 500 ms. S BLE lze poskládat zařízení i do stromové a peer-to-peer síťové topologie. (22)

5.2.3 Z-Wave

Tento síťový protokol je specifický tím, že funguje na principu Master Slave, u kterého konfigurátor (Master) posílá krátké zprávy ostatním podřadným zařízením (Slaves). Z-Wave funguje na nelicencovaných frekvenčních pásmech pod 1 GHz a udává se maximální vzdálenost přenosu 100 m. V jedné síti může být současně až 232 zařízení, která mohou

komunikovat maximální rychlostí 100 kbps. Na rozdíl od ZigBee a BLE, Z-Wave podporuje pouze topologii sítě typu mesh. (5)

5.2.4 6LoWPAN

6LoWPAN je síťový protokol založený, stejně jako ZigBee, na standardu IEEE 802.15.4. Podstatnou vlastností tohoto protokolu je, že umožňuje použití aktuálního IPv4 i nastupujícího IPv6 protokolu současně. Výhodou pro zařízení komunikující prostřednictvím 6LoWPAN je, že se dovedou přímo připojit do vícero sítí IPv4 a IPv6 jen prostřednictvím IP routeru, což při implementaci do stávajícího provozu sníží náklady. Síťový protokol využívá nelicencovaná frekvenční pásma pod 1 GHz a 2,4 GHz. V ideálních podmínkách dokáže přenášet data až do vzdálenosti 100 m. Udává se maximální datová rychlost 250 kbps s velmi nízkou latencí do 6 ms. Nicméně toho lze docílit pouze specifickou konfigurací komunikace, která má negativní dopady na spolehlivost přenosu dat. (22)

5.2.5 IEEE 802.11ax

IEEE 802.11ax je nová generace standardu 802.11 a dostal pojmenování Wi-Fi 6. Ten je primárně určen pro robustní a vysokorychlostní přenos dat s point-to-point či point-to-multipoint komunikací. V ideálních podmínkách dovede přenášet data až na 100 metrů. Obecně standardy Wi-Fi využívají frekvenční pásma 2,4 a 5 GHz, 802.11ax není výjimkou. Rozdíl je však v tom, že je schopný přenést až 600,4 Mbps a oproti předchozím generacím je lépe uzpůsobený pro internet věcí. Podstatnou novinkou tohoto standardu je vlastnost vysílat v menším vysílacím pásmu, díky čemuž lze rozdělit dosavadní vysílací kanály Wi-Fi na tzv. sub-kanály, čímž lze připojit větší počet zařízení v rámci jedné sítě a snižuje se tak šance, že dojde k vzájemnému rušení s okolními sítěmi. Další inovativní funkcí je tzv. TWT, která definuje časové intervaly k vzájemné komunikaci. V případě koncových zařízeních tato funkce dovede radikálně snížit energetickou náročnost. (22), (26)

5.3 RFID

Jako RFID se označuje bezdrátová komunikace mezi vysílačem (transpondérem nebo tagem) a přijímačem (čtečkou) využívajícím radiové vlny k pasivní identifikaci označeného objektu. Transpondér se skládá z antény (často cívka), čipu a nosného materiálu nebo krytu. Čip je vybaven analogovými a digitálními obvody a pamětí, která uchovává unikátní ID zařízení. Tagy

se vyrábí v mnoha provedeních. Můžou se lišit v rozměrech, tvaru, životnosti, funkční frekvenci nebo velikosti paměti. (27)

Tagy využívají pro svoje fungování specifické nelicencované frekvence. V závislosti na frekvenci lze docílit určitých vlastností tagu. Tagy, jak je vidět v Tab. 4, s frekvencí 125-135 KHz a 13,56 MHz jsou levné, nepotřebují baterii a lze je bezchybně číst i skrze některé materiály. Přenos dat je nicméně pomalý a na vzdálenost maximálně jednoho metru. Tagy s frekvencí 868-930 MHz, 2.45 GHz a 5.8 GHz mají vyšší přenosovou rychlost a mohou mít dosah až 30 m. Nevýhodou je, že ke čtení je potřeba cenově náročnější čtečka, na vyšší vzdálenost je potřeba dodat zdroj elektřiny pro transpondér a vlny s vyšší frekvencí mají problém s průchodem skrz materiály. (28)(29)

Každý tag má ve své paměti dva identifikační prvky. Prvním je unikátní identifikační číslo zařízení, které nelze měnit a je přiřazeno při výrobě. Druhým Auto-ID, které lze editovat pomocí čtečky konstruované speciálně k zápisu dat. (28)

Tab. 4 Vlastnosti RFID tágu závislosti na jejich frekvenčním pásmu (29)

FREKVENČNÍ PÁSMO	PŘENOS DAT	VZDÁLENOST PŘENOSU	NAPÁJENÍ
125–134 KHZ	Nízká rychlost čtení, data do 16bitů	Do 1,5 m	Není
13,56 MHZ	Střední rychlost čtení, střední objem přenosu dat	Do 1 m	Není
433 MHZ	Vysoká rychlost čtení, velký objem přenosu udat	Do 300 m	Volitelné
860–960 MHZ	Vysoká rychlost čtení, velký objem přenosu udat	Do 9 m	Je potřeba
2,45 GHZ A 5,4 GHZ	Vysoká rychlost čtení, velký objem přenosu udat	Do 90 m	Je potřeba

NFC

NFC je jedním z typů komunikačních protokolů RFID pro peer-to-peer rádiovou komunikaci prostřednictvím tzv. indukční vazby. Indukční vazbu lze přirovnat vzdáleně k principu transformátoru, kdy magnetické pole dvou cívek slouží ke spojení inicializačního a cílového zařízení. S touto technologií se lze setkat v praxi u bezkontaktních plateb uskutečněných pomocí telefonu.

Pro NFC existují dvě hlavní specifikace: ISO/IEC 14443 a ISO/IEC 18000-3. První definuje ID karty používané k ukládání informací, které jsou součástí například v NFC tagů. ISO/IEC 18000-3 specifikuje RFID komunikaci na frekvenci 13,56 MHz používanou zařízeními s funkcí NFC. Obvykle se udává maximální rychlost přenosu do 106 kbps do vzdálenosti 4 cm, částečně lze přenášet s menší spolehlivostí až 424 kbps. (30)

6 Výběr cloudových IoT platforem a jejich specifikace

IoT je o senzorech, sítích a široce distribuovaných chytrých zařízeních s omezenou kapacitou úložiště a výpočetním výkonem, s vyskytujícími se reálnými bezpečnostními problémy Jak už bylo řečeno, výstupem početného množství zařízení jsou Big Data, u kterých je nutné najít efektivní způsob jejich zpracování.

Nabízí se proto ideální řešení v podobě cloud computingu, který poskytuje decentralizované virtuální služby jako jsou neomezené úložiště či výpočetní výkon. IoT a cloud computing jsou neoddělitelné technologie a pracují současně s cílem zvýšit efektivitu každodenních úkonů. IoT produkuje nepřetržitě velké množství dat a cloud computing dává těmto datům smysl a též k nim poskytuje uživatelům cestu v reálnem čase. Kromě toho poskytuje vzdálený výpočetní výkon, díky kterému nemusí koncová zařízení mít zbytečně výkonný hardware, což vede i ke snížení nákladů. Cloud umožnuje též snadnou škálovatelnost jak v případě výpočetní kapacity, tak i paměti. V případě komunikace v internetu věcí cloud funguje jako prostředník, a tak usnadňuje komunikaci mezi zařízeními. V neposlední řadě umožňuje vyšší úroveň zabezpečení a ochrany dat, než jakou by byl běžný uživatel schopný zajistit.

Cloud v použité architektuře IoT tvoří třetí vrstvu. Součástí této vrstvy jsou též aplikační protokoly (HTTP, MQTT), které jsou použity k odeslání dat do aplikací. Cloud je tedy místem, kde se data uchovávají a zpracovávají se do podoby, která je použitelná pro koncovou aplikaci ovládanou uživatelem.

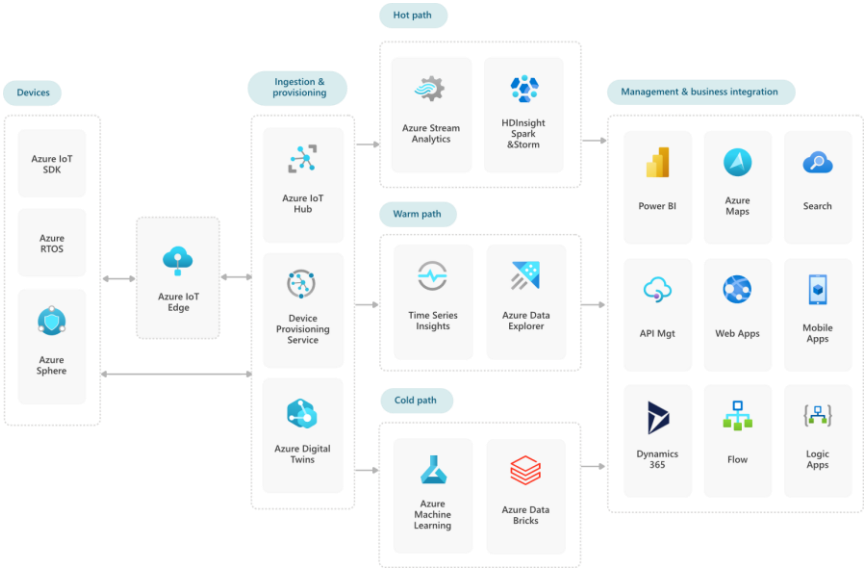
Existuje široká řada komerčních i opensourceových cloudových platforem vhodných pro integraci do internetu věcí, na které zde není prostor. V následujících sekcích a Tab. 5 jsou tři největší zástupci, kteří aktuálně podle portálu iot-analytics.com společně tvoří téměř 80 % globálního trhu s cloudovými IoT platformami. (31)

Tab. 5 Vlastnosti vybraných cloudových IoT platforem (32–34)

PLATFORMA	AZURE IOT HUB	AMAZON IOT CORE	GOOGLE IOT CLOUD
ZÁKLADNÍ FUNKCE	Konektivita Autentizace Monitoring zařízení Správa zařízení	Konektivita Autentizace Modul pravidel Vývojové prostředí	Konektivita Správa zařízení
CENA	Úroveň Basic: 12-600 $ za balíček se základními funkcemi měsíčně Úroveň Standard: 30-3000 $ za balíček s pokročilými funkcemi měsíčně (cena balíčku se odvíjí od počtu odeslaných zpráv)	0,08 $ za milion minut konektivity 0,7-1 $ za milion zpráv 1,25 $ za milion operací 0,15 $ za milion aktivací pravidel	0,00045 – 0,0045 $ za MB přenesených dat
KOMUNIKAČNÍ PROTOKOLY	HTTP MQGT AMGP WebSockets	HTTP MQTT WebSockets	HTTP MQTT
ZABEZPEČENÍ	X.509/TLS	X.509 a kognitivní identifikace AWS	X.509/TLS

6.1 Microsoft Azure

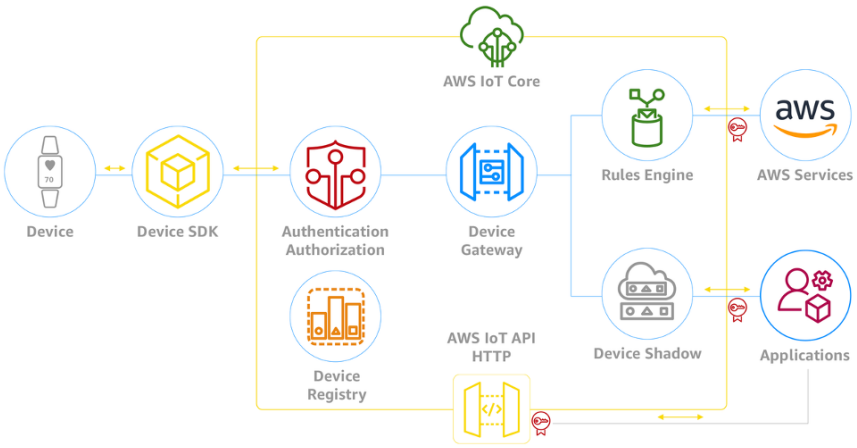
Azure je komerční platforma nabízená společností Microsoft, která nabízí velkou škálu aplikací prostřednictvím různých rozšiřitelných komponentů, díky kterým lze vytvořit celý funkční diagram IoT řešení – viz. Obr. 6. Azure též podporuje široké spektrum operačních systémů a programovacích jazyků (C, Node.js, Python, Java, .NET). Zařízení IoT interagují s cloudem prostřednictvím služby Azure IoT Hub a brány, která umožnuje agregaci, ukládání a předávání dat s centrální jednotkou. Data ze zařízení jsou uložena v cloudu a lze je analyzovat i pomocí strojového učení vyvinutého firmou Microsoft. Umožňuje též virtualizovat a sledovat data v reálném čase. (5)



Obr. 6 Diagram architektury služeb Microsoft Azure pro IoT (35)

6.2 Amazon Web Services IoT Core

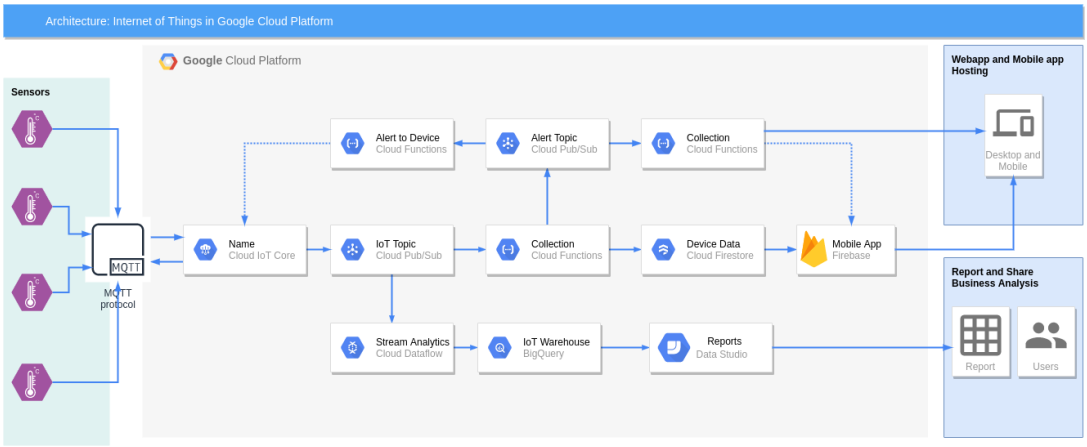
AWS IoT core je jedna ze služeb cloudové platformy vyvinuté a poskytované společností Amazon pro internet věcí. AWS a Azure jsou veřejností v rámci cloud computingu často skloňovaná jména. AWS stejně jako Azure podporuje řadu programovacích jazyků (C, Node.js, Arduino). Nejzajímavější funkcí AWS je však schopnost pracovat i se zařízeními, která jsou offline – díky službě IoT Device Shadow service. AWS jako součást své platformy nabízí řadu zpoplatněných dodatečných služeb například pro výpočty (Lambda, EC2), pro úložiště (Amazon S3), databáze (DynamoDB), strojové učení (Amazon DeepLens), či pro analýzu dat (kineze). Níže uvedený diagram architektury znázorňuje příklady různých služeb AWS, které lze při zpracování dat využít. (5)



Obr. 7 Schéma architektury komponentů AWS IoT Core (36)

6.3 Google Cloud IoT

Google Cloud Platforma je vyvinuta společností Google a využívá možností více než 100 cloudových služeb firmy Google jako jsou např. Cloud Dataflow, BigQuery, Data Studio či Datalab. Nicméně pouze jediná služba Google Cloud IoT Core je skutečně zaměřená na IoT a na rozdíl od svých konkurentů neposkytuje další IoT služby, jako je např. IoT Analytics v případě Amazon Web Services. Google Cloud IoT Core je rozdělena do dvou modulů. Jedním modulem je Správce zařízení, který umožňuje nastavení autentifikace, konfigurace a ovládání individuálních zařízení. Druhým modulem je Protokolová brána, která zajišťuje konektivitu s aplikacemi prostřednictvím protokolů MQTT či HTTP. Jednou z velkých výhod IoT platformy od společnosti Google je, že lze integrovat správu sítě IoT do populárních Map Google. Stejně jako u konkurence, i zde lze vytvořit vlastní architekturu zpracování dat pomocí Google služeb naznačenou na Obr. 8. (31)



Obr. 8 Diagram architektury služeb Google Cloud platformy pro IoT (37)

7 Výběr hardwaru pro domácí automatizaci

V současnosti je na trhu řada řešení umožňujících implementaci internetu věcí do procesu domácí automatizace. Vhodným nástrojem mohou být různé programovatelné stavebnice a SDK, u kterých je potřeba tvorba vlastních obvodů a softwarového řešení. V takovém případě se nejčastěji využívají mini počítače Raspberry Pi a mikrokontrolery Arduino. Další možností je koupě hotových zařízení nebo využití služeb firem, které zajišťují celkovou instalaci IoT pro automatizaci na míru.

Vzhledem k široké variaci možností řešení pomocí programovatelných stavebnic, které by bylo příliš rozsáhlé na její pokrytí, je aktuální kapitola zaměřená především na hotová zařízení. Obvykle při zhotovení domácí sítě IoT z produktů v podobě hotových zařízení je třeba brát v úvahu vhodný výběr hubu a koncových zařízení.

7.1 Hub

Primární funkcí hubu funkcí je spojovat a překládat protokoly mezi koncovými zařízeními a cloudem. Z pravidla po připojení hubu k routeru lze posléze postupně přidávat libovolná zařízení do této sítě. Zásadním problémem při výběru vhodného hubu je kompatibilita s koncovými zařízeními. Ke vzájemné komunikaci mezi zařízeními a hubem se nejčastěji využívají komunikační protokoly ZigBee a Z-Wave, které spolu nelze kombinovat.(38)

Zařízení a senzory po zprovoznění sítě lze ovládat a monitorovat díky aplikacím, které většinou poskytuje samotný výrobce hubu či koncových zařízení. I zde však může dojít k nekompatibilitě, kvůli použití zařízení od různých výrobců, kteří používají odlišné aplikace. Řešením může být vlastní realizace pomocí různých cloudových IoT platforem, či využití platforem třetích stran jako jsou Google Assistant, Amazon Alexa či Apple HomeKit. V případě těchto aplikací je kompatibilita zaručena pouze u certifikovaných výrobků. (38)

Možnou výhodou při použití výše zmíněných aplikací je, že firmy, které za jejich vývojem stojí, nabízí pro své aplikace další možnosti v podobě chytrých asistentů s hlasovým ovládáním často v podání reproduktoru či tabletu. Ty obvykle dovedou dále komunikovat s dalšími zařízeními pomocí Wi-Fi nebo Bluetooth. Nicméně aktuálně postrádají českou lokalizaci, a proto hlasový asistent pro místní uživatele nemá takové uplatnění.

Vybrané příklady hubu

Na trhu je široky výběr hubů od různých firem. Nicméně kromě využívaného komunikačního protokolu, počtu možných připojených zařízení a podpory platforem se nijak zásadně ve svých vlastnostech neliší. Všechny plní stejnou funkci a jsou limitovány pravidly daného komunikačního protokolu. Proto hlavními parametry při výběru technologie jsou v tomto případě uživatelské recenze a použitý komunikační protokol.

7.1.1 Philips Hue bridge

Philips Hue bridge využívá systém Philips Hue, který je vyvinut především pro pokročilou správu sítí chytrých žárovek Philips. Vzhledem k jeho oblíbenosti se však jeho podpora rozšířila i pro jiná zařízení i od široké škály různých výrobců. Konkrétně zařízení Hue bridge využívá síť Zigbee a umožňuje připojit až 50 zařízení. Podporuje aplikace Amazon Alexa, Google Assistant, Apple HomeKit a Microsoft Cortana. Kromě napájení má zdířku na Ethernet. Z oficiálního obchodu jej lze pořídit za 55 €. (39)

7.1.2 Thinka for Z-Wave

Thinka je hub fungující na komunikačním protokolu Z-Wave a umožňuje kompatibilitu až se 3000 různými zařízeními využívajícími protokol Z-Wave. Výrobce neposkytuje vlastní aplikace a rovnou odkazuje na Apple HomeKit, Google Assistant a Amazon Alexa a Olisto. Výrobce dále udává, že se lze na tento hub připojit až se 700 zařízeními. Cena zařízení je 429 €. (39)

Obr. 9 Philips Hue Bridge a Thinka for Z-Wave (40, 41)

7.2 Koncová zařízení

Koncová zařízení komunikují s centrální jednotkou či hubem a mohou buďto sloužit jako senzory a měřit veličiny, nebo slouží jako akční členy, které vykonávají různé úkony. Ve zvolené architektuře IoT jej lze nalézt jako první prvek vytvářející data, která se dále zpracovávají – viz. sekce 4.1.1. Zařízení komunikují prostřednictvím vícero typů protokolů. Jak

už bylo řečeno v předešlé sekci, obvykle se využívají protokoly Zigbee a Z-Wave. Často se však využívají i protokoly Wi-Fi, u kterých není potřeba vlastnit dodatečný hub.

Na trhu je široká variace provedení koncových zařízení s různými funkcemi, obvykle se označují jako chytrá zařízení. Součástí sítě IoT mohou být i různé chytré spotřebiče jako je lednička, kávovar, pračka či horkovzdušná trouba. Obvykle se však využívají zařízení v podobách jako například:

- Chytré žárovky – často umožňují nastavení jasu, teplotu bílého světla nebo barvu.
- Chytré zásuvky a termostaty – kromě tradičních funkcí, některé modely umožňují i měření spotřeby energie.
- Bezpečnostní systém – senzory pohybu, kouře, plynu, alarmy.
- Různé typy senzorů – snímače teploty, tlaku, vlhkosti, CO2, meteostanice.
- Chytrý kamerový systém – posílá data na základě určitého podnětu.

8 Analýza aplikačních možností vybraných technologií v domácí automatizaci

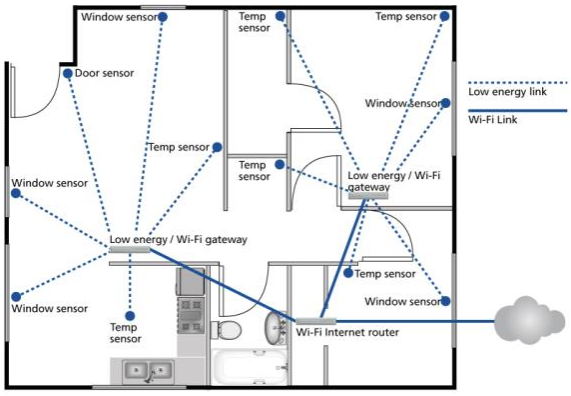
Součástí kapitoly je porovnání vybraných technologií v rámci jejich aplikačních možností. Dalším cílem je vybrat nejvhodnější technologii pro domácí automatizaci a co možná nejobjektivněji popsat důvody jejího výběru.

8.1 Analýza aplikačních možností bezdrátových komunikačních technologií

Bezdrátovou komunikační technologie jsou v této sekci rozdělené do stejných skupin jako v kapitole 5. Protože technologie v těchto skupinách mají podobné vlastnosti, lze usuzovat, že budou mít i podobné možnosti použití.

8.1.1 Aplikační možnosti sítí krátkého dosahu

Společnou vlastností této skupiny komunikačních protokolů je malá vzdálenost přenosu, a proto zařízení, která využívají tuto technologii, nesmí být příliš vzdálená od své centrální jednotky. Centrální jednotka může být v podobě gatewaye či hubu, který je připojený k internetu – viz. Obr. 10. Z toho vyplývá, že komunikační protokoly z této skupiny lze využívat pouze na místech, kde je zajištěný přístup na internet. S vědomím tohoto faktu lze nyní začít uvažovat o aplikačních možnostech sítí s krátkým dosahem.



Obr. 10 Příklad domácnosti využívající komunikační protokoly krátkého dosahu (42)

ZigBee, Z-Wave a 6LoWPAN

Tyto technologie sdílí společné rysy komunikace. ZigBee, Z-Wave i 6LoWPAN jsou schopny nízkoenergetické komunikace za cenu množství a rychlosti přenosu dat. Díky tomu, že jsou schopny provozu pouze z napájení baterie a dovedou tvořit mesh sítě, jsou tyto protokoly obecně vhodné ke komunikaci většího množství zařízení v uzavřených prostorech s omezeným

dosahem signálu. Pro představu lze využít například termostaty jako aktivní prvky, které rozšiřují síť. Koncová pasivní zařízení pak mohou být senzory teploty pro následnou regulaci teploty v místnosti. V praxi jsou ZigBee i Z-Wave hojně užívány při zřizování domácího internetu věcí, naopak 6LoWPAN je díky snadné implementaci využívaný především v průmyslu a dopravní logistice.

IEEE 802.11ax

Komunikační protokol IEEE 802.11ax je schopný operovat ve více režimech, kdy jej lze použít k přenosu velkého objemu dat z IP kamer či k připojení většího počtu nízkoenergetických zařízení. Díky svému frekventovanému výskytu a interoperabilitě se zdá být ideálním prostředkem ke komunikaci mezi zařízeními. Protože však využívá frekvence 2,4 a 5 GHz, tak stejně jako předchozí standard má horší šíření signálu skrze překážky, a tudíž má ve vnitřních prostorech menší dosah. Na rozdíl od předešlých protokolů samotná zařízení nevytváří mesh síť, a tak je potřeba pro rozšíření dosahu používat opakovače signálu. Vzhledem k tomu, že tato technologie je relativně nová, zařízení podporující tento standard jsou oproti zařízením využívajícím starší standardy nákladnější. Navíc nelze 802.11ax implementovat do stávajících sítí a je nutné pořídit nový hardware podporující tento protokol. I přes lehce nákladnější implementaci, lze Wi-Fi 6 doporučit jako vhodnou komunikační technologii při zřizování internetu věcí v domácnosti. Dosud však není mnoho koncových zařízení, které by 802.11ax podporovalo.

BLE

Díky svým vlastnostem se BLE osvědčilo především v nositelných zařízeních k monitorování životních funkcí. Jakožto energeticky nenáročný komunikační protokol je též však vhodnou technologií ke komunikaci s koncovými prvky. Ke svému fungování bude však potřeba hubu, který bude komunikaci překládat.

8.1.2 Aplikační možnosti LPWAN

Komunikační technologie LPWAN mají užití především v situacích, kdy není snadný přístup k internetu nebo je nutná dlouhodobá energetická soběstačnost koncových prvků. Protože obvykle je připojení k sítím LPWAN zpoplatněno, bylo by v rámci jedné domácnosti finančně náročné připojovat větší množství zařízení. Typicky se sítě LPWAN využívají v dopravě, ke sledování provozu, v zemědělství, při monitorování vlastností půdy a lokaci zvířat, nebo

k detekci přírodních katastrof. LPWAN má mnohé využití, z hlediska domácí automatizace je však výhodnější využít sítí krátkého dosahu, neboť mohou vysílat častěji a tím zajistit větší množství aktuálnějších dat. Kromě toho není potřeba vynakládat další finanční prostředky na přístup k síti u připojených zařízení.

Navzdory zmíněným nedostatkům se však najdou aplikace sítí LPWAN pro domácnosti. Vhodné může být jejich použití v situaci, kdy je třeba získat informace ze senzoru v místech bez přístupu na internet a bez potřeby komplexní sítě senzorů. Například se může jednat o senzor teploty zabudovaný ve vodovodním potrubí u víkendové nemovitosti, který zjišťuje, jestli nehrozí zamrznutí a poškození potrubí. V takovém případě lze využít technologie Sigfox, LoRa, NB-IoT podle jejich místní dostupnosti.

U standardů White-Fi a HaLow se nečeká, že budou stejně jako výše zmíněné technologie vysílány a nabízeny lokálními poskytovateli připojení, ale že si přímo uživatel vytvoří vlastní lokální síť stejně jako u standardu LoRa použitím LoRa gateway. Tato síť může mít až kilometrové rozměry. Nicméně kvůli vysoké ceně hardwaru jsou White-Fi a LoRa nevýhodné při nasazení v domácnosti. Standard HaLow je již dostupnější technologie, nicméně byl vytlačen příchodem Wi-Fi 6. Všechny tyto technologie ovšem našly díky svým vlastnostem uplatnění v průmyslu při řízení a monitorování procesů výroby a kontrole stavu strojů.

8.1.3 Aplikační možnosti RFID

RFID je hojně využívané při třídění, lokalizaci a identifikaci objektů, a proto má důležitou roli v dopravní a výrobní logistice. Z hlediska využití v domácnosti má uplatnění především v přístupových systémech, kdy díky tagu s identifikačními údaji lze odemknout dveře bez použití klíče, či automaticky otevřít garážová vrata pouhým přiblížením k nim. RFID má nicméně do budoucna díky snadno dostupným tagům velký potenciál v domácí automatizaci.

8.2 Analýza aplikačních možností cloudů

Jak už bylo řečeno v kapitole 6, cloud je ve struktuře IoT místem, které propojuje zařízení a aplikace, ke kterým přistupují uživatelé. Kvůli velkému množství a surové formě dat ze všech zařízení je nutné data před odesláním do aplikací nějakým způsobem zpracovat. Cloudy proto nabízejí rozsáhlou škálu nástrojů, které lze při zpracování dat využít.

V první řadě je obvykle nutné data dlouhodobě ukládat. K tomu lze využít služby jako Azure Synapse Analytics, Google BigQuery či Amazon S3 z vybraných cloudových platforem. Data z delšího časového intervalu lze zpracovávat pomocí Azure Data exploeru, AWS IoT analytics či modulu v Google IoT core. Nyní je možno data využít k řízení zařízení či k jejich vizualizaci pomocí různých webových či mobilních aplikací. Často však lze vizualizovat data přímo v cloudu prostřednictvím služeb Azure IoT Hub, Amazon Kinesis či Google data studio. Tyto velké společnosti nabízejí též možnost využití strojového učení k vyhodnocení dat, kdy jej lze využít například k rozpoznávání různých objektů z kamerových záběrů či k analýze a vyhodnocení budoucího vývoje dat.

Google Cloud IoT

Cloudová platforma od společnosti Google má díky svým službám a možnosti využití Google map ideální využití u zařízení v dopravní a energetické logistice. Oproti ostatním platformám je však používaní méně intuitivní a nenabízí tarif pro menší projekty, to jsou nejspíš důvody proč se v nasazení při domácí automatizaci moc nevyskytuje.

Microsoft Azure

Společnost Microsoft a její cloudová platforma internetu věcí si klade za cíl především zjednodušit způsob, jakým lze využívat IoT v podnicích a průmyslových odvětvích a zlepšit interoperabilitu zařízení a služeb. Microsoft se též zaměřuje na edge computing zejména produkcí certifikovaných čipů Azure Sphere a vývojem služby Azure Percept edge AI. Edge computing řeší potíže s přetíženými sítěmi a dlouhou latencí komunikace díky rozložení výpočetního výkonu do několika koncových zařízení. To má široké využití především v průmyslu.

Amazon Web Services

AWS nabízí největší portfolio až 13 cloudových IoT služeb. Kromě toho nabízí velké množství tzv. mikroslužeb, což jsou sdílená cloudová řešení na platformě AWS třetích stran. Svoji velkou popularitu má také díky intuitivnímu prostředí, kvalitní uživatelské podpoře a různým výukovým programům a pravidelným, veřejně dostupným seminářům. Proto je často využíván za nekomerčními účely. I z hlediska nastavení předplatného je AWS ideální platforma pro zastřešení domácího řešení internetu věcí.

Alternativní řešení

Alternativou pro cloudové platformy může být domácí server či přímo NAS. Tímto způsobem lze vytvořit prostředí schopné ukládat, analyzovat a vizualizovat data ze zařízení a tím se vyhnout nákladům za předplatné cloudových služeb. Existuje široká paleta možností při tvorbě vlastního serveru, ten však nemusí nutně nabídnout takové možnosti jako cloudové platformy. Mimo to za provoz vlastního serveru je zodpovědný samotný uživatel a domácí server zdaleka nedosáhne takové dostupnosti a zabezpečení jako cloud. V nekomerčních aplikacích však není potřeba klást tak velký důraz na spolehlivost jako je tomu třeba v průmyslových řešeních. Proto je zcela opodstatněné používat vlastní server v domácím internetu věcí.

9 Finanční porovnání s běžnou technologií

Ke srovnání finanční náročnosti automatizace prostřednictvím internetu věcí a běžné technologie se využije fiktivní situace, ve které bude vyžadována určitá úroveň automatizace. Po stanovení základních podmínek se vybere technologie pro řešení pomocí běžných prostředků a technologií využívající IoT. Vybrané technologie se zhodnotí a porovnají se z hlediska finanční náročnosti.

Stanovení základních podmínek

V objektu je vyžadováno zprovoznění regulace teploty na určitou hodnotu podle časového harmonogramu u elektrického vytápění, který má pouze režim chodu a je tedy čistě regulovatelný jen pomocí napájení. Druhým objektem automatizace je interiérové osvětlení, které se má rozsvítit na podnět pohybového čidla, ale pouze za soumraku. Součástí podmínek je absence jakéhokoliv síťového zařízení, nicméně je k dispozici ethernetový kabel umožňující připojení na internet. V případě bezdrátového přenosu se počítá s tím, že zařízení jsou v bezprostřední blízkosti a není možné, aby byla mimo dosah signálu. Celkově se jedná především o výběr technologie a jejího finančního zhodnocení. Cena kabelů, instalace a montáž se nebere v úvahu.

9.1 Výběr běžné technologie

Z běžných prostředků k regulaci elektrického topení se při výběru technologie uvažovalo nad cenově dostupnějším řešením v podobě zásuvkového termostatu a robustnějším řešením pomocí dvoustavového regulátoru MAGELIYA v provedení do panelu a vstupem pro teplotní čidlo. Jak u zásuvkového termostatu, tak i u regulátoru se měří teplota pomocí externích čidel, která by měla poskytnout nezkreslené hodnoty o teplotě v místnosti.

U automatického osvětlení byl zvolen soumrakový spínač SS-T1 a PIR čidlo MERGE JQ-L pro detekci pohybu. Kombinací obou zařízení by měly být stanovené podmínky splněny. Levnější alternativou je hybridní čidlo LED21 Mini, které kombinujíce jak senzor pohybu PIR, tak i soumrakové čidlo.

Tab. 6 Finanční náročnost použitých běžných technologie (43–47)

Alternativa	Použitá technologie	Cena	Celková cena
Nízká cena	2v1 Zásuvkový termostat s externím čidlem a časovačem	380 Kč	659 Kč
	LED21 Mini pohybové / soumrakové čidlo	279 Kč	
Robustnost	MAGELIYA dvoustavový regulátor	599 Kč	1 108 Kč
	Soumrakový spínač SS-T1	220 Kč	
	PIR čidlo pohybu MERGE JQ-L	289 Kč	

9.2 Výběr technologie IoT

Stejně jako v předchozí sekci, i zde se bude pracovat s dvěma alternativami. V první alternativě bude konektivitu zajišťovat protokol ZigBee a data budou zpracována prostřednictvím AWS IoT core. Druhou alternativou bude použití komunikačního protokolu BLE a vlastního serveru v podobě NAS. K fungování ZigBee i BLE je potřeba pořídit hub. U ZigBee je vhodnou volbou certifikovaný hub pro AWS od značky DUNSUN. Pro BLE lze využít hub od společnosti Zemismart.

K ovládání elektrického topení se využije chytré relátko. Protože jsou cenově méně náročná a mají otevřený systém, použijí se relátka od značky MHCOZY pro ZigBee a u BLE relátko od PartsBeiz. Ke správné regulaci teploty místnosti je potřeba zjišťovat aktuální hodnotu teploty, ideálně dál od vytápění. Proto je třeba pořídit teplotní sensor. Pro síť ZigBee byl vybrán SONOFF SNZB-02, což je bateriově napájený senzor teploty a vlhkosti vzduchu, který umožňuje konektivitu s AWS. V případě BLE se použije též bateriově napájený senzor teploty a vlhkosti, tentokrát však od firmy Jinou.

U automatizace osvětlení lze využít opět relátka, častěji se však využívají chytré žárovky. V případě ZigBee i Bluetooth jsou poměrně kvalitní a kompatibilní s AWS chytré žárovky od společnosti Philips. Jako senzor pohybu se u ZigBee použije SNZB-03, opět od SONOFF a u BLE

od společnosti QWYEURO, přičemž oba jsou bezdrátové. V případě IoT není potřeba senzor soumraku, neboť aktuální data z internetu o západu slunce lze implementovat do logiky automatizace.

K výpočtu předplatného AWS IoT core je potřeba sečíst poplatky za konektivitu, odeslané zprávy a použitá pravidla. Předpokládá se, že každou minutu jedno ze 4 zařízení odešle data, použije se nějaké pravidlo, provede se akce a koncové zařízení data opět přijme. Zadáme-li tyto údaje do calculator.aws, což je online kalkulačka k výpočtu tarifu, zde vyjde, že měsíčně se bude platit 13 Kč. Za jeden rok využívání služby se tedy zaplatí 156 Kč. (48)

Ke zpracování dat u alternativy s BLE využijeme NAS od společnosti QNAP, která má již od výroby v rámci operačního systému instalované aplikace pro vlastní realizaci internetu věcí. Vzhledem k tomu, že není vyžadováno připojení většího počtu zařízení ani náročnější operace s daty, postačí i model nižší třídy jako je QNAP TS-130.

Tab. 7 Finanční náročnost použitých Iot technologií (49–57)

Alternativa	Použitá technologie	Cena	Celková cena
ZigBee + AWS	DUSUN OpenWRT ZigBee hub	727 Kč	2 566 Kč + 156 Kč/ročně za AWS
	Chytré ZigBee relé MHCOZY	532 Kč	
	SONOFF SNZB-02 senzor teploty a vlhkosti	357 Kč	
	Philips Hue LED žárovka [B22 Bayonet Cap]	535 Kč	
	SONOFF SNZB-03 senzor pohybu PIR	415 Kč	
	AWS IoT core předplatné	156 Kč/ročně	
BLE + NAS	Tuya BLE Gateway	827 Kč	6 786 Kč

	PartsBeiz chytré BLE relátko	591 Kč	2 837 Kč bez NAS
	JINOU bezdrátový BLE teploměr a vlhkoměr	562 Kč	
	Philips Hue LED žárovka [GU10 Spot]	443 Kč	
	QWYEURO pohybové čidlo PIR	414 Kč	
	QNAP TS-130	3 548 Kč	

9.3 Zhodnocení finanční náročnosti technologií

Porovnáme-li celkové ceny z Tab. 6 a Tab. 7 můžeme jednoznačně říct, že automatizace pomocí internetu věcí je nákladnější. Při zvyšování počtu zařízení by se však cenové rozdíly obou řešení snižovaly. Navíc v této situaci obě technologie plní stejné funkce, nicméně v případě IoT lze bez dalších nákladů, pomocí rozšíření aktuální logiky použití cloudových nástrojů přidat do domácnosti další prvek automatizace. Například se může jednat o dlouhodobé zpracování dat z pohybového čidla a podle toho lze následně určit časy přítomnosti uživatele v domácnosti a v závislosti na těchto datech topit. Tímto krokem by bylo docíleno energetické úspory.

Při srovnání ZigBee s cloudovou platformou a BLE s NAS lze konstatovat, že zásadním rozdíl v ceně obou alternativ tvoří právě NAS. Vzhledem k nízké ceně za cloudové služby by byla návratnost NAS při aktuálním návrhu přes 18 let, což je pravděpodobně již mimo životnost samotného zařízení. Proto lze tvrdit, že v nekomerčním použití IoT sítích, kde jsou řádově desítky zařízení, je koupě serveru čistě pro účely IoT nepraktické a finančně zbytečně nákladné.

10 Předpoklad budoucího vývoje IoT v domácnostech

Internet věcí je bezpochyby oblast, která se bude rychle vyvíjet. Páteří této technologie je schopnost vzájemné komunikace. Tato komunikace je též záležitostí, která rozvoj internetu věcí zpomaluje. Chytrá zařízení v budoucnu mohou být chytřejší a dostupnější. Stejně tak cloudové platformy mohou být frekventovaněji využívané a budou nabízet větší množství nástrojů pro různorodé použití. Nicméně dokud nebude existovat dostupný, bezpečný a spolehlivý způsob přenosu dat nemůže se internet věcí dále rozvíjet.

Dosavadním problémem je zahlcení vysílacího spektra a s tím související nízká míra dostupnosti volných frekvenčních pásem pro další vysílání. Jako jedno z řešení se nabízí přijetí kognitivního rádiového systému, který má schopnost získávat informace o provozní strategii a o prostředí, ve kterém je provozovaný. Systém tyto získané informace zpracuje a v závislosti na nich dynamicky a bez cizího zásahu koriguje své provozní parametry tak, aby dosáhl optimálního provozu. Během tohoto procesu se systém dále „učí“ a nově získané informace využije při své korekci. Z hlediska blízké budoucnosti se dá očekávat rozšíření NB-IoT, a to především díky tomu, že využívá volné vysílací bloky GSM a LTE – viz. sekce 5.1.3. (58)

Rozšířením internetu věcí je stále větší problém s adresováním nových zařízeních. Již řadu let se v komunikačních technologiích nahrazuje starý hardware za nový, který již podporuje IPv6. Přechodem na IPv6 by se tento problém definitivně vyřešil.

Na trhu je široká škála IoT řešení pro domácnosti, i přes tento fakt se tato technologie rozšiřuje v této oblasti pomaleji, než by se dalo čekat. Řešením by mohlo být rozšíření Wi-Fi 6. Díky své interoperabilitě a snadné instalaci by do budoucna mohl nahradit doposud hojně používaný ZigBee.

Dalším velkým krokem pro budoucnost domácího prostředí internetu věcí by mohla být technologie RFID. Chytré domácnosti se dlouhodobě učí návykům uživatele a vytváří jeho digitální profil, podle kterého následně automatizují každodenní úkony. Problém nastává ve chvíli, kdy v jedné domácnosti je vícero uživatelů s různými preferencemi. To komplikuje jak tvorbu uživatelského profilu, tak i jeho následné vyžití. Jako řešení se nabízí výše zmíněný RFID, díky kterému domácnost bude schopna spolehlivě rozpoznat uživatele a podle toho k němu přiřadit správný profil.

To by však bylo pouhým začátkem. Stejným způsobem lze detekovat a lokalizovat i běžné předměty. Tím by se rozšířily možnosti vzájemné interakce předmětů, které nemusí být nutně chytré. Vhodným příkladem může být chytrá lednička, která je schopná identifikovat svůj obsah a upozornit například na blížící se datum spotřeby skladovaných potravin.

11 Závěr a doporučení

Internet věcí je často skloňovaným pojmem, který v sobě má zahrnout širokou škálu technologií. Cílem této práce je ujasnit význam tohoto pojmu a stručně popsat vlastnosti vybraných technologií a jejich možnosti při nasazení v domácí automatizaci. Součástí práce je i porovnání finanční náročnosti internetu věcí a běžné technologie při automatizaci domácnosti.

Zásadní schopností internetu věcí je komunikace mezi zařízeními. Proto je podstatná část práce věnována právě této problematice. Protože je však široká škála komunikačních technologií a je nereálné zmínit všechny, byly vybrány pouze ty nejrychleji rostoucí a ty, které mají ambice v podobě inovativních technologií. Při výběru komunikačních technologií se nebraly v úvahu jejich aplikační možnosti především proto, aby vznikl prostor pro zhodnocení jejich aplikačních možností při nasazení v domácnosti. Výsledkem je názor, že ve většině domácností se využijí především komunikační technologie krátkého dosahu. Aktuálně nejspolehlivější volbou je použití standardu ZigBee, závisí však na požadované aplikaci. Je ale reálné, že v blízké budoucnosti jej nahradí nová generace standardu Wi-Fi, která nabízí lepší vlastnosti.

Dalším esenciálním prvkem internetu věcí je cloud, ve kterém probíhá veškerá datová činnost. Při výběru cloudových platforem se postupovalo stejným způsobem jako u komunikační technologie. Protože však tomuto trhu dominují tři technologičtí giganti, výběr nebyl náročný. Jako nejvhodnější cloudová platforma pro domácí automatizaci byl zvolen AWS IoT Core od společnosti Amazon. Především díky intuitivnímu ovládání, veřejně dostupným výukovým programům a příznivému předplatnému pro drobné IoT sítě.

V neposlední řadě bylo realizováno finanční porovnání běžné technologie s technologií IoT. Ve fiktivní situaci byl vytvořen hrubý návrh domácí automatizace pro obě skupiny technologií. Výsledkem bylo potvrzení hypotézy, že nasazení internetu věcí je finančně náročnější než běžná technologie. IoT je však lépe škálovatelný a umožňuje pokročilejší automatizaci. Při té příležitosti se vyskytla i možnost porovnat ekonomickou zátěž při použití cloudové platformy a vlastního serveru. Použití vlastního serveru pouze k realizaci malé sítě IoT je finančně a prakticky nevýhodné v porovnání s cloudovými platformami.

12 Seznam použitých zdrojů

1. *What is the Internet of Things, and how does it work?* [online]. [vid. 2022-03-05]. Dostupné z: https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

2. *How the Internet of things uses Big Data: IOT system architecture - Parsers* [online]. [vid. 2022-03-05]. Dostupné z: https://parsers.me/how-the-internet-of-things-uses-big-data-iot-system-architecture/

3. BURIAN, Pavel. *Internet inteligentních aktivit*. nedatováno. ISBN 9788024751375.

4. *Eclipse IOT [IoT World Santa Clara]* [online]. [vid. 2022-03-16]. Dostupné z: https://www.slideshare.net/IanSkerrett/eclipse-iot-iot-world-santa-clara

5. ALAM, Mansaf, Kashish Ara SHAKIL a Samiya KHAN. Internet of things (IoT): Concepts and applications. *Internet of Things (IoT): Concepts and Applications* [online]. 2020, 1–515. Dostupné z: doi:10.1007/978-3-030-37468-6

6. *Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper - Cisco* [online]. [vid. 2022-03-06]. Dostupné z: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html?dtid=osscdc000283

7. *IoT Security Issues, Threats, and Defenses - Security News* [online]. [vid. 2022-03-06]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses

8. *What's the Difference Between a Smart, Connected, and Automated Home? | Direct Energy* [online]. [vid. 2022-03-09]. Dostupné z: https://blog.directenergy.com/difference-between-smart-connected-automated-home/

9. *Smart Home Vs. Home Automation* [online]. [vid. 2022-03-09]. Dostupné z: https://www.connectedhomenc.com/post/2019/04/04/smart-home-vs-home-automation

10. *Smart vs Connected Products: What's the Difference?* [online]. [vid. 2022-03-09]. Dostupné z: https://www.verypossible.com/insights/smart-vs-connected-products-whats-the-difference

11. *(PDF) Wireless sensors networks in road transportation applications* [online]. [vid. 2022-02-24]. Dostupné z: https://www.researchgate.net/publication/252020517_Wireless_sensors_networks_in_road_transportation_applications

12. *5 Things to know about the LPWAN market in 2020* [online]. [vid. 2022-03-17]. Dostupné z: https://iot-analytics.com/5-things-to-know-about-the-lpwan-market-in-2020/

13. *State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 B* [online]. [vid. 2022-03-17]. Dostupné z: https://iot-analytics.com/number-connected-iot-

devices/

14. *LPWAN - přehled IoT sítí | HARDWARIO IoT Blog* [online]. [vid. 2022-02-11]. Dostupné z: https://www.hardwario.com/cs/blog/2020-06-09-lpwan/

15. CHAUDHARI, Bharat S. a Marco ZENNARO. LPWAN technologies for IoT and M2M applications [online]. nedatováno, 448 [vid. 2022-02-11]. Dostupné z: https://books.google.com/books/about/LPWAN_Technologies_for_IoT_and_M2M_Appli.html?hl=cs&id=68i2DwAAQBAJ

16. *What is SIGFOX? | SIGFOX technology in M2M and IoT* [online]. [vid. 2022-02-11]. Dostupné z: https://www.rfwireless-world.com/Terminology/SIGFOX-technology-basics.html

17. *FAQ | Sigfox* [online]. [vid. 2022-03-16]. Dostupné z: https://sigfox.cz/cs/faq

18. *LPWAN Network architecture | Download Scientific Diagram* [online]. [vid. 2022-02-13]. Dostupné z: https://www.researchgate.net/figure/LPWAN-Network-architecture_fig1_335442047

19. *Sítě pro internet věcí v České republice - TZB-info* [online]. [vid. 2022-02-11]. Dostupné z: https://elektro.tzb-info.cz/informacni-a-telekomunikacni-technologie/16519-site-pro-internet-veci-v-ceske-republice

20. MEKKI, Kais, Eddy BAJIC, Frederic CHAXEL a Fernand MEYER. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* [online]. 2019, **5**(1), 1–7. ISSN 2405-9595. Dostupné z: doi:10.1016/J.ICTE.2017.12.005

21. NB-IoT DeploymeNT GuIDe To BasIc FeaTure seT requIremeNTs. 2019.

22. BUTUN, Ismail. Industrial IoT : challenges, design principles, applications, and security. 2020.

23. *6 Leading Types of IoT Wireless Technologies | BehrTech Blog* [online]. [vid. 2022-02-11]. Dostupné z: https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/

24. *Časopis Automa Bezdrátové sítě typu mesh* [online]. [vid. 2022-02-13]. Dostupné z: https://automa.cz/cz/casopis-clanky/bezdratove-site-typu-mesh-2005_12_30826_1141/

25. *Mesh vs Star Topology - Find your right IoT Architecture | BehrTech Blog* [online]. [vid. 2022-02-13]. Dostupné z: https://behrtech.com/blog/mesh-vs-star-topology/

26. *IEEE 802.11, The Working Group Setting the Standards for Wireless LANs* [online]. [vid. 2022-03-21]. Dostupné z: https://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm#tgax

27. *RFID Frequency bands | IDTechEx Research Article* [online]. [vid. 2022-02-12]. Dostupné z: https://www.idtechex.com/de/research-article/rfid-frequency-bands/40

28. *What is RFID? - Definition & Function in detail* [online]. [vid. 2022-02-12]. Dostupné z: https://www.etmm-online.com/what-is-rfid--definition-function-in-detail-a-824632/

29. *Understanding choosing RFID tag based on the tag frequency* [online]. [vid. 2022-02-12]. Dostupné z: https://rfid4u.com/rfid-frequency/

30. *What is RFID? - Definition & Function in detail* [online]. [vid. 2022-03-16]. Dostupné z: https://www.etmm-online.com/what-is-rfid--definition-function-in-detail-a-824632/

31. *The IoT cloud: Microsoft Azure vs. AWS vs. Google Cloud* [online]. [vid. 2022-03-10]. Dostupné z: https://iot-analytics.com/iot-cloud/

32. *Data encryption options | Cloud Storage | Google Cloud* [online]. [vid. 2022-03-16]. Dostupné z: https://cloud.google.com/storage/docs/encryption

33. *IoT Platforms: AWS vs Azure vs Google vs IBM vs Cisco | AltexSoft* [online]. [vid. 2022-03-16]. Dostupné z: https://www.altexsoft.com/blog/iot-platforms/

34. *Informace o cenách – IoT Hub | Microsoft Azure* [online]. [vid. 2022-03-16]. Dostupné z: https://azure.microsoft.com/cs-cz/pricing/details/iot-hub/

35. *Azure IoT reference architecture - Azure Reference Architectures | Microsoft Docs* [online]. [vid. 2022-03-16]. Dostupné z: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/iot

36. *An Introduction to AWS IoT Core | AWS Startups Blog* [online]. [vid. 2022-03-16]. Dostupné z: https://aws.amazon.com/blogs/startups/an-introduction-to-aws-iot-core/

37. *Cloud IoT Core | Google Cloud* [online]. [vid. 2022-03-16]. Dostupné z: https://cloud.google.com/iot-core

38. *A Guide to Smart Homes in 2022 | Learn All About Home Automation* [online]. [vid. 2022-03-09]. Dostupné z: https://www.security.org/smart-home/

39. *Hue Bridge | Philips Hue* [online]. [vid. 2022-03-18]. Dostupné z: https://www.philips-hue.com/en-us/p/hue-bridge/046677458478#overview

40. *Philips Hue White LED Smart Light Bulb 1 Pack [GU10 Spot] , with Bluetooth, Works with Alexa, Google Assistant and Apple Homekit. : Amazon.co.uk: Lighting* [online]. [vid. 2022-03-23]. Dostupné z: https://www.amazon.co.uk/Philips-Single-Spotlight-Bluetooth-Assistant/dp/B07SS37HPV?ref_=ast_sto_dp&th=1

41. *Thinka for Z-Wave* [online]. [vid. 2022-03-18]. Dostupné z: https://www.thinka.eu/z-wave#zwave-tech-spec

42. Use case possibilities with Bluetooth low energy in IoT applications White paper Use case possibilities with Bluetooth low energy in IoT applications-White paper [online]. nedatováno [vid. 2022-03-21]. Dostupné z: www.u-blox.com

43. *2V1 Zásuvkový termostat s externím čidlem s funkcí časovače - ChipModule.cz* [online]. [vid. 2022-03-23]. Dostupné z: https://chipmodule.cz/produkt/2v1-zasuvkovy-termostat-s-externim-cidlem-s-funkci-casovace/

44. *MAGELIYA AC 110V-220V Temperature Humidity Controller Timer SHT20 Sensor Thermostat LCD : Amazon.co.uk: DIY & Tools* [online]. [vid. 2022-03-23]. Dostupné

z: https://www.amazon.co.uk/MAGELIYA-110V-220V-Temperature-Controller-Thermostat/dp/B094T277ZJ/ref=sr_1_51?keywords=temperature+controller+with+timer&qid=1648045246&refinements=p_36%3A1500-&rnid=118657031&sr=8-51

45. *Soumrakový spínač s časovačem SS-T1 | GM electronic, spol. s.r.o.* [online]. [vid. 2022-03-23]. Dostupné z: https://www.gme.cz/ss-t1-soumrakovy-spinac-s-casovacem

46. *LED21 Mini pohybové soumrakové čidlo PIR pro spínání LED světelných zdrojů 12-24V DC 96W | Největší výběr svítidel a osvětlení* [online]. [vid. 2022-03-23]. Dostupné z: https://www.led-zarovky-usporne.cz/p/led21-mini-pohybove-soumrakove-cidlo-pir-pro-spinani-led-svetelnych-zdroju-12-24v-dc-96w/12219

47. *PIR pohybové čidlo 1200W, 150°, 9m MERGE JQ-L | GM electronic, spol. s.r.o.* [online]. [vid. 2022-03-23]. Dostupné z: https://www.gme.cz/pohybove-cidlo-kanlux-merge-jq-l-cidlo

48. *AWS Pricing Calculator* [online]. [vid. 2022-03-23]. Dostupné z: https://calculator.aws/#/

49. *SONOFF SNZB-03 ZigBee Motion Sensor, Wireless Motion Detector Get Alerts or Trigger Lights to Turn on, SONOFF Zigbee Bridge Required, Batteries Included : Amazon.co.uk: DIY & Tools* [online]. [vid. 2022-03-23]. Dostupné z: https://www.amazon.co.uk/Wireless-Detector-Required-Batteries-Included/dp/B08BCKHSB7/ref=sr_1_9?crid=25Q11S0286G0O&keywords=zigbee+PIR&qid=1647998848&sprefix=zigbee+pir%2Caps%2C157&sr=8-9

50. *SONOFF SNZB-02 ZigBee Temperature Humidity Sensor, Compatible with Alexa/Google Home, SONOFF ZigBee Bridge is Required, Battery is Included : Amazon.co.uk: DIY & Tools* [online]. [vid. 2022-03-23]. Dostupné z: https://www.amazon.co.uk/SNZB-02-Temperature-Humidity-Compatible-Including/dp/B08BFW697F/ref=sr_1_4?crid=1Y698ZCRFACM&keywords=zigbee+temperature+sensor&qid=1647996920&s=diy&sprefix=ZigBee+tem%2Cdiy%2C179&sr=1-4

51. *QWYEURO Adjustable PIR Motion Sensor Detector Switch 180° Max 1200W/12M (black) : Amazon.co.uk: DIY & Tools* [online]. [vid. 2022-03-23]. Dostupné z: https://www.amazon.co.uk/QWYEURO-Adjustable-Motion-Detector-180°Max/dp/B08C55W8VQ/ref=sr_1_25?crid=1I5865PM7ZKGP&keywords=bluetooth+pir+sensor&qid=1647999626&sprefix=Bluetooth+PIR+se%2Caps%2C161&sr=8-25

52. *Api/sdk Integration Service Programmable Health Care Smart Iot Gateway - Buy Smart Iot Gateway,Health Care Gateway,Gateway Hub Product on Alibaba.com* [online]. [vid. 2022-03-23]. Dostupné z: https://www.alibaba.com/product-detail/API-SDK-Integration-Service-Programmable-Health_1600082324461.html?spm=a2700.shop_plgr.41413.30.65c017cfy3pMJE

53. *MHCOZY 2CH WiFi Wireless Switch Relay,App Remote for Access Control Smart Garage Door,Compatible with Alexa Goolge Home (Smart Life app WiFi RF Bluetooth Relay) : Amazon.co.uk: DIY & Tools* [online]. [vid. 2022-03-23]. Dostupné z: https://www.amazon.co.uk/MHCOZY-Wireless-Control-Compatible-Bluetooth/dp/B08LVZR9WP/ref=sr_1_4?crid=OO5RFXUYU2I4&keywords=bluetooth%2BMHCOZY%2Brelay&qid=1647998198&s=diy&sprefix=bluetooth%2Bmhcozy%2Brela

y%2Cdiy%2C132&sr=1-4&th=1

54. *Tuya BT Gateway, BLE Mesh Wireless Gateway Hub, Tuya or Smart Life APP Control, Only for Tuya Compatible Devices : Amazon.co.uk: DIY & Tools* [online]. [vid. 2022-03-23]. Dostupné z: https://www.amazon.co.uk/Gateway-Wireless-Control-Compatible-Devices/dp/B09FTCPN2J/ref=sr_1_3?crid=3UWPCQ1W1B7XG&keywords=BLE+gateway&qid=1647997845&s=diy&sprefix=ble+gateway%2Cdiy%2C112&sr=1-3

55. *Bluetooth 5.0 Wireless Humidity and Temperature Sensor Beacon with Output Data and Monitor Ambient Weather For Android/iOS : Amazon.co.uk: Business, Industry & Science* [online]. [vid. 2022-03-23]. Dostupné z: https://www.amazon.co.uk/Bluetooth-iBeacon-Wireless-Humidity-Temperature/dp/B07FM4PSGB/ref=sr_1_6?crid=2HKWCW1D91LVD&keywords=ble+temperature+sensor&qid=1647997925&sprefix=BLE+temp%2Caps%2C96&sr=8-6

56. *MHCOZY 1 Channel 5V 12V ZigBee Smart Relay Switch,Adjustable Selflock and Momentary Working Mode,Works with Philips Hue, SmartThings, Alexa, Google Home (ZigBee Hub Required) : Amazon.co.uk: DIY & Tools* [online]. [vid. 2022-03-23]. Dostupné z: https://www.amazon.co.uk/MHCOZY-Adjustable-Selflock-Momentary-SmartThings/dp/B08X218VMR/ref=sr_1_6?keywords=zigbee+relay&qid=1647995650&sr=8-6

57. *Find IoT hardware that works with AWS | Search by industry, application, features, and more* [online]. [vid. 2022-03-23]. Dostupné z: https://devices.amazonaws.com/search?conn=zigbee&page=1&sv=iot&type=gateway

58. KRAMOSIL, Ing Jan. Dynamické sdílení rádiového spektra a komunikační sítě 5G Radiokomunikace 2018. nedatováno.