Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Internet věcí - IoT (využití LPWAN v prostředí IoT)

Bc. Pavel Skalický

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Pavel Skalický

Informatika

Název práce

Internet věcí – IoT (využití LPWAN v prostředí IoT)

Název anglicky

Internet of Things – IoT (LPWAN usage in IoT environment)

Cíle práce

Cílem práce je představit internet věcí, jeho současné možnosti a očekávaný vývoj. Praktická část je zaměřena na konkrétní oblast využití internetu věcí pro běžné uživatele – prostředí chytré domácnosti. V první části práce je přiblíženo, co je internet věcí, stručná historie, jak je možné propojit zařízení a kde se s ním můžeme setkat v reálném životě.
Dílčí cíle:
- Definice internetu věcí a jeho základní charakteristika
- Analýza modelové domácnosti s ohledem na zavedení IoT
- Výběr prvků do chytré domácnosti a návrh variant řešení
- Volba finálního řešení za pomoci finanční analýzy
- Závěry a doporučení

Metodika

Metodika teoretickéčásti diplomové práce, je založena na analýze a zkoumání bibliografických a elektronických zdrojů. V teoretické části bude uvedena definice internetu věcí a jeho základní charakteristika. Hlavní důraz bude kladen na dvě důležité kapitoly – aplikace a služby, zabezpečení zařízení spadajících do internetu věcí.

Praktická část práce se zabývá analýzou modelové chytré domácnosti. Pro výběr nových prvků je využita vícekriteriální analýza. Vybrané prvky budou zařazeny do struktury chytré domácnosti. Dále bude provedena finanční analýza možných variant řešení.

Na základě výsledů vlastní práce budou stanovena doporučení a formulován závěr diplomové práce.

Doporučený rozsah práce

50 – 60 stran

Klíčová slova

Internet věcí, LPWAN, Wi-Fi, chytrá domácnost, zabezpečení

Doporučené zdroje informací

Ganguli, M.: GettingstartedwithBluetooth. Cincinnati, Ohio: PremierPress, 2002, xviii, ISBN 1-931841-83-7.

Gislason, D.: Zigbeewirelessnetworking. Amsterdam ; Boston: Elsevier / Newnes, 2008, ISBN 978-0-7506-8597-9.

G. Margelis, R. Piechocki, D. Kaleshi a P. Thomas, „LowThroughputNetworksfortheIoT: LessonsLearnedFromIndustrialImplementations," IEEE Journal, Bristol, 2015.

V. Sulc, R. Kuchta a R. Vrba, „IQMESH, Technology forWirelessMeshNetworks: Implementation Case Studies," TheEighth International Conference on Networking and Services, Jičín, Brno, Czech Republic, 2012. ISBN 978-1-61208-186-1.

X. Xiong , Z. Kan , X.Rongtao , X. Wei a C. Periklis , „Lowpower area machine-tomachinenetworks: Keytechniques and prototype," IEEE Communications Magazine, 2015.

Předběžný termín obhajoby

2017/18 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 5. 6. 2017

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 13. 6. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 31. 03. 2018

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Internet věcí - IoT využití LPWAN v prostředí IoT" jsem vypracoval samostatně pod vedením vedoucího diplomové 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 diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 2. 4. 2018 _____

Poděkování

Rád bych touto cestou poděkoval Ing Jiří Vaněk Ph.D. za vedení mé práce a za cenné informace, které mi poskytl při řešení diplomové práce.

Internet věcí - IoT (využití LPWAN v prostředí IoT)

Abstrakt

Tato diplomová práce se věnuje internetu věcí. Na úvod v teoretické části definuje, co to je internet věcí, stručný popis toho jaké technologie se využívají a ukazuje oblasti využití internetu věcí. Seznamuje se stručnou historií, základními pojmy a jaké se využívají komunikační technologie. Důležité téma, kterého se dotýká i tato práce je bezpečnost. V praktické části se práce zaměřuje na tvorbu zařízení, které spadá do kategorie internetu věcí. Hlavní částí praktické části je ale návrh chytré domácnosti, za předpokladu využití nejčastějších komponent, které se využívají pro tvorbu chytrých domácností. Je navržena síť, která bude spolupracovat, komunikovat ke zlepšení komfortu uživatelů. Celá studie je postavena na plné automatizaci chytré domácnosti. Tímto může internet věcí ovlivnit životy všech lidí. Zároveň je představena budoucnost internetu věcí, jaké jsou jeho možnosti do budoucna. Tímto může internet věcí ovlivnit životy všech lidí.

Klíčová slova: Internet věcí, LPWAN, Wi-Fi, chytrá domácnost, zabezpečení, chytré město

Internet ofThings - IoT (LPWAN utilitisation in IoT environment)

Abstract

This diploma thesis deals with the Internet of Things. The introduction to the theoretical part defines what the Internet of Things is, a brief description of what technology is being used, and shows the areas of the Internet of Things. It deals with a brief history, basic concepts and the use of communication technologies. An important topic that concerns this work is security. In the practical part, the thesis focuses on the creation of devices that fall into the category of Internet of Things. The main part of the practical part is the design of a smart home, assuming the most common components used for creating smart homes. A network is designed to work together to communicate to improve user experience. The whole study is based on full automation of a smart home. This way, the Internet of Things can affect the lives of all people. At the same time, the future of the Internet of Things is presented, what are its options for the future. This way, the Internet of Things can affect the lives of all people.

Keywords: Internet of Things, Wi-Fi, LPWAN, smarthome, security, smartcity

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Iternet věcí je fenomén poslední doby. Tento pojem se objevuje v poslední době velmi často v oblasti informačních technologií. Tato myšlenka není sice nová, ale až nyní se v něm děje velký průlom. Většinou se internet věcí osznačuje IoT z anglického spojení Internet of Things. Podle toho co prorokují odborníci by se měl internet věcí rozvíjet. Určitě se v něm skrývá velký potenciál, který si ani neumíme v tuchle chvíli představit. Základem je připojování zařízení k internetu.

Rozhodl jsem se tomuto tématu věnovat, protože se jedná do budoucna o zajímavý technologický pokrok. Cílem je představit internet věcí a jeho současné možnosti. Současně chci ukázat jeho budoucnost, kam by se mohl ubírat.

V praktické části se budu zabívat inernetem věcí v praktickém využití. Vytvořím zařízení, které spadá do této kategori a navrhnu k tomu chytrou domácnost, kterou budu demonstrovat na modelovém domě. Podívám se na tento problém spíše z pohledu uživatelského.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je představit internet věcí, jeho současné možnosti a očekávaný vývoj. Praktická část je zaměřena na konkrétní oblast využití internetu věcí pro běžné uživatele – prostředí chytré domácnosti. Na tomto základě je vytvořená chytrá domácnost, do které se zapojí nově vytvořené zařízení. V první části práce je přiblíženo, co internet věcí je, jeho stručná historie, jak je možné propojit zařízení a kde se s ním můžeme setkat v reálném životě.

Dílčí cíle:

- Definice internetu věcí a jeho základní charakteristika
- Analýza modelové domácnosti s ohledem na zavedení IoT
- Výběr prvků do chytré domácnosti a návrh variant řešení
- Volba finálního řešení za pomoci finanční analýzy
- Závěry a doporučení

2.2 Metodika

Metodika teoretické části diplomové práce, je založena na analýze a zkoumání bibliografických a elektronických zdrojů. V teoretické části bude uvedena definice internetu věcí a jeho základní charakteristika. Hlavní důraz bude kladen na tyto důležité kapitoly – aplikace, služby, možnosti přenosu informací, technologie přenosu, oblasti internetu věcí, zabezpečení zařízení spadajících do internetu věcí.

Praktická část této práce se zabývá analýzou modelové chytré domácnosti. Pro výběr nových prvků je využita vícekriteriální analýza. Vybrané prvky budou zařazeny do struktury chytré domácnosti. Současně bude vytvořeno zařízení, které spadá do kategorie internetu věcí. Dále bude provedena finanční analýza, zda se vyplatí využít navrženou chytrou domácnost.

Na základě výsledků vlastní práce budou stanovena doporučení a formulován závěr této diplomové práce.

3 Teoretická východiska

Internet věcí je v poslední době chápán jako velký fenomén. I když je teprve v začátcích, očekává se jeho velká expanze. V budoucnosti se bude každý člověk s internetem věcí denně potkávat ve svém životě. V prostředí internetu věcí se potkávají fyzické a virtuální objekty, které si vyměňují data za pomoci internetu. Toto spojení přináší úplně nové možnosti. Díky připojení k internetu a sběru dat se mohou tyto zařízení rozhodovat autonomně. Hlavní myšlenkou je vytvořit „chytré“ věci všude okolo nás.

3.1 Základní pojmy

Jedna výzkumná společnost Gartner definovala Internet věcí (IoT), jako „síť fyzických objektů, která obsahuje vestavěné technologie, technologie pro komunikaci a vnímání nebo jejich vnitřní stavy či vnější prostředí.“ [1]

Jednou z dalších možností vysvětlení dané problematiky je definice od společností Accenture a Bankinter Foundation of Innovation. V publikaci od těchto společností s názvem The Internet of Things: In a Connected World of Smart Objects je uvedeno:
„Internet věcí se skládá z věcí připojených k internetu kdykoliv a kdekoliv. V technickém smyslu internet věcí začleňuje senzory a zařízení do běžných objektů, které jsou připojeny k internetu přes pevné nebo bezdrátové sítě.“ [2]

Najít jednu jedinou definici internetu věcí je velmi obtížné, né-li skoro nemožné. Každá společnost si definuje internet věcí po svém, odlišně než ostatní společnosti. Podstata definic je ale v jádru věcí s tejná.

Konceptuálně je internet věcí postaven na tom, že lze připoj jakoukoliv věc[1] za pomoci přenosové sítě k internetu. Díky komunikaci po internetu mohou mezi sebou komunikovat věci mezi sebou, ale i s uživateli. Tato problematika bude dále řešena v následujících kapitolách. V jedné z následujících kapitol bude i uvedeno, jaké zařízení lze považovat za zařízení spadající do internetu věcí. Internet věcí se v poslední době rozšiřuje neobvyklou rychlostí, proto

[1] Věcí se myslí neživý objekt, fyzický, nebo virtuální.

přibývají další zařízení, které se mohou připojit a spadají tak do internetu věcí. Základním stavebním kamenem internetu věcí nejsou samotná zařízení, ale data, která tyto zařízení produkují. [3]

3.2 **Historie**

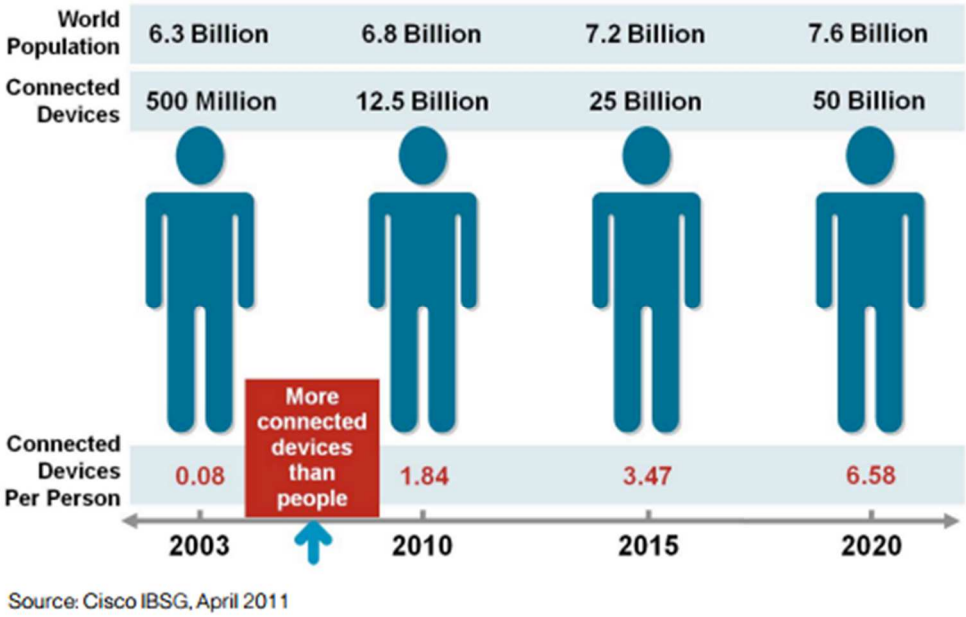
Historie internetu věcí se datuje až do 19. století. V roce 1832, kdy byl vynalezen první elektromagnetický telegraf Baronem Shillingem von Canstatt. Následně byl vyvinut elektromagnetický telegraf, který dokázal komunikovat až na vzdálenost 1200 metrů. Tento telegraf byl vynalezen dvojicí Carl Friedrich Gaus a Wilhelm Weber.

Za necelé století se začal o připojování předmětů zajímat Nicola Tesla. Ten v roce 1926 řekl: „Když bude bezdrátovost perfektně aplikována, celý svět se stane jedním
obrovským mozkem, všechny věci se stanou součástí jednoho reálného a rytmického celku. Budeme schopni spolu komunikovat kdykoliv, bez ohledu na vzdálenost. Nejen to, ale prostřednictvím televize a telefonování se budeme vidět a slyšet tak dokonale, jako bychom stáli tváří v tvář, navzdory vzdálenosti tisíců mil, a nástroje, jejichž prostřednictvím bychom toho byli schopni, se budou podobat dnešním telefonům. Člověk bude moci nosit takový přístroj ve své kapse.“[4]

Poprvé byl pojem internet věcí použit v roce 1990 Kevinem Asthonem v prezentaci s názvem „ The internet of things.“ A proto je to přelomový rok pro toto odvětví. [5]

Jako takový vznik internetu věcí se datuje mezi roky 2008 a 2009, kdy bylo podle společnosti Cisco překročeno počet připojených zařízení k internetu k počtu celkové populace na zemi. V roce 2015 bylo vypočteno, že na každého jednoho člověka vychází 3,47 kusů zařízení. Předpoklad na rok 2020 je 6,58 kusů zařízení na jednoho člověka. V celkovém měřítku je to odhadem 50 miliard kusů zařízení.

Okolo roku 2014 se o internet věcí začalo zajímat mnohem více lidí, a to vše díky mediím, která začala šířit povědomí o internetu věcí. V roce 2015 se k internetu připojilo 4,9 miliard kusů zařízení. Pro rok 2020 předpokládá firma Gartner, Inc. 20,8 miliard kusů zařízení. Tato předpověď je střídmější, než předchozí od společnosti Cisco. [7]



Obrázek 1 - internet věcí od roku 2003 - 2020 převzato z[7]

Další předpověď je od společnosti ABI Research, která předpokládá, že v roce 2020 bude připojeno k internetu 40,9 miliard kusů zařízení. Není jednoduché najít spolehlivou předpověď. Je jasné, že každá společnost počítá s jinými zařízeními. Jsou to nejasnosti, ke kterým dochází hlavně proto, že není jasně definováno, co je internet věcí a co není. Co všechno do internetu věcí spadá. V tomto ohledu je společnosti Gartner nejkontroverznější, protože podle nich mezi zařízení internetu věcí nepatří chytré telefony, tablety, počítače. Toto vše se dá vyčíst na jejich webových stránkách. [6]

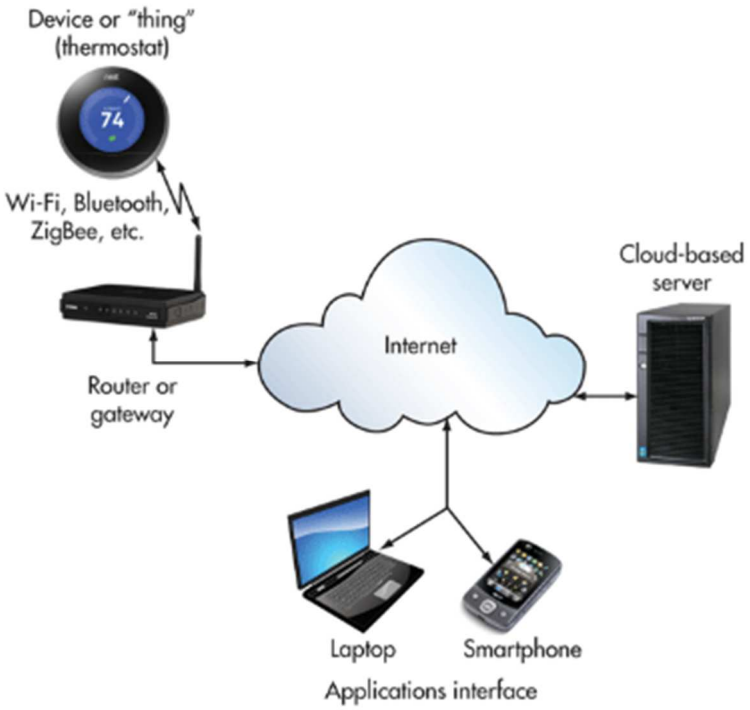
Samozřejmě jsou to pouze odhady, které se nemusí naplnit, není však vyloučeno, že i tyto odhady budou menší, než bude skutečnost. Vše ukáže čas, jak to dopadne. Je nesporným faktem, že oblast internetu věcí bude i nadále expandovat. Kdo ví, co nastane dál? Hlavní výhodou proč se dostává tak do popředí je fakt, že mnoha lidem dokáže zjednodušit život. Teď je už jen na uživatelích, jak tuto možnost využijí.

3.3 Technologie

Zaprvé je potřeba říci, jak internet věcí funguje. Princip fungování internetu věcí je znázorněn na následujícím obrázku. Veškerá zařízení jsou-li připojena do internetu věcí, mají nejčastěji zabudovaný bezdrátový vysílač, přes který komunikují buď s routrem, nebo bránou připojenou

k internetu s využitím přenosových sítí. Druhy přenosových sítí budou řešeny v následujících kapitolách. Zařízení se spojují přes internet s cloudovým serverem.

Na serveru běží jádro aplikace, která sbírá data z připojených zařízení, následně je analyzuje a ukládá. Následně vyhodnotí výsledky a rozhodne se inicializovat náležitou akci. Server dále komunikuje s uživatelem prostřednictvím aplikace, která umožňuje uživateli komunikovat a ovládat příslušné zařízení. V poslední době se dělají tyto aplikace na chytré telefony, které má člověk neustále k dispozici. Proto se z mobilních zařízení stávají ovladače na cokoli. Samozřejmě lze využit ke komunikaci jak počítač, tablet, tak i chytrý mobilní telefon, který má téměř každý člověk. [8]



Obrázek 2 - Schéma komunikace převzato z [8]

Jakmile uživatelé komunikují za pomoci zařízení spadajících do internetu věcí, tak se vytvářejí tzv. Big data, vzniká velké množství záznamů. Big data jsou základním kamenem internetu věcí. Big data dokážou vyhodnotit obrovské množství dat, které by lidé nedokázali zpracovat.

Technologií, které jsou používány internetem věcí, je spousty. Zde je zmíněno z mého pohledu to nejdůležitější, aby byl pochopen pojem internet věcí. Bude zde zmíněná technologie identifikace a komunikace, ale nebude opomenuta ani bezpečnost.

3.3.1 **Identifikační technologie**

Pokud chce zařízení komunikovat přes internet, je potřeba aby se nějak identifikovalo, tento identifikátor musí být jedinečný, bez něj není možné komunikovat. První ideou, se kterou se přišlo, bylo, že se bude využívat ke komunikaci v internetu věcí RFID[2] kód. To byl jen předvoj k tomu, aby se začal dělat zařízení s vlastní IP adresou.

Proto každému zařízení byla přidělena IP adresa. Nejprve se začala využívat IPv4 adresace, která má sice omezený, ale i tak velký adresní prostor. V přesných číslech to je 2^{32}, tedy cca 4 miliardy IP adres. Bohužel díky plýtvání s IPv4 adresním prostorem a rostoucími nároky na zařízení, které potřebují vlastní IP adresu, byl již vyčerpán celý adresní prostor.

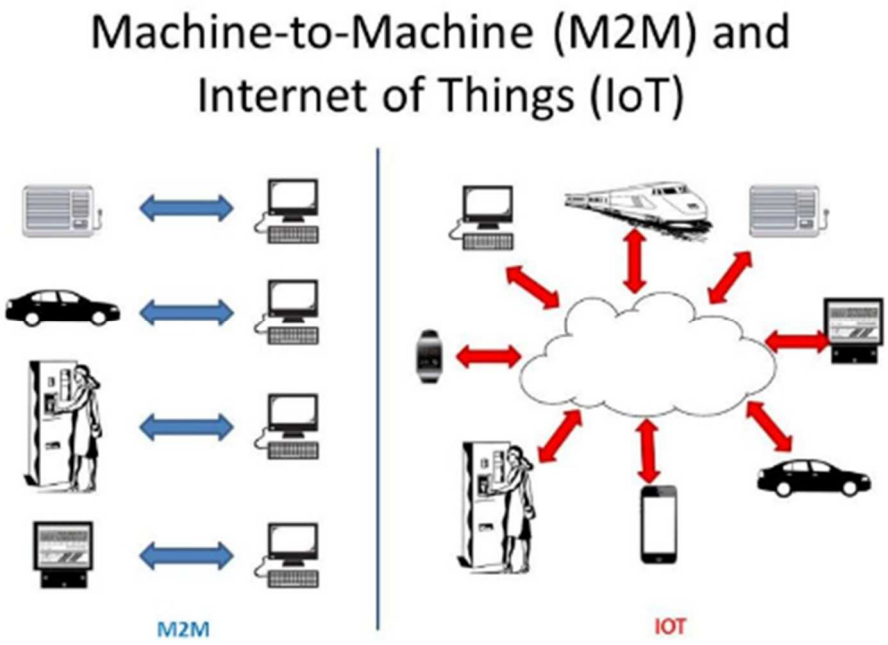
Proto se začalo hledat nové řešení, jakou adresaci použít. Poté byla vyvinuta IPv6 adresace, která má své výhody v obrovském adresním prostoru. V číslech to je 2^{126}. Bohužel i s tímto adresním prostorem se začíná hned od začátku plýtvat. Jakmile si uživatel zakoupil veřejnou IPv6 adresu, dostal k tomu dalších 100 000 adres. Pokud by se vyplnila čísla analytiků, i těch nejméně odvážných, tak by IPv4 adresace nestačila počtu připojených zařízení. Proto je IPv6 budoucností pro internet věcí. Kapacita je tak veliká, že každé zařízení může mít svojí unikátní adresu. Jedinou nevýhodou IPv6 z hlediska administrátora sítě je zapamatovat si IPv6 adresu. Oproti IPv4 adrese, která se zapamatovala snadno, má IPv6 složitou strukturu na zapamatování. Jedná se o osm skupin čtyř čísel v hexadecimální soustavě, které se ne úplně vždy lehce pamatují. Oproti tomu IPv4 měla čtyři skupiny čísel v desítkové soustavě v rozsahu od 0 do 255.

3.3.2 **Připojení zařízení**

Hlavní myšlenkou internetu věcí je propojování zařízení do jednoho celku. Společnou komunikací vytváří celkový funkční mechanismus, až se z nich dokáže stát autonomní systém, který nepotřebuje zásah uživatele. Komunikace je základ všeho a proto se využívá přes internet, vlastní síť, nebo napřímo mezi zařízeními, s vlastním komunikačním protokolem. Internet věcí a jeho komunikace se liší od běžné komunikace M2M, neboli machine to machine. V M2M

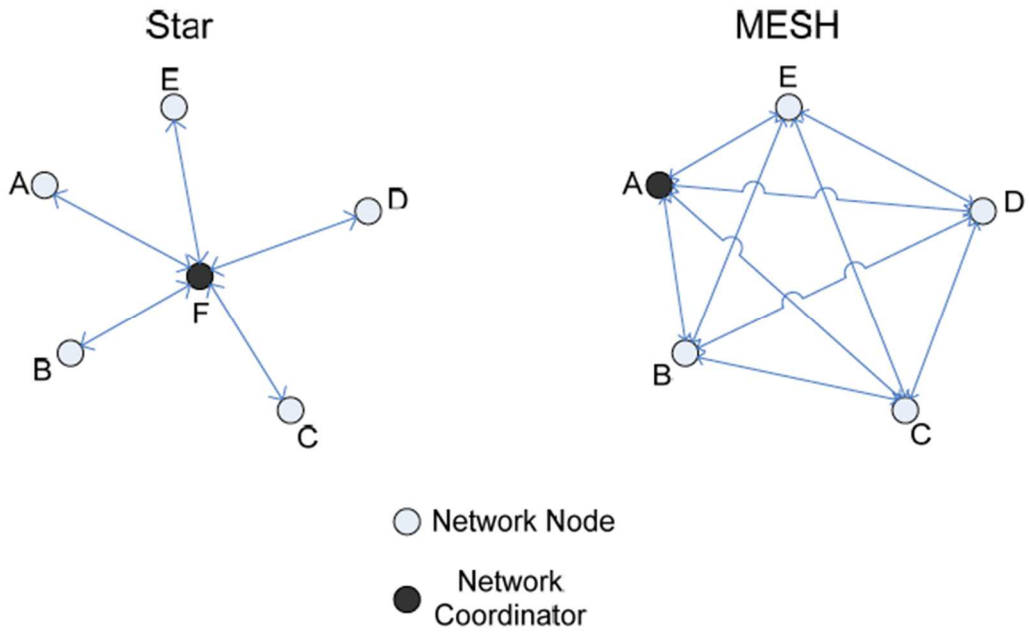
[2] RFID je technologie sloužící k identifikaci, snadné komunikaci na kratší vzdálenost.

spolu komunikují strojově, naprogramovaně a hlavně jednorázově. Zatímco v internetu věcí je tato komunikace neuspořádaná a neustálá.



Obrázek 3 M2M vs IoT převzato z [12]

Existuje několik druhů připojení internetu věcí, prvním a asi tím základním je pomocí síťového kabelu. Jedná se o spolehlivou přenosovou metodu, kde nevzniká žádné rušení signálu okolním světem. Většina zařízení ale využívá bezdrátovou podobu komunikace, kdy odpadá vymýšlení trasy pro kabelový přenos. Jedním z nejvyužívanějších bezdrátových protokolů je Wi-Fi a Bluetooth. Tyto protokoly zná v dnešní době skoro každý. Internet věcí ale využívá další protokoly, které už nejsou pro běžné uživatele tak známé. Jsou to například Zigbee, Z-Wave, které se vyznačují především smíšenou topologií sítě tzv. mesh network. Tento typ sítě se vyznačuje hlavně tím, že každé zařízení je připojené ke každému zařízení v síti, a současně jsou tyto zařízení připojeny i k přenosové bráně. Znázorněno to bude na další obrázku. Protistranou k této topologii je hvězdicová topologie, kdy se veškerá komunikace přenáší přes přenosovou bránu. Příkladem hvězdicové topologie je Wi-Fi. Hlavní nevýhoda hvězdicové topologie je v tom, že pokud selže přenosová brána, tak spolu přestanou veškerá připojená zařízení komunikovat. Smíšená topologie je tedy pro internet věcí úplně ideálním řešením, protože pokud selže přenosová brána, tak zařízení spolu budou nadále komunikovat. [11]



Obrázek 4 - rozdíl mezi mesh a star topologii [13]

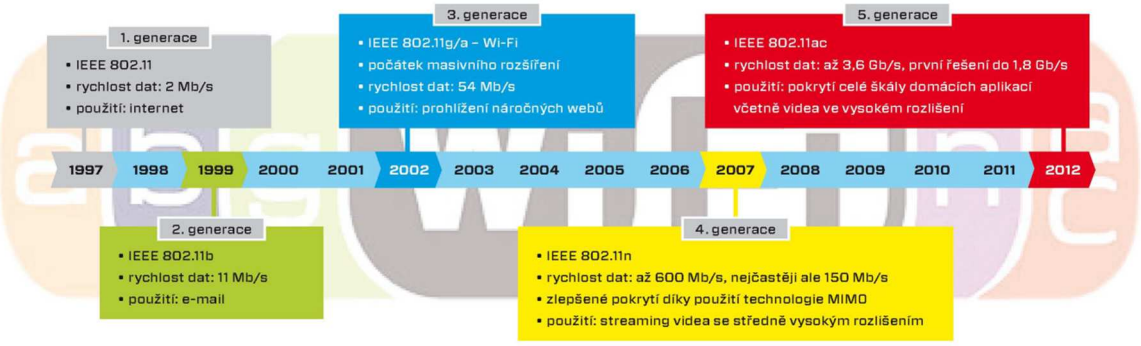
Není tomu tak dlouho, co byl představen nový protokol jmenující se Thread, mělo by se jednat o další evoluční stadium protokolu Zigbee, čas však ukáže, jak tomu bude.

V příštích podkapitolách budou představeny jednotlivé komunikační protokoly, které se momentálně využívají.

3.3.2.1 Wi-Fi

Zde se jedná o jeden z nejrozšířenějších komunikačních protokolů, který se momentálně u internetu věcí využívá. V této době se u Wi-Fi využívají dvě frekvenční pásma a to 2,4 GHz a 5 GHz. První generace Wi-fi vznikla už v roce 1997, kdy se jednalo o standard IEEE 802.11 s přenosovou rychlostí do 2Mb/s. Následující generace na sebe nenechala dlouho čekat a přišla v roce 1999. Jednalo se o standard IEEE 802.11b s rychlostí do 11Mb/s, což bylo výrazně lepší. Na další generaci se čekalo 3 roky. Následující generace, z roku 2002, měla standard IEEE 802.11g s propustností 54 Mb/s. Tento standard je k vidění v zařízení do dnes. Čtvrtá generace přišla v roce 2007 se standardem IEEE 802.11n. Vyhlídky pro tuto generaci byli vysoké, bohužel teorie se nepotkala s praxí. Teoreticky bylo slíbeno 600Mb/s, ale v praxi je přenosová rychlost 150 Mb/s. V roce 2012 přišel další standard IEEE 802.11ac. Přenosová rychlost bude odvozena podle počtu antén. Pokud bude jedna anténa tak je přenosová rychlost 433Mb/s s šířkou pásma 80 MHz. Maximální přenosová rychlost je 3,47 Gb/s, při použití osmi antén.

Poslední pátá generace funguje výhradně v 5GHz pásmu. Je však zaručená zpětná kompatibilita, ale nepůjde o standard IEEE 802.11ac, ale o nějaký z předchozích standardů a vše běží i na 2,4GHz, avšak preferovaná frekvence je 5GHz. [16]



Obrázek 5 - Historie Wifi převzato z [16]

Na veletrhu Consumer Electronics Show, neboli CES, byl na začátku roku 2018 oznámen nový standard IEEE 802.11ax. Tento nový standart navazuje na předchozí standard a zrychluje ho až o 40 procent. Což je tedy zrychlení ze 433 Mb/s na 600 Mb/s. Celý princip tohoto standardu je v tom, že dokáže 4 krát zrychlit komunikaci mezi stejně vybavenými zařízeními, dokáže lépe pracovat s daty. Konkrétně umožňuje lepší komunikaci v prostoru se zahlceným signálem na jak na frekvencích 2,4 GHz, tak i v pásmu 5 GHz. Dokáže zjistit rušení a volí dynamicky po jakém pásmu bude vysílat, tak aby se jednotlivé zařízení nerušili. Každé zařízení tak dostane své data, tak jak má. Nemusí se překřikovat. Nespornou výhodou je i energetická náročnost. Díky výše uvedenému se sníží spotřeba energie a tím se šetří baterie zařízení, jako jsou mobilní telefony, notebooky. Tuto novou technologii představila společnost Intel. První zařízení s touto novou technologií se mají objevit na začátku roku 2019. [17]

3.3.2.2 Bluetooth

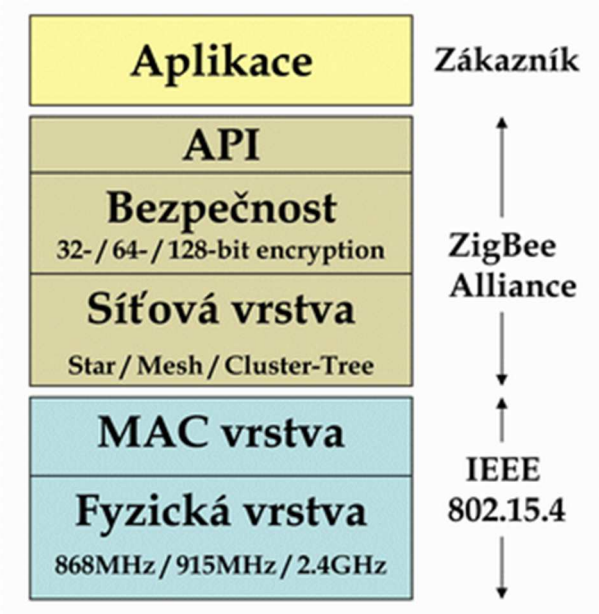
Jedná se o další hojně využívanou komunikační technologii. Není sice tak výkonná jako Wi-Fi, ani nemá takový dosah, ale je využívaná ke komunikaci mezi dvěma zařízeními. Jako každá komunikační technologie se i bluetooth vyvíjí. Momentálně je nejnovější verzí bluetooth 5.0. Oproti předchozí verzi 4.2 má bluetooth 5.0 výrazně lepší vlastnosti. Naštěstí je Bluetooth 5.0 zpětně kompatibilní a nebude tak probléme s jeho implementací. Nespornou výhodou pro internet věcí bude i to že byl vyvíjen pro toto odvětví. Dokáže v sobě skloubit komunikaci na velkou vzdálenost, nízkou energetickou náročnost a vysokou přenosovou rychlost. Jedná se i o lépe zabezpečenou komunikaci než u předchozích verzí. Obrovskou výhodou je i to že má

plnou podporu pro internet věcí a první zařízení s Bluetooth 5.0 se začnou objevovat v roce 2017. Standardem se tato verze stalo již 16. června 2016. [14,15]

3.3.2.3 Zigbee

Komunikační rozhraní Zigbee je známo od roku 2004. Správu nad tímto rozhraním má Zigbee Alliance. Toto komunikační rozhraní bylo vytvořeno na základě nevhodného využití Bluetooth ve spojení s průmyslovými aplikacemi. Velice jednoduchý komunikační standard na bázi bezdrátového spojení, které běží v 2,4GHz frekvenčním pásmu. Vzdálenost komunikace jsou stovky metrů. Nespornou výhodou jsou nízké nároky na hardware a spotřebu energie. Díky této výhodě se využívá na automatizaci budov, průmyslovou automatizaci, zdravotnictví, či ve spotřební elektronice. Nižší spotřeba si vybrala svou daň, a to v přenosové rychlosti. Přenosová rychlost se pohybuje mezi 20 a 250 kilobity za sekundu. Má však velkou odolnost vůči rušení. V průmyslu nahrazuje RS232 nebo RS-485.

Pomocí OSI modelu lze popsat komunikační standard. Rozdělen je do tří základních bloků. IEEE 802.14.52 popisuje fyzickou a linkovou vrstvu. Další vyšší vrstvy, síťovou a transportní, definuje Zigbee Alliance. Poslední aplikační vrstvu definuje zákazník pomocí zákaznické aplikace. [19]



Obrázek 6 - ISO model Zigbee [19]

Pro identifikaci se využívá binární adresovací kódy, tyto kódy mají dvě délky, a to buď dlouhé, které mají 64 bitů, nebo ty zkrácené, které mají 16 bitů. Každá sestava je jasně identifikovaná pomocí PAN ID. Jedná se o 16 bitový identifikátor, který pomáhá rozlišit překrývající se sítě.[19]

Existují tři hardwarové zařízení. První z nich je ZigBee Coordinator, druhé je ZigBee router a posledním typem zařízení je ZigBee End Device.

ZigBee Coordinator (ZC) – Jedná se o nejschopnější zařízení. Toto zařízení tvoří kořen stromu sítě a díky němu lze propojit ostatní sítě. Toto zařízení se dá přirovnat mostu spojuje ostatní sítě. Shromažďuje informace o síti, zajišťuje zabezpečení a uchovává zabezpečovací klíče.

ZigBee Router (ZR) – Funguje jako směrovač v síti, přeposílá data v rámci sítě.

ZigBee End Device (ZED) – Obsahuje pouze funkcionalitu, aby dokázali komunikovat s ZC a RZ. Jedná se o koncové zařízení, které má nízkou spotřebu i nízký výkon. Většinu času jsou tyto zařízení v úsporném režimu, díky čemuž se prodlužuje výdrž baterie. Výrobní náklady jsou oproti předchozím dvou typům hardwaru nižší. [21]

3.3.2.4 Z-Wave

Z-Wave je komunikační technologie, která pracuje na bezdrátovém principu s nízkou spotřebou energie. Vyčnívá několika úrovněmi zabezpečení a vysokou odolností proti rušení. Pracovní frekvence je 900 MHz, díky tomuto se vyhne přeplněnému frekvenčnímu pásmu 2,4 GHz, kde pracují jiné bezdrátové technologie a je již velice zaplněné. Z-Wave je navržen pro komunikaci v domě. Využívá se ke komunikaci dálkových ovládání, kouřové hlásiče, všelijaká čidla a podobné zařízení, které se v domě nachází. Přenosová rychlost není nijak závratná, ale je dostačující. Maximální rychlost přenosu je až 100 kilobitů za sekundu. Lze využít vysoké šifrování, IPv6 adresaci a vícekanálový provoz. Hlavní výhoda je využití mesh sítí, což znamená že každé zařízení může, a je schopné, přijímat a vysílat řídící příkazy. Každá síť má svoje 32 bitové ID a každé zařízení má své vlastní 8 bitové ID. [20]

Obrázek 7 - Z-Wave [20]

3.3.2.5 WiGig

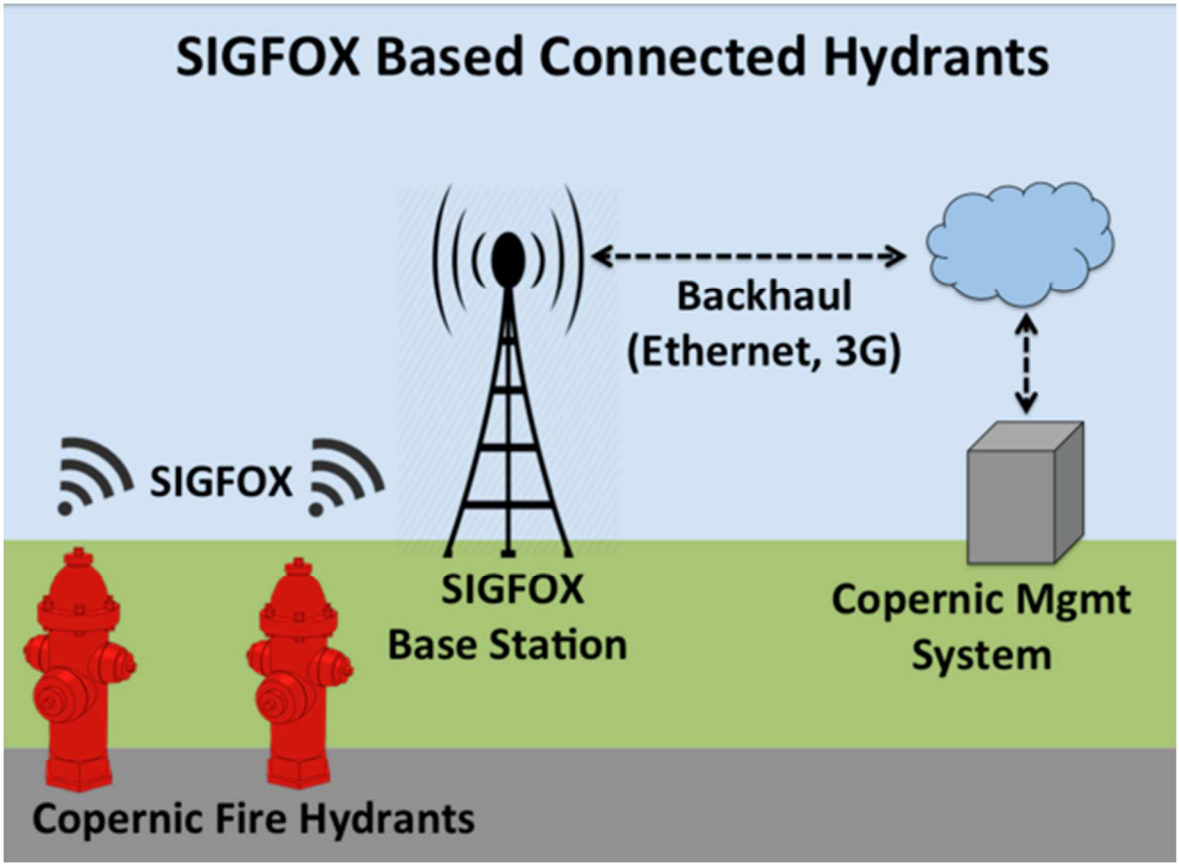
Neboli Wireless Gigabit Alliance, jedná se o obchodní sdružení, které vyvíjí a podporuje přijetí multi-gigabitové bezdrátové komunikační technologie. Operuje nad nelicencovaný frekvenčním pásmem 60 GHz. Využívá se zde norma IEEE 802.11ad.

Tato specifikace umožňuje multi-gigabitovou rychlost, bez použití spojení pomocí metalických sítí. Povoluje bezdrátová data, grafické a zvukové aplikace, které doplňují předchozí bezdrátové LAN sítě. WiGig operuje ve třech frekvenčních pásmech. První dvě z těchto pásem jsou již známé, a hojně využívané. Jedná se o pásma 2,4 GHz a 5 GHz Rychlost přenosu dosahuje až 7 Gigabitů za sekundu, jedná se o přibližně stejnou rychlost jako osm antén IEEE 802.11ac. Oproti 802.11n je až 50 krát rychlejší, avšak při zachování zpětné kompatibility s WiFi. Signál o frekvenci 60 GHz většinou neprojde stěnami, ale zase to se může šířit odrazem od stěn, podlah, stropů a objektů, které tvarují paprsky do WiGig systému. Při přenosu mimo místnost se využije nižší frekvence, automaticky se přepne na nižší vysílací frekvence, které již projdou zdmi. Nespornou výhodou je to, že v pásmu 60 GHz není tolik rušení a při využití tohoto frekvenčního pásma ubyde i v ostatních dvou frekvenčních pásmech rušivých signálů. [22]

3.3.2.6 Sigfox

Jedná se o bezdrátovou komunikační síť s dlouhým dosahem. Dosah této technologie je několik kilometrů a využívá se k občasné komunikaci s malým množstvím informací, většinou

z měřících čidel a senzorů. Obecně patří do kategorie LPWAN sítí. Typickou oblastí, kde s v Evropě Sigfox využívá jsou odečty vody, elektřiny, plynu, parkovací senzory, Industry 4.0, SmartCity, zabezpečovací zařízení, péče o seniory, logistika, měření srážek a průtoků na záplavových tocích, a mnoho dalšího. Pomocí Sigfox sítě mohou být zařízení připojeny nezávisle na elektřině a vydržet desítky let na baterii. Zároveň zaručí vysokou úroveň bezpečnosti a spolehlivosti. Pro tuto technologii mluví i cena modulů. Základní modem i komunikace se pohybuje v řádech desetikorun a díky tomu není problém s masovým rozšířením a nasazení mnoha zařízení. Další nespornou výhodou je i jednoduché programátorské rozhraní, které umožňuje postavit aplikace nad daty. Zároveň není problém s integrací do již vzniklých informačních systémů. Jedná se zde o řády hodin, maximálně dní. [23]



Obrázek 8 - Využití sítě Sigfox [23]

Celoplošná síť pro Sigfox je vybodována ve Francii, Španělsku, Velké Británii. Například ve Francii se nachází více než 1000 základových stanic. Pro příklad je vidět na obrázku výše, jak se využívají požární hydranty. Tyto požární hydranty v sobě mají zabudovanou podporu technologii Sigfox a každý den tak hlásí tlak vody, který nesmí klesnout pod určitou hranici.

Díky lithiové baterii by měli vydržet, až 10 let v provozu. Dalším příkladem jsou chytrá parkovací místa, která dokáží určit, zda je či není obsazeno. Respektive hlásí změnu stavu. Využití této technologie je mnoho, příkladů by bylo nesčetně. Velkou oblastí využití je odesílání všemožných telemetrických dat, jako jsou odečty vodoměrů, plynoměrů a podobných měřidel, která jednou za čas odešlou informaci o svém aktuálním stavu. Využití je i v zemědělství, kde všemožné senzory hlásí teplotu, vlhkost, úroveň vody v nádržích, studních, popřípadě dokáží i nahlásit překročení limitů. Tyto senzory se dají využít v počasí, měření ovzduší, stavitelství, kde měří pevnost, tlak na určité konstrukční prvky, zatížení silnice.

Základové stanice se instalují většinou na již postavené vysílače mobilních operátorů, aby se ušetřili náklady na výstavbu infrastruktury, ale i na provoz. Sigfox pracuje v bezlicenčním ISM pásmu 868 MHz, ve Spojených státech amerických se využívá též bezlicenční pásmo, ale o vyšší frekvenci, a to 906 MHz. V tomto bezlicenčním pásmu se již dnes využívají domácí meteostanice, ovládání garážových vrat, avšak přesto není nijak rušena, protože tyto zařízení nevysílají pořád. K přenosu se využívá tzv. UNB (Ultra Narrow Brand). Jedná se o pásmo pro vyslání krátkého pulsu dat s vysílacím výkonem maximálně 100 mW. Každá přenášená zpráva ve chvíli přenosu zabírá maximálně 100 Hz a je přenášená rychlostí od 100 do 600 bitů za sekundu v závislosti na regionu, odkud se informace odesílá. Díky tomuto řešení je zajištěn dlouhý dosah s velkou odolností proti rušení. Každá vysílaná zpráva využívá tzv. DBPSK modulaci, které stačí pro přenos 1 bitu za sekundu šířka pásma 1 Hz. Jedná se zde o velmi vysokou efektivnost využití přenosového spektra, dá se dobře implementovat a přijímač dokáže demodulovat i signály velmi blízké hladině šumu.

Obrázek 9 - Architektura Sigfox [23]

Technologie je založená na hvězdicové topologii, zároveň je budována na buňkovém principu. Obsahuje základové stanice a buňky, které zajišťují pokrytí. Miliony zařízení vysílají svoje zprávy do sítě Sigfox, pakliže jsou v dosahu nějaké základové stanice. Každá stanice využívá místní Sigfox operátory, kteří následně obdržené zprávy, informace dále posílají do Sigfox cloudu. Tato následná komunikace probíhá přes TCP/IP komunikaci. Všechny základové stanice demodulují přijaté signály pouze pro účely Sigfox cloudu. Následně Sigfox cloud tyto informace přetřídí a pošle pomocí internetu do zákaznických zařízení a IT platforem. Data nemají žádnou konkrétně definovanou strukturu, proto je na odesílateli a zároveň i na příjemci, co a jak si do prostoru dat vloží a jak budou u příjemce tyto data interpretovány. Příjemce si data stahuje ze Sigfox cloudu pomocí API do svého systému či aplikace. Co se týká adresace, tak se nevyužívají žádné nastavitelné adresy, jako například IP adresy. Nepoužívají se ani SIM karty a tomu podobné technologie. Jednotlivé koncové zařízení se adresují pomocí interního identifikátoru, které si lze představit jako sériová čísla. Jednotlivé moduly s podporou Sigfox, jsou certifikované a tím pádem se sériovým kódem, pomocí něhož se zařízení identifikuje. Je zde určitá podobnost s MAC adresou každého ethernetového zařízení. Díky tomuto způsobu identifikace, adresování není nijak omezen maximální počet zařízení, které je možno připojit do jedné sítě, kolik zařízení dokáže obsluhovat. Jediným omezením pro základové stanice jsou jen podmínky všeobecného oprávnění, které jsou omezeny tzv. klíčovacím poměrem. Ten ovlivňuje, jak dlouho může základová stanice aktivně vysílat, což znamená, že je omezen počet zpráv, kolik přes základovou stanici projde.

Sigfox byl vytvořen primárně jako lehký protokol, který má přenášet krátké zprávy. Prakticky jde o to, že menší zpráva spotřebuje menší množství energie, čímž se zvyšuje životnost baterie. Celý přenesený rámec má pouze 26 bajtů, kde volitelně 0 až 12 bajtů je určeno pro užitečná data, zbytek je pro potřeby zajištění komunikace. V poslední verzi Sigfoxu je umožněn zpětný kanál. Maximální velikost kanálu je 8 bajtů užitečných dat a časově je omezen na 4 zprávy za den. Pokud porovnáme Sigfox s IP protokolem. Záhlaví komunikačního rámce IP stacku má 40 bajtů, a to i přesto, že by se přenášelo 12 bajtů užitečných dat. Z tohoto porovnání je jasně vidět, že použití TCP/IP protokolu není zrovna ekonomické, čím více se vysílá dat, tím více energie zařízení spotřebuje. Pokud se přenáší 12 bajtů plus režijní bajty trvá přenes něco málo přes 2 sekundy. Jedná se sice o malou rychlost přenosu, ale je zde převážena jednoduchostí a robustností zařízení, zároveň i levnějším provozem oproti jiným typům přenosu. Sigfox je

omezen na 140 vysílacích zpráv za den a 4 potvrzovací zprávy za den. Komunikace tedy probíhá přibližně jednou za 10 minut.

V praxi lze do 12 bajtů uložit 2 GPS souřadnice s přesností na 3 metry, 6 naměřených teplot s rozsahem -100 °C až 200 °C s přesností 0,004 °C a jiné údaje. Zpětný kanál se dá použít na změnu rozsahu, frekvenci odesílání, vypnutí a zapnutí některé další funkce. Tímto způsobem jde například zapnout komunikačně náročnější způsob komunikace jako je WiFi či GSM. Pomocí těchto komunikačně náročnějších technologií se stahují aktualizace softwaru. [23]

3.3.2.7 Li-Fi

Jedná se o zatím nevyužívanou technologii pro přenos, protože je teprve ve fázi vývoje a do komerčního využití se zatím nehodí. Tuto technologii lze vužívat tam kde je tma, jelikož se jedná o přes informaci pomocí barevného spektra. Vysílač vysílá pomocí blikání ledek, přímač dekóduje podle rychlosti blikání a barvy, neboli podle vlnové délky, zpět na informace.

3.4 **Bezpečnost a soukromí**

Každý nový vynález, technologie, cokoliv co je nové by mělo přinést něco nového. Mělo by to mít nějakou přidanou užitnou hodnotu. Což internet věcí bezesporu má. Přináší mnoho výhod koncovým uživatelům, ulehčuje jim život a automatizuje procesy, při kterých byl dříve nucet uživatel vynakládat energii. Odvrácená strana internetu věcí je bezpečnost, o kterou se většina uživatelů ani trochu nezajímá, naprosto jí podceňují a nedokáží se představit, jakému riziku se tím vystavují. Napadené mohou být jak na straně serveru, který ukládá veškeré data, tak zařízení které tytodata sbírají, měří. O bezpečnost na straně serveru se stará poskytovatel, který tato data sbírá. Avšak hojné množství zařízení, které splňují podmínky pro to aby byli zařazeny do skupiny internetu věcí, nemá žádné zabezpečení. Většina běžných uživatelů ani neví jak tyto zařízení zabezpečit.[24]

Většina odesílaných dat je chráněna pomocí autentifikace uživatele, kdy každý uživatel má své uživatelské jméno a heslo, pod kterým se přihlašuje k danému serveru, na který následně najrává získaná data. Tyto identifikační údaje by neměl znnát nikdo jiný. Při přenosu jsou data chráněna šifrováním. Zašifrovaná data by měl rozluštit jen přijemce, pro kterého jsou data určena. Většinou se jedná o ochranu dat v souvislosti s ochranou soukromí, soukromých informací. Velkým sběratelem citlivých dat jsou zdravocnická zařízení, která hromadí velké množství osobních informací. V dnešní době musí být nemocnice přijeny k intenretu kvůli Ereceptům, které musí vydávat elektronickou cestou. Veškeré záznamy o pacientech se ukládají na server, kde má každý lékař nemocnice, který potřebuje, možnost nahlédnotu do záznamů daného pacienta. Zde je tedy potřeba klást důraz na bezpečnost na straně serveru, aby se do záznamů nedostal nikdo do by je neměl vidět. Tak i na straně lékařů aby nevynášeli informace o pacientech. Potencionální útočník, který by se dostal k těmto datům by s nimi mohl provádět spoustu věcí. Od vydírání po uzavírání půjček na osoby, které by o tom ani nevěděli.

Zařízení, které se připojují k internetu věcí jsou chráněny různym druhy zabezpečení. Počínaje přihlašovacími údaji v podobě uživatelského jména a hesla, otisku prstu, zadáním určitého kódu, který je nastaven z výroby. Nepřijemnosti nastávají ve chvíli, kdy je tato ochrana prolomena. Může dojít i k finančním ztrátám, pokud by se útočník dostal například k ovládání topení a otevírání oken v chytré domácnosti. Nastaví maximální stupeň topení a zároveň otevře okna, tak to vede k finančním ztrátám za teplo, které nikdo nevyužívá. Horší škody jsou však materiální. Je pravda že materiální škody se dají převést z většiny na finanční, ale pokud se

útčník dostane ke kotli a k bezpečnostímu zařízení EPS (elektronický protipožární systém). V tu chvíli může dojít k požáru celého objektu. A v tuto chvíli pokud by se jednalo o chytrou domácnost, tak by škody byli jak finanční tak materiální. Jsou věci co si za peníze nikdo nekoupí. Další velmi nebezpečným případem je i napadení osobního automobilu, kdy se automobil stává neovladatelným a posádka auta je v nebezpečí života.

Celý princip internetu věcí je postaven na velkém množství dat, které sbírá každé zařízení o uživateli, který dané zařízení využívá. Tato data dokáží udělat obraz o uživateli. Čím více systém informací o uživateli schromažďuje, tím méně si uživatelé hlídají jaké data jsou o nich uchovávány. Vezmeme li v potaz pojem soukromí uživatele, tak zjistíme že není nijak vymezen. Většina lidí chápe pojem ochrana soukromí, jako kontrolu toho co komu řekne, jaké informace o sobě nasdílí ostatním. Avšak každý své soukromí vnímá jinak. Bohužel se většina lidí v této oblasti mýlí. Běžný člověk netuší že někdo, nebo něco o něm sbírá data, která může dále použít proti němu. Největší problém je že uživatelé si nedokáží ani představit jaká data se o nich ukládají. Na tomto principu je založená cílená reklama.

Je potřeba zvyšovat zabezpečení internetu věcí pro větší pohodlí uživatelů. S bezpečností souvisí i morální a etické problémy. Internetem věcí se necháváme ovlivňovat každý den. V dnešní době má chytrý telefon u sebe každý. V dnešní době každý odesílá data přes mobilní telefon, i když nevědomky, někdy vědomě se pohybuje po internetu a zanechává za sebou stopu. Využíváním iternetu se digitální stopa stopa zvětšije, i když o ní nemusí uživatel vůbec vědět. Pak už záleží na uživateli, zda dokáže eliminovat zanechávání stop či nikoliv. Je potřeba aby si každý uživatel uvědomil jaké výhody a nevýhody mu internet věcí přináší a podle toho zhodnotit používání internetu věcí. Je potřeba zhodnotit, zda nebude využíváním internetu věcí porušovat své morální zásady.

Je potřeba aby se každý uživatel zamyslel nad otázkou sdílení informací na internetu. Jaké informace by o sobě chtěl sdílet, a do jaké míry si je vědom kolik toho může svým jednáním ovlivit. Každý by si měl položit tyto otázky dříve než začne využívat internet věcí. Musí si na ně popravdě odpovědět a následně zhodnotit klady a zápory. Je potřeba zhodnotit hrozby, finanční stránku věci. Poslední a nejdůležitější otázkou je pak to zda je si uživatel vědom důsledů svých činů. Toto by měl provést každý uživatel, než se rozhodne využívat internet věcí.

Je bezesporu že internet věcí přináší mnoho výhod, ale za jakých podmínek to tak je. Čeho se člověk musí vzdát, aby si dopřál větší komfort? Je důležitější jednotlivec nebo společnost? Je nějaká hranice za kterou už nejít? Tyto otázky by si měl klást každý uživatel internetu věcí, než začně přemýšlet o využívání internetu věcí. Každá generace má tyto hranice nastaveny jinak. Mladší generace sdíli o sobě cokoliv, aniž by nad tím přemýšlela, oproti tomu starší generace jsou zdrženlivější se zveřejňováním informací o svém životě.

3.4.1 **Rizika zabezpečení**

Jednou z největších hrozeb v rámci internetu věcí je „denial-of-serviceattacks“
(popření servisních útoků). Jedná se typicky o zahlcení síťového zařízení více požadavky, než dokáže zařízení zpracovat. Toto vede k přetížení a zařízení není schopné poskytovat svou službu a odpovídat na dotazy.

Pokud se zaměříme na RFID čipy, tak popření servisních útoků lze aplikovat i na ně, nejčastěji se tyto útoky používají k deaktivaci těchto čipů. V rámci RFID i dalších čipů jsou nebezpečné i další útoky. Velmi nebezpečné je klonování RFID tagů, emulace RFID tagů, které pak vytvářejí falešné odpovědi. Patří sem ale i tradiční háčkovací techniky, jako je například vysílání malwaru, který když se dostane do čipů, může ho využívat k vypouštění RFID červů, příkladem je Stuxnet, který je dostupný na černém trhu. Samozřejmostí je i vypouštění RFID virů.

Čip je jednoduchý procesor, který pracuje pouze s binárními daty. K datúm se však nedostanem jinak než pomocí sběrnice a proto z běžných čipů nelzou data získat. Lze je ale na druhou stranu zničit, vyřadit z funkčnosti pomocí tzv. Faradyovy klece. Faradayova klec je ohraničený prostor, který díky povrchovému materiálu nepropustí rádiové vlny. Čip který je takto uložen není zničený ale pouze izovolán. Dají se použít i jené metody, ale většina vychází z tohoto principu.

Součástí jsou i rozsáhle databáze, které je potřeba chránit na co největší úrovni, napadení takové databáze může ochromit celou společnost, která se zabývá sběrem dat pro následující prodej. Hlavním důvodem nabourání se do databáze je poškození společnosti, vydírání, ochromení funkčnosti firmy.

Tématem posledních let je i čipování individuálních osob. Sledování takovýchto osob může být zásahem do soukromí, v případě že o tom netuší, nebo nesouhlasí. Problematika implantace micročipu do podkoží je velkým tématem. V poslední době se toto téma řeší stále častěji, díky pokročující technice. Jedná se o velmi kontroverzní téma, má své zastánce, ale i početnou část odpůrců. Využití se prosazuje především v situachích ztracených dětí, mladistvých, u nichž jsou rozhodující první minuty a hodiny po zmizení. Lze zde uvést program Missing Childern Europe, který byl založen roku 2009 a klade si za cíl vytvořit mezinárodní výstražný systém, horkou telefoní linku, finanční koalici zůčastněných států. Mikročipy by se dali implementovat i pro osoby s recidivou kriminálního chování v případě domácího vězení. [25]

3.4.2 **Data a skoukromí**

Jakmile se kdokoliv připojí do komunikační sitě a využívá specifická zařízení, začínají se o nich samotncých vytvářet velké záznamy dat, tzv. big data. Big data jsou velkou rychlostí narůstající množství dat z různých zdrojů. Prostžedí si dokáže ty to data vzít a ukládat. Bez zabezpečení není problém tyto data zístkat automaticky.

Privacy Encahnced Technology neboli soukromí díky designu je design zaměřený na soukromí s ohledem na hodnoty. Uživatel v tomto případě dokáže ochránít svá osobní data sám s dostupnými prostředky, jako je anonymizování na vstupních a výstupních dat, přihlašovacích údajů, či blokování cookies. Další částí ochrany informačního soukromí je minimalizace dat potřebných pro daný cíl. Každý uživatel by měl mít přehled co kam a komu odesílá, přehled na svými osobními údaji. Je potřeba dát každému uživateli možnost správy svých osobních dat, i dat specifických.

Potřeba je i transparentnost, je potřeba aby uživatelé věděli, jaké entity spravují jejich data, a je naprosto žádoucí aby měli přehled o tom jak a kdy je s těmito daty nakládáno. Součástí toho je i management dat. Je třeba znát kdo s těmito daty disponuje, kdo je uchovává a spravuje. Obecně platí, že kryptografické mechanismy, protokoly disponují dostatečnou sílou na ochranu toku dat, avšak existují prvky, které postrádají prvky řízení. Jinak řečeno bezpečnostní politika jednoho datového manažera se nemusí vypořádat s každou situací, která může nastat. Proto je potřeba aby existovaly systémy učijící pravidla chování pro jednotilivé situace, aby se různá data spravovali podle různých pravidel. Vývoj takovýchto systému je finančně a časově velmi náročný, je třeba zvláštní interpretace, překlad a optimalizace nejrůznějších pravidel. Většina

těchto pravidel je v různých jazycích. Každé pravidlo musí korespondovat se zákony o ochraně dat v dané zemi. Navíc tyto zákony se mohou měnit, a proto je potřeba při změně zákonů upravit i pravidla.

Veškerá data, pořízená měřením okolních senzorů, jsou pro většinu uživatelů dostupné z webového rozhraní, ke kterému je potřeba se připojit pod určitým identifikátorem. Proto je naprosto nezbytné, aby služba měla patřičný vzhled a přístupnost. Je potřeba aby si každý uživatel uvědomil, že zabezpečení citlivých dat je vždy dvoustranné. Na jedné straně je server, který zajištuje zabezpečení dat v databázi. K těmto datům se nesmí připojit nikdo kdo nemá oprávnění. Na druhé straně je uživatel, který by si měl sám zabezpečit svůj počítač proti úniku dat, když si je ztázhne do počítače. Ve chvíli kdy se uživatel autentifikuje, tak si tím dokáže zajistit jistou míru soukromí, ale je potřeba aby si uživatel při vytváření jednotlivých prvků, které ho mohou identifikoval uvědomil, že je potřeba vytvořit tyto prvky co nejsložitější, aby nedošlo k jejich prolomení potencionálním útočníkem.

3.4.3 **Zabezpečení informací**

Na informace se dá nahlížet z několika různých úhlů. Například znát polohu nějaké osoby, kde se zrovna nachází se hodí v případech, kdy se někdo pohřešuje. Avšak v opačném případě, kdy se nejedná o pohřešování se dá tato informace zařadit do informací, které zasahují do soukromí jedince. Jedinec, který vstupuje na území nějakého státu nemá možnost kontrolovat informace, které se o něm předávají. [26]

Pro efektivní systém, který bude dobře sloužit, je potřeba aby poskytované informace měli tři základní vlastnosti. Tou první vlastností je dostupnost ihned. Dostupné tehdy kdy to je potřeba. Jednoduchý příklad je napadení domova zlodějem, v tom případě je potřeba aby alarm reagoval ihned, ne až někdy později. V tom případě by alarm pozbýval smysl. Druhou vlastností je důvěrnost informace. Každá informace by měla být důvěrná a vlastník informace má právo udělat přístup díky autentifikaci uživatele a zároveň musí být dobře nastavený všechny mechanismy databáze, jinak příjde o důvěru uživatele v informace. Neméně důležitým faktorem je i to kde je informace uložená, jedná se o takzvanou kredibilitu nosiče a jedná se o klíčovou otázku v zabezpečení dat. Třetí vlastností je integrita dat. Je potřeba aby byla zajištěna integrita dat, v tu chvíli je jistota, že data jsou autentická a kompletní, v tu chvíli je možné data dále bez obav používat. [27]

3.4.4 **Zabezpečení sítí**

Nejpravděpodobnější možností útoku je útok vedený na jednotlivé síťové komunikační protokoly za účelem získání dat s relativně vysokou pravděpodobností. Veškeré hrozby, které se v dnešní době objevují v rámci internetu věcí, pravděpodobně i do budoucna jim bude muset každý uživatel internetu věcí čelit, pochází od člověka, který chce získat data určité osoby. Před útoky je možné se chránit vícero způsoby. Jako první se kradou osobní informace, které jsou pro uživatele nejcitlivější a krádež těchto dat je nejvíce ohrožena za pomoci nabourání se do bezdrátové sítě uživatele. Proto je semozřejmostí, že se tyto data mohou zabezpečit.

Prvním způsobem zabezpečení je šifrovaní dat při přenosu, tím se zajistí ochrana dat. Postup je takový, že se data přeloží do nesmyslného náhodného shluku znaků, pouze oprávněný příjemce dat je schopen je rozluštit. Pokud mluvíme o nejvýkonnějších druzích šifrování, tak ty obsahují velmi náročné šifrovací klíče či algoritmy, které je velmi náročné rozluštit. Dalším způsobem je odrážení neautorizovaných uživatelů pomocí autentifikace. Tato metoda si klade za cíl zabezpečit data pomocí unikátního přihlašovacího jména a hesla. Za předpokladu že se dodá ještě další možnoti doplnění je autentifikace bezpečnější a zároveň i spolehlivější. Jednou z nejlepších možností autentifikace je autentifikace uživatelská tj. v rámci jednoho přihlášeného. Třetí možností je předcházení neoficiálních spojení za pomoci eliminace skrytých přístupových bodů. K vytvoření skrytého přístupového bodu dochází většinou nevědomky, bez úmyslu. Stačí aby se někdo snažil příhlásit k bezdrátové síti a v tu chvíli vznikají díry v možnostech ochrany, uživatel co se snažil připojit ani nemusel mít za cíl nabourat se do sítě, mohl chtít jen využít připojení na internet, ale to stačí k vytváření děr. K zachytávání dat ze sítě stačí pouze laptop a speciální software, který bude odposlouchávat komunikaci.

Záleží pouze na uživatelích a na jejich možnostech a chuti zabezpečit si svou síť, vytvořit ochrané nástroje pro svou síť. Důležité je aby si každý uživatel uvědomil, že zabezpečení dat není nikdy brzy, vždy se bude někdo pokoušet někam se dostat bez povolení vlastníka.

Zařízení, které spadají do intenretu věcí nedokáží pracovat samostatně. Je potřeba aby mezi sebou komunikovali a zároveň musí mít velmi malou energetickou náročnost. S dostatečnou baterií je tak zajištěna jejich dlouhá doba použitelnosti.

3.5 Využití internetu věcí

První „Dům budoucnosti“ byl představen v roce 1989 v nizozemsku. V té době ještě nikdo netušil že se jednou bude jednat o Internet věcí. Význam tohoto nového domu byl hlavně v tom, aby si veřejnost dokázala představit, jak bude jednou vypadat budoucnost. Vybavením domu byli elektronické systémy, ovládání klimatizace a požárních čidel. Dokázal dokonce i rozpoznávat hlasy. Hlavním cílem bylo propojení všech systémů v domě, aby všechny informace zpracovával jeden počítač, který sloužil jako centrální ovladač. [28]

Jako první se k internetu připojovali počítače, následně se začali připojovat i chytré telefony. Již v roce 2013 se podle výzkumné firmy IDC vyrábělo více chytrých telefonů než těch obyčejných, tradičních mobilních telefonů. Nyní je na trhu stále více trz. wearables, specifikováno bude níže. V průmyslu se prosazují a přichází na trh chytré domácí spotřebiče. Je to tím že obliba internetu věcí neustále roste. Rapidně vzrostl počet zařízení, které jsou připojené k internetu, současně se i veřejnost začíná zajímat o oblast internetu věcí. V posledních letech se objevuje diskuze o tom, jak se bude oblast internetu věcí vyvíjet, co můžeme v budoucnosti očekávat. [29]

Internet věcí se dá uplatnit všude, kde si to jen jde představit v našem životě. Veškeré systémy, které fungují na internetu věcí vidíme všude okolo sebe, i když si to nemusíme plně uvědomovat. Možností, kde lze internet věcí využít je nepřeberné množství a každým dnem vznikají nové a nové řešení, které by měli lidem ulehčit život. Internet věcí se dá rozdělit na dvě hlavní oblasti. Jednou oblastí je spotřebitelský internet věcí a duhou oblastí je průmyslový internet věcí. Tyto oblasti se mohou prolínat, těmto oblastem se budu věnovat v následujících kapitolách.

3.5.1 Průmyslový internet věcí

Toto odvětí je zaměřeno na usnadnění provozu průmyslových společností, Vyrovnává tím možnosti konkurenceschopnosti společností a díky tomu otevírá novou éru ekonomického růstu. Internet věcí je v profesionální sféře možné využít všude. Proto se tato práce zaměří jen na určitě oblasti, které patří mezi ty nejzajímavější. Tyto oblasti jsou chytrá města, dopravní průmysl a zdravotnictí.

3.5.1.1 Chytrá města

Velký potenciál internetu věcí, který není zatím naplněn, představují chytrá města. Chytrým městem je myšleno město, které je propojeno sítí tvořenou ze senzorů aby se dosáhlo efektivnějšího chodu města. Tento koncept chytrého města usnadňuje život nejen lidem, kteří v nem žijí ale i návštěvníkům, či těm co městem pouze projíždí. Je jen otázkou času, kdy se začne internet věcí prosazovat do plánů měst. Avšak aby nebyl jen kritika, tak některá města již začala připravovat plány, na to jak integrovat internet věcí do infrastruktury města. Jedná se o modernizaci celé infrastruktury, která není hned, je to proces, který potřebuje čas. Je však nesporné že internet věcí má velký potenciál vylepšit životní úroveň ve městě, šetřit čas obyvatelům.

V rámci městské hromadné dopravy je koncept internetu věcí integrován již v dnešní době. Zastávky městské hromadné dopravy jsou opatřeny informačními tabulemi, které předávají cestujícím informace o tom, za jak dlouho přijede autobus, tramvaj na zastávku. Například v Praze se tyto zastávky začínají objevovat, jejich rozšíření je však jedná se o běh na dlouhou trať.

Chytré parkování je jeden ze systémů, který dokáže usnadnit život obyvatelům chytrého města. Veřejné parkoviště, které se nachází v centru města patří mez nejvytíženejší místa v centru města, proto je systém chytrého parkování účiným řešením k regulování zaparkovaných aut. Senzory dokáží detekovat volná parkovací místa, pozici těchto míst dokáže online sdílet mezi řidiče pomocí informačních tabulí, nebo mobilní aplikace. Díky tomu ví řidiči, kde může zaparkovat, ví i přesné místo volného parkovacího místa. [30]

Aby se usnadnilo dopravě ve městě je možné využívat inteligentní řízení dopravy k zajištění a zvyšení plynulosti a bezpečnosti silniční dopravy ve městě. Čidla, která jsou zabudovaná ve vozovce, dokáží poskytnout informace o vytíženosti vozovky. Díky tomuto lze dynamicky sledovat dopravní situaci ve městě. Základním prvkem tohoto systému je inteligentní semafor, který dokáže reagovat na hustotu silničního provozu a reaguje na nastálou situaci úpravou intervalů světelných signálů, díky čemuž se minimalizují kolony aut. Samozřejmostí je aby tyto inteligentní semafory byli rozšířeny co nejvíce a současně je potřeba aby se nenasazovali náhodně ale na předem vytipované místa, kde mohou pomoci dopravě. Je však potřeba aby byla jistá součinost těchto inteligentních semaforů mezi sebou. Pokud bude jeden semafor, tak nemá

šanci s dopravou nic udělat. Proto je v první řadě potřeba nasadit tyto inteligentní semafory na hlavní tahy ve městě a tím ulevit silniční doravě. Toto je nejlepší možnost jak nasadit inteligentní semafory do města.

Významným systémem v oblasti chytrých měst jsou inteligentní budovy. Hlavním problémem ve městě je velká spotřeba elektrické energie. Inteligentní budovy dokážou snížit spotřebu elektrické energie díky regulaci teploty v prostorách budovy. Za pomocí čidel v bodově se reguluje teplota, ale nereguluje se jen tím že se zapne klimatizace, vypne klimatizace. Řídící systém budovy bere v potaz více faktorů, jako je například venkovní teplota, počet osob v místosti, otevřenost oken, úhel slunečních paprsků. Na základě těchto informací řídící systém rozhodne zda spustí klimatizaci, zavře okna, vytáhne rolety proti sluníčku či spustí topení. Zároveň pokud je otevřené okno, které nedokáže systém ovládat, tak nezapne klimatizaci, topení, díky cemuž se nezvedá spotřeba elektrické energie. Takto dokáže inteligentní budova ušetřit obrovské množství energie. V rámci šetření elektrické energie je možné mluvit i o inteligentním veřejném osvětlení, které reguluje samo o sobě, kdy je potřeba svítit a kdy nikoliv. V současnosti se rosvicí celé město centrálně, většinou se nastaví čas, kdy se má rosvítit a kdy zhasnout. Světla svítí celou noc, což má za následek obrovskou spotřebu elektrické energie. Vespělejší města mají senzor na světlo, který ovládá pouliční osvětlení, ale pořád svítí celou noc. Proto inteligentní pouliční lampy dokáží svítít jen ve chvíli když se někdo pohybuje v okolí. [31]

Velice zajímavým konceptem je tzv. chytrý odpadkový koš. Jedná se o odpadkový koš s čidlem, které hlídá zda je koš plný, ve chvíli kdy čidlo zjistí že je naplněn, tak odpad v něm zmačká a tím uvolní další místo. Po úplném naplnění, kdy se do koše už ni nevejde, si sám koš objedná odvoz odpadu. Město tím šetří, tím že odváží pouze ty koše, které jsou potřeba a zároveň se zbyvuje přetékajících košů, o kterých nikdo neví a hyzdí pohled na město. Tento koncep dokáže výrazně ušetřit náklady na vývoz odpadu. Avšak testovací provoz ve Filadelfii ukázal, že úklidové čety museli chytré odpadkové koše vyvážet stejně často jako ty obyčejné, ale pořízovací cena byla rozdílná. Cena obyčejného koše se pohybovala okolo 2 000 Kč, zatímco chytré koše stály okolo 82 000 Kč, což je nepoměrně vyžší pořizovací cena s nulovou úsporou peněz. [32]

Již drívě jsem zmiňoval, že využívání internetu věcí se lidem zjednodušší život, ale na druhou stranu přichází o část svého soukromí. Proto je zásadní otázkou, zda senzory jež jsou rozmístěny

po celém městě nebudou narušovat soukromí obyvatelů města. Chtějí obyvatelé objetovat část svého soukromí pro lepší život ve městě? Jsou ochotní podstaoupit takovouto oběť? Bohužel lze tyto data velmi lehce zneužít. Je možné pomocí senzorů vytipovat, kde se daná osoba v daném čase pohybuje. Jedná se zde o bezpečnost i morální zásady, zda se necháme takto sledovat moderními techlologiemi.

3.5.1.2 Zdravotnictví

Velký potenciál internetu věcí se skrývá v oblasti zdravotnictví. Nejedná se však o vizi budoucnosti, již dnes se setkáme se zařízeními pracující na principu internetu věcí. V nemocnicích se využívá internet věcí ke sledování personálu, lékařských přístrojů, ale i pacientů. Díky využívání internetu věcí se zdravotní péče zjednodušuje, ale je třeba se zamyslet nad otázkou, jak moc je vhodné sdílet záznamy o pacientech po internetu, Je to vůbec vhodné? Pacienti, kterří využívají internet věcí mají své zařízení, které se nazýva wearables. Tato zařízení sledují zdravotní stav pacienta a odesílají data. Více o těchto zařízeních budu hovořit v následujích kapitolách týkajících se spotřebitelské oblasti internetu věcí. Waerables jsou navržena ke sběru dat o zdravotním stavu pacienta, proto mohou být pacienti sledování a kontrolování na dálku, díky cemuž se minimalizuje počet osobních návštěv u lékaře a tím se zvyšuje pohodlí pacienta, který se může věnovat čemu chce. Toto sledování se dá využít na monitorování seniorů, kteří žijí sami. [3]

3.5.1.3 Automobilový průmysl

Do budoucna čeká automobilový průsmysl velký počet změn. Většina výrobců automobilů došla k názoru, že k vylepšování aut nemusí navyšovat výkon motoru, ale mnohem důležitější je konektivita a využívání moderních technologií. Vozy mezi sebou dokáží sami komunikovat, díky čemuž se sníží riziko dopravnách nehod. Současně to ovlivní i provoz na sinicích, jenž se stane plynujejší. V současné době se využívá adaptivní tempomat, který na základě senzorů, co sledují vzdálenost před vozidlem upravuje rychlost tak, aby automobil nenaboural do auta jedoucího před ním. Pokud automobil před ním zrychlí, tak automobil vybavená adaptivním tempomatem také zrchlí avšak maximálně do nastaveného limitu.[33]

V této oblasti se stále častěji objevují hlasy, jak dlouho ještě bude automobil řídit člověk? Již v dnešní době se testují samořídící automobily, které by časem mohli nahradit v řízení člověka. Jedná se však o vzdálenou budoucnost. Autonomní vozidla testuje například společnost Google,

Uber a každý automobilový koncern pracuje na systému autonomního řízení. Díky propojení vozů bude možné vzájemné sledování vozidel, budou se předávat informace o poloze, směru a rychlosti. Současně bude potřeba aby automobily komunukovaly s inteligentními semafory a vozovkami. To bude mí za následek plynulejší dopravu ve městech. Je však potřeba součinosti více systémů, které zajistí lepší kvalitu dorpavy. Cena za pokrok nebude malá, ale i kdyby zachránil jediný lidský život, tak se tato investice vyplatí. [34]

Internet věcí se dá do budoucna využít i v jiných dopravních prostředcích. Principy lze aplikovat na jakýkoliv dopravní prostředek. Dorpavní prostředek integrující principy internetu věcí může dosáhnout větší efektivity a bezpečnosti, než si dokáže většina lidí představit.

3.5.2 **Spotřebitelský internet věcí**

Spotřebitelský internet je zaměřen na usnadnění života jednotlivce. Každé takové zařízení by mělo jednotlivci nějakým způsobem přinášet nějakou přidanou hodnotu. V této oblasti se nachází i chytré domácnosti, nositelná zařízení a chytrá zařízení, které se nachází v domácnosti. V literatuře se dá setkat s pojmem chytrá domácnost, nebo inteligentní domácnost, jedná se o to samé, záleží jen na autorovi dané literatury, jaké spojení použije, ale využívají se obě terminologie. Kam se bude ubírat budoucnost, nedokáže nikdo posoudit, ale již dnes se obejvují chytré oděvy, které jsou plné senzorů a s uživatelem komunikují pomocí mobilní aplikace. V následujících kapitolách budou představeny řešení, se kterými se již v dnešní době setkává většina lidí. [35]

3.5.2.1 Wearables

Jedná se o různá zařízení připojitelná k internetu, je zde možnost aby je člověk nosil na svém těle. Proto se nazývají nositelná elektronika tzv. wearables, z čehož vznikl stejnojmený název. Mezi tyto zařízení se zařazují chytré hodinky, fitness náramky, brýle, sporttestery, lokátory, atd. Hlavní devízou wearables je osobní užití. Mezi nejčastější způsoby využití těchto zařízení je sledování fyzické aktivity a s tím související monitorování životního stylu nositele.

Životní styl jde dohromady se zdravím člověka. Díky tomuto se začíná waerables prosazovat i ve zdravotnictví, kdy měří životní funkce uživatele a následně je odesílá lékaři, pokud to je potřeba. Toto řešení zajišťuje možnost nepřetržité kontroly pacienta na dálku svý lékařem. Následně lékař provede analýzu dat získaných od pacienta, což mu pomůže určit přesnější

diagnózu. Čím více dat lékař nasbírá, tím snáze se mu diagnóza určuje. Je to velmi jednoduché řešení pro pacienty s dobrou dostupností. Za pomoci dálkového monitorování pacientů mohou být pacienti propuštěni dříve do domácího léčení a dohled nad nimi bude prováděn na dálku. Ušetří se tak místo v nemocnicích pro vážné případy, které by nebylo možné sledovat na dálku a ušetří se tak náklady na vybavení a údržbu.

Fitbit sportovní náramky

Využívání sportovních trackerů se stává modní záležitostí. Je nespornou pravdou, že sportovní náramky jsou užitečným pomocníkem pro každodenní používání. Jednou ze společností, která se zabývá výrobou fitness zařízení pro lidi. Tyto zařízení monitorují aktivity uživatelů, měří pohyb uživatele a od otoho odvozuje spálené kalorie, dokáže změřit i kvalitu spánku. Veškeré informace má uživatel ve svém chytrém telefonu, ke kterým se dostane prostřednictvím aplikace umožňující i sdílení mezi přáteli a porovnávání se s ostatními. Uživatel má přesné inforamce o tom co dělal, jak dlouho to dělal, má pod kontrolou své aktivity a ví kde se může zlepšovat. Díky sdílení mezi ostatní přátele, ostatní uživatele se každý snaží zlepšovat, má motivaci být lepší.

Obrázek 10 - Fitbit Ionic Charcoal Smoke-Gray převzato z [36]

Nejlevnější fitness náramky od společnosti Fitbit se dají sehnat na českých internetových eshopech od 630 Kč. Jedná se o model Fitbit Alta Classic Teal Large, což je základní model z portfolia produktů. Dražší varianty jako je Fitbit Flex 2, který má více funkcí se pohybuje cenově v rozmezí 1300 Kč až 3000 Kč v závislosti na variantě. Vlajková loď společnosti Fitbit Ionic s velkým displayem, se pohybuje v cenové relaci od 8 000 Kč do 11 500 Kč[3]. Zmiňovaný náramek je na obrázku výše. Avšak konkurence se nemůže se zmíněným zařízením vůbec srovnávat. V odvětví fitness náramků je Fitbit ve velice dominantním postavení. Konkurenci, která mu rostla, stihl skoupit dříve než společnost Fitbit stihla ohrozit. Tento top model by se dal zařadit již mezi chytré hodinky. [37]

Chytré hodinky

Prvními chytrými hodinkami byli hodinky od společnosti Apple s názvem Apple Watch. Hodinky disponují nepřeberným množstvím funkcí. Tyto hodinky se dokáží chovat jako chytrý mobilní telefon. Dokáží zobrazit aktuální počasí, předpověď, přijímají a odesílají SMS zprávy, uživatel přes ně dokáže telefonovat, přehrávat hudbu. Samozřejmostí je i to že dokáži být součiné při sportovních aktivitách stejně jako waerables.

Obrázek 11 - Apple Watch series 3 převzato z [38]

[3] Ceny jsou uvedeny včetně DPH

Nejnovější verzi hodinek Apple Watch je series 3. S cenovkou atakující 10 000 Kč se rozhodně nejedná o levné zařízení. Výbavou se vyrovná leckterému telegonu a navíc dokáže přidat senzory navíc, jako je například GPS, GLONASS, Galileo, QZSS, barometrický výškoměr, snímač tepové frekvence, akcelerometr, gyroskop, snímač okolního světla. Mezi vlastnosti patří voděodolnost do 50 metrů, 8 GB interní uložiště. Standartní je konektivita a to pomocí wifi (802.11b/h/n) a bluethooth 4.2. Výdrž baterie je někde okolo 18 hodin. Je zde možnost vložení digitální sim karty, v tu chíli se stáva z hodinek plnohodnotný mobilní telefon, která dokáže fungovat bez jiného zařízení. Bohužel tato možnost není prozatím dostupná v české republice.

Obrázek 12 - Samsung Gear S3 převzato z [39]

Největší konkurencí pro Apple Watch je v této době, stejně jako na poli mobilních telefonů, Samsung Gear S3. Cenově se tyto chytré hodinky dají zakoupit stejně. Velkou výhodou je, že k funkčnosti hodinek není potřeba chytrý telefon od společnosti Samsung, aby hodinky mohli fungovat. Je sice pravda, že tyto chytré hodinky pracují nejlépe s telefony od společnosti Samsung, ale stačí jim jakékoliv zařízení s operačním systémem Adnroid, dokonce dokáží spolupracovat i s iOS. Zatímco Apple Watch umí pracovat jen se svým systémem, který firma Apple vyvýjí a aplikuje ve svých telefonech. Pro Samsung Gear mluví i udávaný výdrž 4 dny, oproti 18 hodinám, kterými se chulubí Apple Watch. Ale pokud by někdo nechtěl ani jednu značku a chtěl si připlatit, tak od společnosti Garmin by si mohl pořídit hodinky Garmin Fenix

5X s cenovkou od 17 000 Kč do 25 000 Kč. Jedná se jako u předchozích zástupců o topmodel značky. Cena se liší podle zpracování, ale funkčností se neliší. Oproti konkurenci mají lepší deklarované vlastnosti. Která vlastnost bude pro užovatele asi nejdůležitější je výdrž baterie. Gármin udává že výdrž je až 12 dní používání.

Obrázek 13 - Garmin Fenix 5X převzato z [40]

3.5.2.2 Chytrá domácnost

Nejčastější tématem, které se řeší ve společnosti v rámci internetu věcí je chytrá domácnost. Současné chytré domácnosti se většinou zaměřují na ovládání osvětlení, klimatizace, vytápění, automatické otevírání oken, atd. Počítačový systém dokoáže na základě dat, které má ze senzorů, určit optimální nastavení topení, klimatizace, větrání, atd. Vše se děje v rámci co nejmenších nákladů na energie, aby uživatel ušetřil peníze. Systém dokáže rozpoznat ve kterých místnostech se svítí oprávněně a ve kterých se svítí naopak úplně zbytečně a zhasne, aby se opět ušetřila elektrická energie. [41]

Pro lepší fungování chytré domácnosti se využívají i chytré spotřebiče, které spolu komunikují a koordinují. Stále častěji se diskutuje o chytrých lednicích, která se řadí mezi nejčastější zařízení z chytrých spotřebičů. Tato chytrá lednice pozná, že jí dochází nějaká potravina a upozorní uživatele o jejím stavu. Poprvé se objevila chytrá lednice ve filmu z roku 2000. Tento film se jmenoval The 6th Day, kde hlavnímu protagonistovi v podání Arnolda Schwarzeneggra oznámila, že mu došlo mléko. [42]

Chytrých domácností se objevuje stále více, uživatelé využívají nových technologií a možností, které se objevují na trhu a napojují je na již stávající systém. Největší problém je v množství produktů na trhu, kdy dochází k nekompatibilitě mezi zařízeními různých značek. Jenž způsobuje, že uživatel musí využívat více aplikací na ovládání chytré domácnosti. Nemá vše sjednocené v jednom centrálním systému, toho způsobuje uživateli jistou míru komplikací. Naštěstí výrobci se snaží domluvit na kompatibilitě zařízení, aby se zlepšila v komunikaci mezi zařízeními. Je naprosto nezbytné, aby si zařízení vyměnovali společně informace, je to totiž jediná možnost, jak by mohla vzniknout chytrá domácnost. Chytrou domácností se budu dále věnovat v praktické části. [43]

4 Vlastní práce

4.1 Chytrá domácnost

Následující kapitoly budou zaměřeny na praktické využití internetu věcí, které se mohou dotknout každého z nás. Někdo se potkává s internetem věcí každý den, někdo se s ním nepotkává, ale do budoucna se tomu jistě nevyhne. Hlavní důraz bude kladen na odvětví spotřebitelské a přesněji na chytré domácnosti.

Chytrá domácnost přináší něco nového, inovativního a bezesporu pro užívatele této domácnosti mnoho výhod. Mezi hlavní důvody, proč si pořídit chytrou domácnost, je jednodužší a pohodlnější život. Chytrá domácnost počítá se všemi okolními vlivy, díky čemu je schopná lépe kontrolovat a řídit chod domácnosti. Díky této kontrole je somácnost schopná uspořit elektrickou energii a tím způsobem ušetřit peníze, současně snižuje zátež na životní prostředí. Součástí chytré domácnosti je i bezpečnost , která je většinou na vysoké úrovni. Obrovskou výhodou je modifikovatelnost domácnosti, uživatel si může nastavit svou domácnost podle svých představ. Hlavním cílem chytré domácnosti je maximální komfort uživatele s co nejmenšími náklady a dopadem na životní prostředí.

V dnešní moderní době lze připojit k internetu skoro každá věc. Možností je nepřeberné množství, ať už od kuchyňských spotřebičů přes garážová vrata až po bezdrátové reproduktory od domácího kina. Pokud budou všechna zařízení navzájem komunikovat, tak jsme na dobré cestě k pohodlnému bydlení. V tomto směru je i potřeba zmínit automatizaci, díky které může internet věcí fungovat naplno. [44]

Nejprve je potřeba nastavit si úroveň automatizace, aby bylo jasné, jaký rozsah komunikace mají mezi sebou mít. Jakou spolupráci mají mezi sebou navázat. Představy jednotlichých uživatelů se mohou lišit, podle požadavků na funkčnost. Do internetu je možné připojit jeden spotřebič, nebo celou síť spotřebičů a senzorů, která řídí celou domácnost. Dům může být kompletně automatizovaný vrámci všech oblastí, avšak cena takovýchto systémů se pohybuje v řádu statisíců, ale i jednotek miliónů korun. Proto je na místě otázka, zda je potřeba aby dům dělal vše za uživatele.

Veškerá zařízení, které jsou připojená k internetu je možné ovládat pomocí chytrých mobilních telefonů, tabletů nebo počítačů. Stačí nainstalovat příslušnou aplikaci a následně je možné

ovládat prvky v domácnosti. Ovšem nejčastěji bude chytrá domácnost ovládaná pomocí mobilního telefonu, protože většina lidí v dnešní době má svůj chytrý telefon, takže i jednoduchou možnost, jak ovládat svou domácnost.

4.2 Vlastní zařízení

V této práci jsem se rozhodl vytvořit jednoduché zařízení, které bude splňovat zásady internetu věcí. Proto jsem se rozhodl vytvořit jednoduchou meteostanici, která má za úkol integrovat se chytré domácnosti. Tato meteostanice umí měřit teplotu, tlak a vlhkost. Součástí meteostanice je i komunikační čip, který komunikuje pomocí WiFi. Součástí meteosatnice je i bateriový shield. Přesné specifikace budou upřesněny v následujících kapitolách.

4.2.1 Bateriový shield

Nabíjecí bateriový shield je jednou z důležitých komponent, zajišťuje napájení meteostanice, buď pomocí baterie, nebo za pomoci 5 voltové nabíječky. V tomto případě byl k baterii přidán 6 voltový solární panel, který má na starost udržet baterii nabitou, aby ona mohla následně zásobovat meteostanici elektrickou energií. Schéma zapojení je jednoduché solární panel je zapojen do měniče napětí. Následně tento měnič napětí napájí baterii, a pokud je bateri plně nabítá, tak napájí solární stanici. V době kdy je tma, a solární panel nemá šanci napájet meteostanici, tak se o napájení stará baterie.

4.2.2 Wemos D1 mini

Wemos D1 mini je mozek celé meteostanice. Jedná se o malou vývojovou WiFi desku. Deska je plně kompatibilní s Arduino IDE, NodeMCU a MicroPython. Deska má 11 digitálních vstupů / výstupů a jeden analogový vstup / výstup, ale ten je omezen na maximální napětí 3,2 voltu. Všechny I/O piny mají přerušení. Každá takováto deska je dodávána s několika propojovacími piny. Záleží pak na každém, jak příslušné piny připájí. Samotná deska má pro mé využití naprosto dostačující parametry. Operační napětí je 3,3 voltu, avšak dokáže pracovat i s 5 volty. Frekvence na které čip pracuje je 80 MHz nebo 160MHz. Tato frekvence je dostatečná pro obslužnost připojených senzorů a následnou komunikaci přes WiFi. Je na uživateli, jakou frekvenci procesoru si vybere, ale musí počítat s tím že vyšší takt procesoru spotřebuje větší množství energie. Wifi modul je součástí desky, což je výhoda, protože není potřeba další

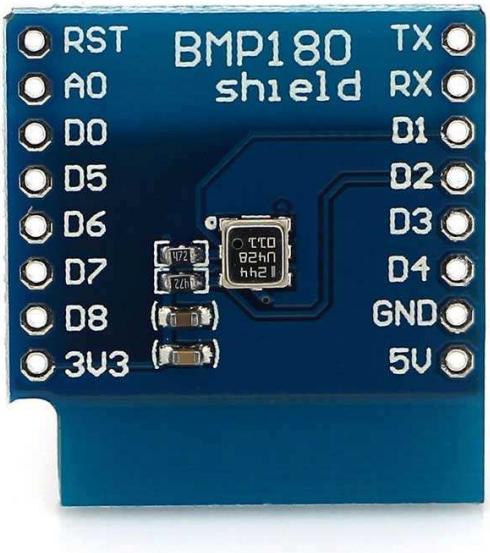
shield, co by spotřebovával energii. Samozřejmostí je i to že deska má interní flashovou paměť. Velikost je 4MB, což je v dnešní době neuvěřitelně malá velikost, ale jelikož zdrojový kód má několik stovek kilobajtů, přesněji 280 kB, takže je ještě dostatek volného místa pro další úpravy kódu. Deska obsahuje USB převodník CH340 a je osazena MicroUSB konektorem, proto je možné připojit desku k počítači, přes USB kabel. Na jedná straně USB a na druhé MicroUSB. U některých vývojových desek je potřeba před připojením využít převodník, který se připojí do USB v počítači. Následně pomocí převodníku se komunikuje přes USB kabel s deskou. Minimální spotřeba je 80 mA, záleží však na vzdálenosti zařízení od přístupového bodu, přes který se zařízení připojuje na internet.

Obrázek 14 - Wemos D1 mini

4.2.3 **Barometrický shield BMP180**

Jedná se o jednoduchý barometrický senzor, který je velikostně stejně velký jako vývojová deska Wemos D1 mini. Tento senzor je od firmy Bosh a je kompatibilní s Arduino moduly. Jedná se o levnější variantu senzoru BMP085, který je o něco přesnější. Rozsah tlaku který je možný měřit je v rozmezí 300 až 1100 hPa (hekto Pascalů), jenž odpovídá nadmořské výšce +9000 metrů až –500 metrů. Přesnost je zde -4 až +2 hPa. Další výhodou je i měření teploty pomocí integrovaného teplotního senzoru, avšak jeho rozsah je značně omezený. Přesněji je rozsah 0 az +65 °C (stupňů Celsia) s přesností na ±2 °C. Rozsah teplotního senzoru je nedostatečný pro venkovní využití, kde by měla meteostanice primárně sloužit. Za pomoci tlakového senzoru a teplotního senzoru lze vypočítat nadmořská výška, avšak k výpočtu se vyžívají údaje z obou senzorů a teplotní senzor neměří úplně přesně, což může ovlivnit i výpočet nadmořské výšky. Je potřeba upozornit, že se tyto naměřené hodnoty nedají srovnávat s profesionálními meteorologickými senzory, jsou tam občas velké rozdíly v naměřených

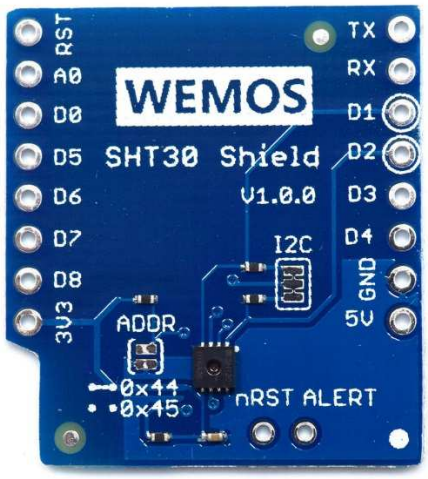
hodnotách. Odběr proudu je v aktivním stavu 5 µA (microAmper), ve stand by reřimu odebírá méně než 1 µA.



Obrázek 15 - BMP180 shield

4.2.4 Teplotní shield SHT30

Jedná se o kompatibilní shield s Wemos D1 mini a tím pádem je kompatibilní i s shieldem BMP180. S tím souvisí i velikost, která je obdobná jako vývojové desky a barometrického shieldu. Tento shield obsahuje teplotní senzor a senzor měřící vlkost. Teplotní senzor dokáže měřit od -40 °C až do +120 °C s velkou přesností. Odchylka tohoto senzoru jsou pohé tři desetiny stupně Celsia. Cože je velmi dobré, když vezmu v potaz, kolik tento senzor stojí. Druhou schopností, kterou tento shield disponuje je měření vlhkosti. Senzor měří vlhkost v procentech od 0 do 100 procent relativní vlhkosti. Přesnost měření jsou 3 procenta relativní vlhkosti. Na zkoušku jsem tento senzor skusil zasypat naprosto suchým křemičitým pískem a změřit vlhkost. Vlhkost vyšla 0 procent, jak jsem doufal. Spotřeba tohoto shieldu je větší než u předchozího, přesněji se pohybuje okolo 800 µA, což už není málo. A napájecí napětí je 2,4 až 5,5 voltu.



Obrázek 16 - SHT30 shield

4.2.5 **Sestavení meteostanice**

K sestavení meteostanice bylo nejprve sehnat pájku a pájecí stanici. Bez tohoto bych nedokázal meteostanici sestavit. Samozřejmostí je i základní elektrotechnické znalosti a jistá dávka zručnosti, aby se nestalo, že někdo bude pájet moc dlouho, a spálí odpory, rezistory a veškeré senzory. Veškeré součástky jsou velmi citlivé na teplo, proto je potřeba být velmi obezřetný při pájení. Nejprve je potřeba rozmyslet si, jak bude zařízeno poskládáno za sebou. Co bude nahoře a co bude níž, toto je potřeba rozmyslet již na začátku. Já udělal při prvním prototypu zásadní chybu, že jsem usadil nabíjecí shield nahoru, pod něj vývojovou desku Wemos D1 mini, další jsem dal barometrický shield a jako poslední jsem usadil teplotní shield. Hlavní chyba byla v tom že vývojová deska vyzařuje teplo, což nepříznivě ovlivňuje naměřenou taplotu na barometrickém shieldu, ale i na teplotní shieldu. Proto jsem se ve druhém prototypu ponaučil ze svých chyb a prohodil vývojovou desku Wemos D1 mini s nabíjecím shieldem, abych odstínil senzorické shieldy od vyzařovaného tepla. Rozdíl v teplotě byl vidět ihned, avšak nejvíce byl vidět rozdíl teplot při delším využívání, kdy rozdíl činil až 5 °C. Abych mohl umístit meteostanici ven, bylo potřeba dokoupit radiační štít, který zaručuje ochranu meteostanice před povětrnostními, ale neovlivňuje měřící senzory.

Pájením komponent to ovšem nekončí. Je potřeba komponenty i oživit, a naprogramovat, co mají dělat. Senzory měří sami o sobě, jakmile mají elektrickou energii, ale vývojová deska potřebuje s těmito informacemi nějak pracovat, pokud jí nenaprogramuji, tak naměřené hodnoty ze senzorů se nikam neukládají. První co je potřeba je aby si deska dokázala data

ze senzorů obstarat, ve chvíli kdy deska zjistí informace ze senzorů, tak si je uloží do proměných a dále s nimi pracuje. Je potřeba, aby se meteostanice připojila k wifi síti, a následně distribuovala inforamce dál. Po připojení k wifi síti se spustí webový server, na kterém si může uživatel zjistit aktuální data ze senzorů. Data ze senzorů se aktualizují každou minutu. Je zde i naprogramované JSON api, díky kterému se dají informace jednoduše stáhnout a dále s nimi pracovat například v google apps. Samozřejmostí je i výpis do sériové linky, která zajistí to, že po připojení k počítači se dají vyladit chyby, které se objevují. Popřípadě by šlo zaznamenávat i výpisy do sériové linky, ale to jsem již v této práci nedělal.

4.2.5.1 Zdrojový kód

```
#include <Streaming.h>
#include <ESP8266WiFi.h>
#include <ESP8266WebServer.h>
#include <Wire.h>
#include <Adafruit_BMP085.h>
#include <Adafruit_SHT31.h>
Adafruit_BMP085 tlakomer;
Adafruit_SHT31 teplomer = Adafruit_SHT31();
ESP8266WebServer server(80);
// Promenne senzoru
float tep_0 = 0.0f, tep_1 = 0.0f, tlak = 0.0f;
uint8_t vlhkost = 0;
uint16_t vyska = 0;
// Prihlasovaci udaje k Wi-Fi
const char ssid[] = "Pavel_AP";
const char heslo[] = "arduino1";
/*
  HTML kod stranky ulozeny ve flashove pameti
*/
PROGMEM const char hlavicka_html[] = "<!DOCTYPE html><html><head><title>Meteostanice</title><meta http-equiv=\"refresh\" content=\"70\"><style>html,body{font-family:'Segoe UI',Tahoma,Geneva,Verdana,sans-serif;margin:0;padding:0;display:flex;justify-content:center;align-items:center;width:100%;height:100%;overflow:hidden;background-color:blue;}div{font-size:10vw;color:grey;resize:none;overflow:auto;}.value{color:white;font-weight:bolder;}</style></head><body><div>";
PROGMEM const char paticka_html[] = "</div></body>";
/*
  Obnova údajů každou minutu
*/
uint64_t posledniObnova = 0;
// Funkce setup začíná pracovat hned po spusteni
void setup() {
```

```
 // spusteni seriové linky rychlostí 115 200 bps
 Serial.begin(115200);
 Serial << endl << endl;
 Serial << "    M E T E O S T A N I C E    " << endl << endl;
 /*
   v případě nenačtení dat z teploměru a tlakomětu vyhodí chybu
 */
 if (!tlakomer.begin() || !teplomer.begin(0x45)) {
   Serial << "Tlakomer nebo teplomer neodpovida. Zkontroluj zapojeni!" << endl;
   while (1) {}
 }
 ziskejHodnoty();
 // Jmeno zarizeni v siti
 WiFi.hostname("meteostanice");
 // Rezim Wi-Fi (sta = station)
 WiFi.mode(WIFI_STA);
 // Zahajeni pripojovani
 WiFi.begin(ssid, heslo);
 Serial << endl << "Pripojuji k Wi-Fi siti " << ssid << " ";
 // Vypisují se tečky dokud se nepřipojí
 while (WiFi.status() != WL_CONNECTED) {
   Serial << ".";
   delay(500);
 }
 // IP adresa
 Serial << endl << "Meteostanice ma IP adresu " << WiFi.localIP() << endl;
 /*
   Nastaveni weboveho serveru.
 */
 server.on("/", []() {
   // Ziskej URL jmenem api (/?api=.....)
   String api = server.arg("api");
   // převod na málá písmena
   api.toLowerCase();
   /*
     Pokud URL obsahuje text 'json', posli klientovi HTTP kod 200 a JSON s hodnotami ze senzoru
     a vypis do seriove linky IP adresu klienta
   */
   if (api == "json") {
     server.send(200, "application/json", "{\"tlak\":" + String(tlak, 2) + ",\"teplota\":" + String(tep_1, 2) + ",\"vlhkost\":" +
String(vlhkost) + "}");
     Serial << "HTTP GET: Klient si stahl JSON data" << endl << endl;
   }
   /*
     Jinak pošle HTTP kód 200 a načte
```

```
    */
    else {
      server.send(200, "text/html", String(hlavicka_html) + "Teplota: <span class=\"value\">" + String(tep_1, 2) + " &#x00B0;C</span><br/>Tlak: <span class=\"value\">" + String(tlak, 2) + " hPa</span><br/>Vlhkost: <span class=\"value\">" + String(vlhkost) + " %</span>" + String(paticka_html));
      Serial << "HTTP GET: Klient si stahl HTML stranku" << endl << endl;
    }
  });
  server.begin();
  Serial << "Webovy sever běží a čeká!" << endl;
}
// Opakování stále dokola
void loop() {
  // Zpracuj pozadavky weboveho serveru
  server.handleClient();
  if ((millis() - posledniObnova) > 60000) {
    ziskejHodnoty();
    posledniObnova = millis();
  }
}
// Funkce pro precteni hodnot ze senzoru do promennych
void ziskejHodnoty() {
  // Tlak v hPa
  tlak = tlakomer.readPressure() / 100.0f;
  // Nadmořská výška
  vyska = tlakomer.readAltitude();
  // Teplota z tlakomeru
  tep_0 = tlakomer.readTemperature();
  // Teplota z teplomeru
  tep_1 = teplomer.readTemperature();
  // Vlhkost
  vlhkost = teplomer.readHumidity();
  // Vypsani hodnot do sériové linky
  Serial << "System bezi: " << millis() << " ms" << endl;
  Serial << "Volna pamet heap: " << ESP.getFreeHeap() << " B" << endl << endl;
  Serial << "Udaje z BMP180" << endl;
  Serial << "Atmosfericky tlak: " << tlak << "hPa" << endl;
  Serial << "Teplota vzduchu: " << tep_0 << " C" << endl;
  Serial << "Nadmorska vyska: " << vyska << " m n.m." << endl << endl;
  Serial << "Udaje z SHT30" << endl;
  Serial << "Teplota vzduchu: " << tep_1 << " C" << endl;
  Serial << "Relativni vlhkost vzduchu: " << vlhkost << " %" << endl << endl << endl;
}
```

Celý kód je psaný v Arduino IDE a syntaxe je velmi podobná programovacímu jazyku C++. Člověk se dokáže syntaxi naučit velmi rychle, a většinu návodů si najde na internetu, takže není problém po několika hodinách porozumět, tomu co má udělat, jak to předělat a zlepšit. Největší problém s programováním kódu bylo stažení ovladačů na desku. Bohužel programovací prostředí neobsahovalo ovladače na desku, kterou využívám já, a tak jsem musel nechat dostahovat balíček ovladačů, který obsahoval i mojí desku.

4.2.5.2 Finanční náročnost

Veškeré komponenty jsem z důvodu nejnižší ceny nakupoval na eshopu www.aliexpress.com. Tento obchod se zabývá prodejem věcí z číny, v některých případech prodává klony produktů od jiných značek. V mém případě mi šlo o funkčnost za co nejmenší cenu a hledal jsem originální díly. Ani jsem nepotřeboval doručení do pár dnů. Z číny mi došly veškeré součástky do tří týdnů od objednání. Což pro mne osobně bylo docela velké překvapení, protože jsem nečekal, že bych se toho dočkal dříve než za měsíc. Dalším velkým překvapením bylo, že doprava nestála nic. V případě, že bych využil české obchody, které se specializují na tento druh sortimentu. Zaplatil bych skoro třikrát tolik, ale měl bych to do týdne doma. V tuto chvíli je potřeba dát si otázku, zda je pro člověka důležitější mít zboží dražší ve stejné kvalitě doma dřív, zhruba o 14 dní, nebo jestli je pro něj důležitější cena a nevadí mu, že si počká o 14 dní déle než by čekal na součástky z místních eshopů. Když vezmu v potaz, že cena součástek byla, dle aktuálního kurzu, cca 276 Kč. Na českých eshopech jsem stejné součástky našel i s dopravou za 1082 Kč, což je pro mne osobně výrazný rozdíl, pro který se mi vyplatí čekat tři týdny.

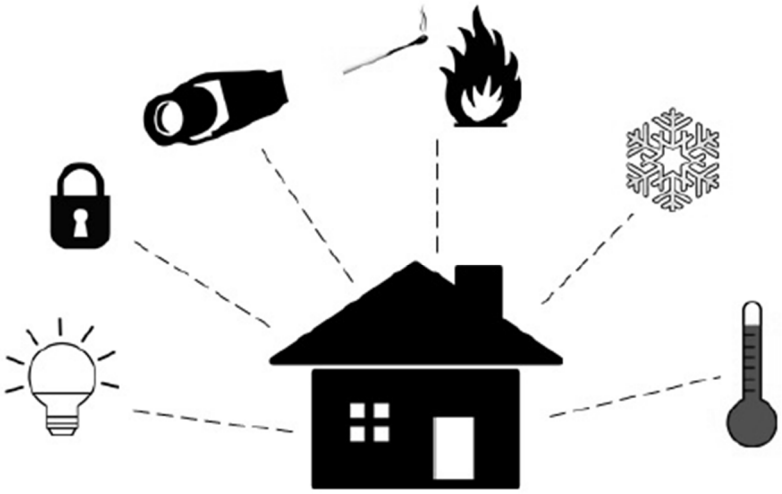
Název	Aliexpress (USD)	Aliexpress (Kč)	ČR (USD)	ČR (Kč)
Wemos D1 mini	3,71	81,14	7,22	158
Bateriový shield	1,94	42,32	5,17	113
BMP180 shield	2,12	46,26	6,04	132
SHT30	2,12	46,26	5,53	121
Solární panel	1,69	36,96	6,40	140
Nabíjecí kontroler	3,56	77,86	9,97	218
Sleva	-2,50	-54,68	0,00	0
Doprava	0,00	0,00	9,14	200
Cena celkem	**12,63**	**276,12**	**49,47**	**1082**

Tabulka 1 - Náklady na meteostanici

4.3 Návrh modelové chytré domácnosti

Hlavním cílem mé práce je navrhnout modelovou chytrou domácnost. Modelová domácnost bude mít dvě podlaží. V prvním podlaží se bude nacházet kuchyň, obývací pokoj, pokoj pro hosty, malá koupelna a technická místnost. Kuchyně s obývacím pokojem bude propojená. První patro bude patřit třem ložnicím, pracovnou a samozřejmě velké koupelně, které bude situována nad malou koupelnu.

Současné chytré domácnosti se skládají z komponent, které jsou znázorněny na následujícím obrázku. Podrobně je popíši v následujících kapitolách. Následně vyberu komponenty, které využiji v modelové domácnosti. Komponenty, které sice existují, ale nejsou pro běžné lidi tak užitečné nebudu zmiňovat.



Obrázek 17 - Základní komponenty chytré domácnosti

4.3.1 Hub – Mozek domácnosti

Jakékoliv zařízení fungující na principu internetu věcí může pracovat samostatně. Pro každé takovéto zařízení může mít uživatel jednu aplikaci v mobilu a ovládat zařízení jednotlivě. Problém nastává ve chvíli kdy se domácnost stává stálechytřejší a přibývají zařízení a současně přibývají i jednotlivé aplikace. Pro uživatele se pak stávají nepřehledné. Toto řešení není nijak výhodné. Jednodužší by bylo, kdyby se veškeré zařízení mohli ovládat pomocí jednoho centrálního systému, pomocí jedné aplikace, ušetřilo by to čas. Toto řešení již existuje a jedná se o pořízení dalšího hardwaru, který se o to stará. Jedná se o tzv. hub.

Hub je schopný dát dohromady všechna zařízení, zajistit mezi nimi komunikaci. Také veškerá zařízení spojuje do cloudu SmartThings a mobilní aplikace. Díky této aplikaci se dají veškeré připojená zařízení ovládat.

Je potřeba brát v potaz, jaké komunikační protokoly se využívají ke komunikaci mezi zařízeními, aby si uživatel zakoupil správný typ hubu. Je dobré mít všechny tyto protokoly předem dané aby pak nakonec nedocházelo k nekompatibilitě. Pokud uživatel ví, že bude mít zařízení, která komunikují pouze pomocí WiFi, popřípadě budou připojeny do místní sítě pomocí kabelu, stačí koupit hub, který bude podporovat pouze LAN a WiFi. Avšak je potřeba aby se uživatel rozmyslel, zda nebude již svou domácnost rozšiřovat o další zařízení, a pokud ano jestli umí komunikovat pomocí WiFi. Pokud by uživatel zakoupil zařízení, které neumí komunikovat pomocí WiFi, došlo by k nekompatibilitě a následně by to musel vyřešit koupí jiného zařízení nebo hubu. Proto se vyplatí počítat s budoucí modernizací a zakoupit hub, který umí co nejvíce komunikačních protokolů.

Za pomoci bodovací metody s využitím kritérií jsem určil jeden ovládací hub chytré domácnosti. Jedná se o hub od společnosti D-Link, přesněji s označením DCH-G020. Má nejlepší hodnocení na základě kritérií, které se dají jednoduše zjistit. Tento hub se vyznačuje velkým množstvím funkcí, co dokáže plnit. Standartní přenosové rychlosti přes LAN port. Ohledně bezdrátové komunikace umí dnes již standartní WiFi protokoly a k tomu umí i Z-Wave. Pokročilá funkcionalita je možnost IPv6 adresace s vlastním DHCP serverm. Další výhodou je i kompatibilita s Apple HomeKit, což žádné z porovnávaných zařízení nemělo. Cena je ucházející a pohybuje se okolo 2000 Kč.

Název	Funkce	Kompatibilita	LAN	Cena	Mobilní aplikace	Bodový součet s kritérii
D-Link DCH-G020	5	5	5	3	5	4,6
Samsung SmartThings Hub	4	3	5	3	4	3,6
BROADLINK S2 HUB	4	3	5	4	5	3,95
Mio Hub G10	3	2	5	5	3	3,25
Koeficient	0,35	0,25	0,05	0,2	0,15	

Tabulka 2 - Výběr hubu

4.3.2 **Vytápění**

Protože vzrůstají ceny energií, tak je dobré hlídat plítvání v podobě vytápění když to není potřeba, když jsou otevřená okna a tak podobně. Nákaldy na energie dělají většinu provozních nákladů domácností.

Na trhu je samozřejmě hodně možností, který se využívají k regulaci vytápění. Většina z nich se využívá pro udržování teploty v domě. Nastavuje se jedna teplota pro celý dům. Tento typ termostatu se využívá v menších domácnostech, kde se využívají všechny pokoje, protože se jedná i o levnější variantu těchto termostatů. Systém je možno ovládat na dálku přes mobilní aplikaci, měnit teplotu, vypínat a zapínat topení. Zástupci těchto termostatů jsou například Nest a Hive.

Existují i vyspělejší vyrianty vytápění jako je například Honeywell Evohome, který byl na základě vícekriteriární analýzy vybrán. Tento sysém umožňuje regulovat teplotu v každé místnosti zvlášť, lze nastavit pro každou místnost jiný režim vytápění. Lze vytvořit týdenní plán vytápění, který se pak následně dodržuje. To způsobí, že se vytápí pouze místnosti, které se využívají a neplýtvá se tak energiemi. Systém reaguje na změny velmi pružně, a dokáže poznat otevření okna a tak vypne topení do doby než se okno zase zavře. Pomocí mobilní aplikace je možné sledovat teploty jednotlivých místností.

Tomuto systému je potřeba i přizpůsobit topení, pokud se instaluje tento systém vytápění na již hotové topení, je potřeba osadit topení bezdrátovými termostatickými hlavicemi, které se následně spárují s řídícím systémem. Je potřeba aby v takovéto místnosti byl i senzor teploty, který bude komunikovat s centrální jednotkou, která vyhodnotí data ze senzoru a z hlavice a na základě toho rozhodne zda se má otevřít, zavřít topení nebo nedělat nic. Avšak není potřeba mobilní aplikace na změnu teploty stačí otočit termostatickou hlavicí a teplota se upraví. V případě že se nejedná o normální topění ale o podlahové, tak tato varianta lze taky využít, ale je dražší než využití normální termostatické hlavice.

Sada centrální jednotky, relé jednotky (směrovače) a tří termohlavic stojí 11 600 Kč. Pro modelovou domácnost je potřeba dokoupit ještě 6 termohlavic. Každá termohlavice stojí 1828 Kč, takže náklady na automatické vytápění činí 22 568 Kč včetně DPH. Cena pořízení systému není tak velká v porovnání s tím kolik peněz může v dlouhodobém měřítku ušetřit.

4.3.3 **Klimatizace**

Je potřeba zmínit i klimatizaci, která se hodí v letních měšících, avšak spotřebovává více eletrické energie, ale na druhou stranu uživateli přináší větší komfort. Neregulovaná klimatizace, která jede i když není potřeba spotřebuje až o 40% více energie než klimatizace, která je regulovaná.

Na trhu se objevuje velké množství klimatizací, tak tomu je i s regulátory klimatizací. Většinou tyto regulátory fungují na principu sledování pohybu v místnosti, pokud se někdo nachází v místnosti a je to potřeba, tak se spustí chlazení místnosti. Samozřejmostí je i ovládání pomocí aplikace na dálku. Kdy si uživatel nastaví že chce vychladit místnost, ve které se bude nacházet za pár minut. Samozřejmostí je i nastavení času, kdy se má chladit jaká místnost, v jakých časech.

V tuto chvíli je možné vybrat si mezi dvěma metodama ovládání, buď se namontouje ovládací systém na již zakoupenou klimatizaci, nebo se koupí klimatizace, která se dá již připojit k hubu pomocí WiFi. Proto jsem se rozhodl vybírat mezi klimatizacemi s připojením s wifi. Za pomoci vícekriteriální analýzy jsem vybral nejlepší variantu a to Frigidaire FGRC1044T1 Cool Connect. Jedná se o klimatizaci, která se dokáže připojit k hubu a následně být ovládána pomocí aplikace. Kdyby se nyvužíval hub, tak má podporu aplikací na android a iOS. Vybraná klimatizace disponuje velmi vysoký chladícím výkonem, což zajistí vychlazení určených místností i v parném létě. Cena jedné jednotky se se pohybuje okolo 7 800 Kč. Nejedná se sice o nejlevnější variantu, ale svými parametry je nejlepší. Pro mojí modelovou chytrou domácnost budou potřeba 4 chladící jednotky. Celkový náklad na koupi klimatizace bude 31 200 Kč. Rozmístění klimatizací bude následující 2 klimatizace se umístí do společného prostoru obývacího pokoje a kuchyně. Zbylé dvě klimatizace půjdou do prvního patra. Jedna do pracovny a druhá na společnou chodbu aby se daly vychladit i ložnice z jedné jednotky.

4.3.4 **Osvětlení**

Určitě si každý vybaví situaci, kdy už leží v posteli a chce se mu spát, ale má rosvícené světlo a musí se zvednout a to světlo zhasnou. V tuto chvíli nastupuje inteligentní osvětlení, díky kterému již nebude potřeba potřeba aby se člověk zvednul. Bude mu stačit zapnou aplikaci a osvětlení vypnout. Stačí k tomu jednoduchá věc a to nahradit stávající žárovky sítí chytrých

žárovek, kterou lze následně ovládat pomocí aplikace hubu nebo přímo aplikací na ovládání žárovek.

Systémem inteligentního osvětlení se na trhu zabýva velké množství firem, z největších hráčů na trhu bych zmínil LG, Samsung, Philips. Proto jsem vybýral pomocí vícekriteriální analýzy od největších hráčů na trhu. Výsledkem vícekriteriální analýzy byl systém osvětlení od firmy Philips. Přesně teda Philisp Hue Connected bulb. Tento systém obsahuje nepřeberné množství funkcí a efektů. Veškeré osvětlení je napojeno na centrální systém, a ten komunikuje s hubem, veškeré osvětlení by šlo napojit přímo na hub, ale nemusla by být zajištěna plná funkčnost. Proto budu využívat bezdrátový most, tzv Hue Bridge. Tento most spojuje veškeré osvětlení v jednu síť. V tom to systému je možné mít maximálně 50 svítidel, žárovek či LED žárovek Hue.

Toto osvětlení je velmi flexibilní a každé zařízení je možné ovládat samostatně, popřípadě po skupinách, či všechny naráz. Za pomoci aplikace je možné nastavovat intenzitu osvětlení, barvamu osvětlení v celém barevném spektru. Navíc lze světla propojit s hudbou a s filmy. Může tak experimentovat s různým nastavením osvětlení.

Uživatel může nastavovat aranžmá pro různé situace. Každou světelnou scénu si může uživatel navolit podle svých představ. Samozřejmostí jsou i přednastavené scény jako například televize, večeře, romantická večeře, čtení. Každou takovouto scénu lze dále upravit podle představ uživatele. Po navolení scény se upraví intenzita světla a barva, aby se navodila ta správná atmosféra. Pokud nebude navolané žádní scéna lze si nastavit základní osvětlení, které se přizpůsobuje fázi dne. Ráno je potřeba jasné světlo světlejší barvy, přes den není většinou potřeba žádné osvětlení, ale večer je potřeba příjemné tlumené světlo v teplejších barvách.

Kvůli zabezpečení je možné nastavit internval rozsvicení v místnosti, aby se simuloval pohyb osob po domě. Je možné nastavit každé místnost zvlášť, nebo posloupnost místností aby to vypadlo jako že někdo někam prochází. Když to nechce mít uživatel nastavené automaticky, může si zapínat jednotlivé místnosti pomocí aplikace. V rámci bezpečnosti lidí v domě zle nastavit i pohybové čidla například u schodů. Jakmile se někdo přiblíží ke schodům, do zóny, že půjde nahoru rosvítí se světlo na schodišti. Takhle to lze nastavit i pro chodbu, v tomto už

záleží pouze na uživateli. Když jsem u těch senzorů, tak je dobré pořídit i senzory pohybu do místností, aby se automaticky rozsvěcelo osvětlení ve chvíli kdy někdo příjde do místnosti.

Mnou vybraný systém osvětlení má i velkou funkcionalitu pro navození atmosféry, například při prohlížení fotek, kdy je na fotve zapadající slunce, dokáže osvětlení upravit aranžmá podle fotky, aby se dodal maximální požitek z prohlížení fotek. Další funkcionalitou je i nastavení časovače, když si uživatel naství, že chce upozornit za 20 minut, že se mu dovařilo jídlo, tak začlou blikat světla v místnosti a on, ví že si může dojít pro jídlo. Světla je možné nastavit i jako budík, kdy se světla, od určité hodiny, začnou rozsvěcovat. Postupně se pomalu zvyšuje intenzita až do maximálně nastavené intenzity.

Za pomoci vícekriteriální analýzy vybrané řešení Philips Hue White and Color ambiance starter kit obsahuje propojovací Hue Bridge, tři LED žárovky a Hue Dimmer Switch. Cena tohoto startovacího kitu je 5 200 Kč. Pro mnou navrhovanou domácnot je potřeba ještě dalších 42 žárovek. Cena jedné žárovky je 1 150 Kč. Takže pořizovací nákady na osvětlení činí 53 500 Kč. Avšak jedná se o žárovky s barevným spektrem, kdyby se vybíraly žárovky s pouze bílým spektrem. Cena jedné takové žárovky je 378 Kč. V tu chvíli by se ušetřilo 32 424 Kč jen na pořizovacích nákladech. Já však dal přednost komfortu uživatele s co možná nějvětší funkcionalitou, a proto jsem vybral žárovky celým barevným spektrem, i když jsou výrazně dražší. [45]

Systém Philips Hue navozuje příjemnou atmosféru v celé domácnosti. Přináší současněj jednoduché ovládání světel s řadou možností. Jakékoliv osvětlení se může stát designovým prvkem domácnosti. Mezi nesporné výhody je i to že na dálku může uživatel zjisti v jaké místnosti se vítí. Jak jsem již zmiňoval výše, tak po připojení senzorů pohybu se může efektivnost osvětlení zvýšit a tím se sníží náklady na elektrickou energii. Když vezmu v úvahu, že se svítí v průměru 8 hodin denně , tak je životnost žárovek 8,5 roku. Za předpokladu, že vydrží svojí životnost, tak se jedná o velkou finanční úsporu jak v oblasti elektrické energie, tak i v nákladech na koupi nových žárovek.

Senzor pohybu byl vybrán s ohledem na co nejlepší kompatibilitu také od společnosti Philips. Jedná se o model Philips Hue Motion Sensor. Cena tohoto senzoru je 1 041 Kč. Pro modelovou domácnost je potřeba 12 těchto senzorů v celkové ceně 12 492 Kč.

4.3.5 **Zabezpečení**

Nedílnou součástí chytré domácnosti je i zabezpečení. Bez něj by se neměla žádná chytrá domácnost objevit. Je potřeba zabezpečit domácnost jak před fyzickým útokem, tak i před kybernetickým útokem.

Pokud systém detekuje někoho v okolí domu, ve chvíli kdy by se tam neměl nikdo pohybovat, tak upozorní uživatele. Díky tomuto lze sledovat chytrou domácnost odkudkoliv pomocí aplikace a mít přehled nad tím, kde se kdo pohybuje. Většinou se využívají senzory pohybu a kamerové systémy. Jak jsem již zmínil výše senzory, které rozsvicí světla pokud se někdo nachází v místnosti, se dají využít i v případě sledování pohybu, zda se nenachází v domácnosti někdo kdo by tam neměl být. Se senzory pohybu by měli spolupracovat i kamery, které natočí útočníka a současně rozpoznají pohyb a informují oprávněnou osobu. Většinou se tato upozornění posílají formou SMS, popřípadě je možné i volání na číslo uživatele s předem definovanou zprávou. Je samozřejmostí, že uživatel si může odkudkoliv zapnout kameru a vidět, co se děje doma i okolo domu. Většina kamer je již vybavena i záznamem zvuku.

Pro tyto účely vyšlo nejlépe zakoupit dražší, ale za to kvalitnější kameru od společnosti Samsung. Jedná se o kameru Samsung SmartCam SNH-V6410PN, která svojí cenou přesahuje 4 650 Kč. Kamera disponuje možností otáčení a naklopení, takže rozsah je velmi dobrý. Rozlišení kamery je taky na dnešní poměru velmi dobré. Kamera zaznamenává v rozlišení 1920 x 1080 pixelů. Další výhodou této kamery je zaznamenávání jak ve dne tak v noci. Navíc je možné nastavit zónu sledování, takže kamera se bude sama natáčet v předem určeném zorném poli. V tuto chvíli je potřeba si dát pozor na nastavení, aby nevznikaly tzv. hluchá místa, kde by se mohl někdo schovávat a využít tak díru v bezpečnostním systému. Je potřeba i nastavit, aby se nespouštěl poplach ve chvíli kdy proběhne jen sousedův pes, kočka. Pro účely modelové domácnosti bude potřeba 6 kamer s celkovou cenou 27 900 Kč.

Součástí bezpečnosti je samozřejmě i elektronický portipožární systém. Využívají se jak detektory kouře, které jsou citlivé na jakýkoliv náznak kouře. Lepší variantou jsou hlásiče požáru s detektorem oxidu uhelnatého. Oxid uhelnatý je pro člověka velmi nebezpečný. Pokud se něco stane a začne hořet, detektor spustí hlasitou sirénu. A následně vyšle informace všem uživatelům chytr momácnosti upozornění na mobilní telefon i těm co se nenachází v objektu, aby věděli o nastálé situaci. Dají se však nastavit vyjímky například u vaření, aby se nespustil

alarm, ve chvíli kdy se připálí maso, buchta, atd. Z vícekriteriální analýzy vyšel nejlépe Elektrobock LM-201A, který se dá připojit k hubu a detekuje plyny, oxid uhličitý a teplotu, kdyby se zvýšila teplota, ale nebyl žádný kouř, tak žačne taky hlásit. Cena tohoto zařízení je 600 Kč za kus. V každé místnosti bude potřeba jeden detektor, takže bude potřeba 12 detektorů v celkové ceně 7 200 Kč.

Další částí zabezpečení je zamezení vstupu do domu, pro ty nemají povolená vstup. Domovní zámek je velmi důležity, existují varianty kdy je zámek připojený k internetu a uživatel, který má administrátorský přístup může kdykoliv kontrolovat, kdo prošel dveřmi a kdy. Popřípadě každý uživatel může otevřít dveře na dálku za pomoci mobilního telefonu. Jediné co je potřeba mít v telefonu digitální klíč. Lepší variantou je zámek, který může komunikovat s uživatelem přes bluetooth. Takže pokud se někdo přiblíží ke dveřím a má v kapse chytrý telefon s digitálním klíčem. Zámek se spojí s mobilním telefonem přes bluetooth a za předpokladu splnění podmínek výše uvedených, se zámek odemkne a uživatel může vejít dovnitř. Samozřejmě se zaznamená vstup oprávněné osoby. Pokud by byl vybitý mobilní telefon, nebo by nešel elektrický proud, lze se dostat do domu i pomocí klasického klíče. Nevýhoda je však ve chvíli kdy uživatel ztratí mobilní telefon. Jde smazat přístup daného telefonu z aplikace, ale je zde otázka zda bude uživatel rychlejší než zloděj. Existují i řešení, které mají kameru aby uživatel viděl, kdo stojí přede dveřmi a komu by měl uživatel otevřít. Otevřít může někomu i na dálku, pomocí aplikace v mobilním telefonu.

Na základě vícekriteriální analýzy vyšel jako vítěz August Smart Lock Pro + Connect, který má podporu Bluetooth, WiFi, Z-Wave a Apple HomeKit. Lze využít lelefon pro odemykání na dálku pomocí aplikace, tak na blízko pomocí bluetooth. Cena tohoto zámku je 5 120 Kč. S tím že za bezpečnost je potřeba si připlatit. [46]

4.3.6 **Chytré spotřebiče**

Mezi chytré spotřebiče, které se dají využít v chytré domácnosti lze počítat inteligentní lednici o které jsem se již jednou zmiňoval, inteligentní myčku, pračku, sušičku, troubu televize. Cokoliv co se dá připojit k internetu se dá považovat za chytré zařízení. Vybírat zařízení, které by měli uživatelé využívat v domácnosti, jako je chytrá lednice je skoro nemožné, protože každý očekává od zařízení něco jiného. Pro někoho je důležitější objem, pro někoho energetická třída, pro někoho barva a velikost, aby pasovala do kuchyně. Proto jsem neporovnával mezi sebou chytré spotřebiče. Je určitě dobré je mít ale je potřeba aby si každý předtím než si vybere

svojí chytrou domácnost promyslel co od ní očekává. Co by měla splňovat a jaké spotřebiče potřebuje využívat.

Mezi tyto spotřebiče by šel zařadit i robotický vysavač, který jezdí celý den po domě a vysává nečistoty. Pomocí WiFi sděluje svojí polohu v domě a zaznamenává, kde ještě nevysával. Sám rozpozná kolik mu zbývá energie a v případě zadokuje a dobije se. Jediné co potřebuje po uživateli je aby ho při nahlášení plnosti zásobníku vysypal.

4.3.7 **Zahrada**

Chytrou domácnost lze rozšířit i na zahradu, kdy senzory mohou hlídat vlhkost půdy, množství závlahy, automatické zavlažování, automatické sečení trávy za pomoci robota. Zavlažování se řídí i pomocí meteorologických stanic, kterou je potřeba kontaktovat aby se zjistilo, zda bude pršet, pokud v předpovědi nemá pršet, spustí se zavlažovací systém. Problém nastává ve chvíli, kdy bude porušená hadice, čidlo detekuje že je potřeba závlaha, a voda teče pořád dál. Čím se plýtvá vodou a zároveň i penězi.

Automatické sekání lze zajisti robotem, který jezdí po zahradě celý den, pokud je sucho a zkracuje trávu o předem nastavenou velikost. Takhle vyjíždí každý den a jezdí po celé zahradě. Tento robot potřebuje natáhnout po zahradě drát, kde na principu indukce detekuje zakázanou zónu a dál nejede. To je proto aby nespadl například ze srázu, do jezírka, nebo nejel někam kam nemá. Proto je na začátek potřeba investice do instalace, poté je již na robotovi aby jezdil po zahradě. Tento robot dává vědět kde se nachází, protože většinou obsahuje i GPS modul. Za pomoci WiFi pak odesílá uživateli data o tom kde sekal a jaká byla v daném místě vlhkost. Cena takovýchto robotů začíná na 25 000 kč ale není problém najít roboty které stojí okolo 80 až 100 tisíci korun. V tu chvíli je potřeba popřemýšlet, zda to je potřeba vůbec kupovat. Zda není lepší vymezit si čas a jednou za týden celou zahradu přejet normální sekačkou na trávu, v případě větší zahrady zahradním traktůrkem.

5 Výsledky a diskuse

V předchozích kapitolách jsem nastínil jaký internet věcí je. A jak dokáže komunikovat. Přiblížil jsem pojem chytrá domácnost, komponenty které se využívají v chytré domácnosti. Přiblížil jsem historii, jak se internt věcí vyvíjel. Důležitá kapitola je bezpečnost a soukromí, kde jsem nastínil problémy spjaté s internetem věcí. Neméně důležitou kapitolou je využití internetu věcí, kde jsem tuto oblas rozdělil na dvě odvětví a to na průmyslová internet věcí a na spotřebitelský internet věcí. V každé kapitole jsem popsal čím se jednotlivé odvětví specifikuje a čím se liší. Je potřeba aby si každý uvědomil kde je internet věcí okolo něj. S internetem věcí se každý potkává každý den, a ani si toho neuvědomuje, a proto je potřeba větší osvěta tohoto fenoménu. Jedná se totiž i o bezpečnost, protože většina lidí ani neví kolik informací se o nich v jejich nevědomí shromažďuje.

Náklady na pořízení modelové chytré domácnosti i se započítáním tvorby vlastního zařízeny činí 162 256 Kč. Veškeré uvedené ceny jsou uváděny s DPH. Vybírané komponenty byli z kategorie centrální ovládací systém, vytápění, osvětlení, zabezpečení. Tyto kategorie by se dali nazvat jako ty nejdůležitější a dokáží uspořit nejvíce energií a tím i peněz.

Název komponenty	**Cena (Kč)**
Hub - D-Link DCH-G020	2 000,00 Kč
Vytápění - Honeywell Evohome	22 568,00 Kč
Klimatizace - Frigidaire FGRC1044T1 Cool Connect	31 200,00 Kč
Osvětlení - Philips Hue White and Color ambiance	53 500,00 Kč
Pohybová čidla - Philips Hue Motion Sensor	12 492,00 Kč
Kamery - Samsung SmartCam SNH-V6410PN	27 900,00 Kč
Detektro kouře - Elektrobock LM-201A	7 200,00 Kč
Zámek - August Smart LockPro + Connect	5 120,00 Kč
Vlastní zařízení - Meteostanice	276,00 Kč
Cena celkem	**162 256,00 Kč**

Tabulka 3 - Náklady na chytrou domácnost

Je potřeba aby se lidé zamysleli nad tím zda chtějí peníze investovat do chytrých domácností, zda jsou ochotní vynakládat další peníze za komfort uživatelů. Jsou lidé ochotni omezit svou svobodu na úkor komfortu? To je zásadní otázka, kterou je potřeba si klást. Záleží už jen na uživatelích jak moc chtějí svou chytrou domácnost využívat někomu stačí osvětlení a topení. Jiní chtějí mít domácnost plně automatizovanou, aby se nemuseli starat o nic. Je pouze na finančních možnostech jednotlivců, jak si sestaví svojí chytrou domácnost. Mé řešení chytré

domácnosti se dá považovat za takový standart, určitě by se dali jednotlivé komponenty sehnat levněji, avšak ne s plnou funkcionalitou, jakou mám ve své práci já. Záleží však na velikosti domu, na kterou se bude aplikovat chytrá domácnost. Je lepší počítat už při výstavbě s prvky chytré domácnosti, aby se nemusli následně provádět stavební práce znovu.

Budoucnost internetu věcí je nejistá, avšak dá se předpokládat, že se internet věcí bude i nadále rozšiřovat dále do společnosti. Lidé ho budou využívat stále častěji a bude jim ulehčovat život. Již dnes se tak děje. Velkou oblastí kde se dá internet věcí i nadále využívat je průmyslový internet věcí, kde se zatím jen lehce ukazují jeho možnosti. Využití je v tomto odvětví nepřeberné množství, jak jsem již nastínil v kapitole věnované tomuto tématu, ale myslím si že se má i nadále kam rozvíjet. V rámci české republiky je určitě dost prostoru pro další rozšiřování. V oblasti spotřebitelského internetu věcí je taky ještě dost prostoru na rozšíření, jelikož moc lidí netuší co to vůbec je. Já osobně bych se snažil využít internet věcí na maximum s ohledem na bezpečnost a soukromí uživatele.

Nákupem součástek na čínských eshopech se dají ušetřit peníze, ale je počítat s tím, že dodací lhůta se může protáhnout. Moje zkušenost byla dobrá, ale nemusí tomu tak být vždy. Proto je potřeba aby si každý uvážil, zda se mu vyplatí a je ochoten objednávat z Číny.

6 Závěr

Hlavním cílem této práce bylo představit fenomén internetu věcí, v dnešní době asi jedno z nejdiskutovanějších témat, jeho možný budoucí vývoj. Hlavní cíl je zpracován v teoretické části. Praktická část je věnována dílčím cílům a to přesněji tvorbě modelové chytré domácnosti. V praktické části jsem i vytvořil zařízení splňující standart internetu věcí. Toto zařízení je schopné integrovat se do stávající chytré domácnosti.

Je jasné že některé věcí, které jsou v práci zmíněny jsou myšleny do budoucnosti, protože zatím se nedají tyto myšlenky realizovat, avšak v blízké budoucnosti tomu bude doufejme jinak. Díky této práci jsem získla rozsáhlé znalosti v oblasti internetu věcí. Na tyto znalosti jsem navázal v praktické části, kde jsem z nich těžil. Díky praktické části se mé vědomosti o internetu věcí prohloubily.

Praktická část mi otevřela oči s tím, že je možné s trochou snahy vytvořit chytrou domácnost za ne velký finanční obnos. Současně se prohloubily moje znalosti z odvětví elektrotechniky a zjistil jsem že není těžké sestrojit zařízení, které by splňovalo nároky internetu věcí. Navíc pokud se součástky objednají z čínských eshopů, tak se dá i výrazně ušetřit. Ale jak říkám záleží na jedinci, jaké má priority. Zajímavé zjištění bylo že se nejvíce využívají systémy, které ovládají celý dům jako je například osvětlení, topení. Největší potenciál bych viděl v inteligentních spotřebičích, které dokáží velmi efektivně ušetřit svým uživatelům čas, náklady a zvýší komfort žití.

Provedl jsem i finanční náročnost mého řešení inteligentí domácnosti. Finanční návratnost je jistě velmi důležitá, avšak tímto se tato práce již nezabývala, to by bylo na další práci. Je jasné že většina chytrých domácností by se měla vyrovnat své investici v řádu let, maximálně desetiletí. Předělávat starší domácnost na chytrou se nemusí vyplatit, proto je potřeba provést analýzu zda je možná nějaká návratnost.

Dosah internetu věcí je neomezený, nebo se aspoň tak zdá. V blízké budoucnosti se s internetem věcí setkáme takřka všude. Sice se internet věcí teprve rozíjí do běžného života, ale naštěstí to již není vize vzdálené budoucnosti, ale rychle nastupující realita. Je to jednoznačně směr, kudy se bude odvětví informačních technologií ubírat.

7 Seznam použitých zdrojů

1. Internet of Things [online]. Gartner, Inc. [cit. 2017-07-10]. Dostupné z: http://www.gartner.com/it-glossary/internet-of-things
2. The Internet of Things: In a Connected World of Smart Objects [online]. Fundación de la Innovación Bankinter. 2011. [cit. 2017-07-10]. Dostupné z: http://www.fundacionbankinter.org/system/documents/8189/original/XV_FTF_Internet_o_of_things.pdf
3. POHANKA, Pavel. Internet věcí. In: Pavel Pohanka [online]. 2015. [cit. 10. 7. 2017]. Dostupné z: http://i2ot.eu/internet-of-things/
4. NOVAK, Matt. Nikola Tesla's incredible predictions for our connected world. In: Paleofuture [online]. 2015. [cit. 2017-07-10]. Dostupné z: http://paleofuture.gizmodo.com/nikola-teslas-incredible-predictions-for-our-connected-1661107313
5. ASHTON, Kevin. That „Internet of Things" Thing. In: RFID Journal [online]. 2009. [cit. 15. 7. 2017]. Dostupné z: http://www.rfidjournal.com/articles/view?4986
6. Gartner Says 6.4 Billion Connected "Things"Will Be in Use in 2016, Up 30Percent From 2015 [online]. Gartner, Inc. 2015. [cit. 2017-07-10]. Dostupné z: http://www.gartner.com/newsroom/id/3165317
7. EVANS, Dave. The Internet of Things how the next evolution of the Internet is changing everything. In: Cisco [online]. 2011. [cit. 2017-07-10]. Dostupné z: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
8. FRENZEL, Lou. The Connected World Awaits. In: Electronic Design [online]. 2014. [cit. 20. 7. 2017]. Dostupné z: http://electronicdesign.com/iot/connected-world-awaits
9. DOLÁK, Ondrej. Big data: Nové zpusoby zpracování a analýzy velkých objemu dat. In: SystemOnline [online]. 2011. [cit. 2017-07-20]. Dostupné z: http://www.systemonline.cz/clanky/big-data.htm
10. ZANDL, Patrick. Internet vecí - Internet of Things. In: Lupa [online]. 2009. [cit. 2017-07-20]. Dostupné z: http://www.lupa.cz/clanky/internet-veci-internet-of-things/
11. PACELLE, Mark. 3 topologies driving IoT networking standards. In: Radar [online]. 2014. [cit. 2017-07-20]. Dostupné z: http://radar.oreilly.com/2014/04/3-topologiesdriving-iot-networking-standards.html
12. CHERUVATHOOR, Joy. IoT and M2M – are they the same?. In: Joy Rajanv heruvathoor [online]. 2015. [cit. 2017-07-20]. Dostupné z: http://joycheruvathoor.com/2015/10/31/iot-and-m2m-are-they-the-same/
13. Sparkfun. *Sparkfun* [online]. [cit. 2017-08-14]. Dostupné z: https://cdn.sparkfun.com/assets/learn_tutorials/5/3/4/Zigbee-topologies.png
14. RF Wireless World. *RF Wireless World* [online]. 2017 [cit. 2017-08-14]. Dostupné z: http://www.rfwireless-world.com/Terminology/Bluetooth-5-vs-bluetooth-4-2.html
15. Svět Androida. *Svět androida* [online]. 2017 [cit. 2017-08-15]. Dostupné z: https://www.svetandroida.cz/bluetooth-5-201706/
16. TRČÁLEK, Antonín a Dušan KOS. Živě.cz. *Nový standard Wi-Fi: Gigabit vzduchem* [online]. 2012 [cit. 2017-08-15]. Dostupné z: https://www.zive.cz/clanky/novy-standard-wi-fi-gigabit-vzduchem/sc-3-a-165687/default.aspx
17. Nová wi-fi 802.11ax slibuje 40% nárůst rychlosti. WPA 3 zvýší bezpečnost. *Technet cz* [online]. 2018, 31.1.2018 [cit. 2018-01-20]. Dostupné z: Zdroj: https://technet.idnes.cz/wi-fi-802-11ax-a-wpa3-02b-/kratke-zpravy.aspx?c=A180108_141832_tec-kratke-zpravy_vse

18. GISLASON, Drew. *Zigbee wireless networking*. New York: Elsevier, Newnes, 2008. ISBN 978-0-7506-8597-9.
19. VOJÁČEK, Antonín. ZigBee - novinka na poli bezdrátové komunikace. In: *Vyvoj.hw.cz* [online]. [cit. 2018-01-20]. Dostupné z: https://vyvoj.hw.cz//navrh-obvodu/rozhrani/zigbee-novinka-na-poli-bezdratove-komunikace.html
20. O'Mara, D.: Z-Wave, All the Rage. Security Dealer & Integrator[online]. Fort Atkinson: SouthComm Business Media LLC, 2013[cit. 2018-01-20]35(6): s. 38–39, ISSN 19410891.
21. ZigBee. En.wikipedia.org [online]. wikipedia.org, 2016 [cit. 2018-01-20]. Dostupné z: https://en.wikipedia.org/wiki/ZigBee
22. PAVLIS, Jakub. WiGig – je bezdrátové HD opravdu o něco blíže?. In: *Notebook.cz* [online]. 9. 4. 2015 [cit. 2018-01-20]. Dostupné z: https://notebook.cz/clanky/technologie/2015/wigig-IEEE-802-11-ad
23. VOJÁČEK, Antonín. SIGFOX - princip, struktura, protokol, použití. In: *Vyvoj.hw.cz* [online]. 26.5.2017 [cit. 2018-01-20]. Dostupné z: https://vyvoj.hw.cz/sigfox-princip-struktura-protokol-pouziti.html
24. Internet vecí klepe na dvere, v bezpecnosti ale kulhá na obe nohy [online]. Ekonomický deník. 2015. [cit. 2018-01-20]. Dostupné z: http://ekonomicky-denik.cz/internet-veciklepe-na-dvere-v-bezpecnosti-ale-kulha-na-obe-nohy/
25. Missing Children Europe [online]. 2014 [cit. 2018-01-20]. Dostupné z: http://missingchildreneurope.eu/
26. ISHAQ, Isam, David CARELS, Girum TEKLEMARIAM, Jeroen HOEBEKE, Floris ABEELE, Eli POORTER, Ingrid MOERMAN a Piet DEMEESTER. IETF Standardization in the Field of the Internet of Things (IoT): A Survey. Journal of Sensor and Actuator Networks [online]. 2013, vol. 2, issue 2, s. 235-287 [cit. 2018-02-14]. DOI: 10.3390/jsan2020235. Dostupné z: http://www.mdpi.com/2224-2708/2/2/235/
27. KARIMI, Kaivan, Gary ATKINSON. What Does Internet of Things (IoT) Needs to Become a Reality. : INTOTHNGSWP [online]. 2013, rev 1, 15 s. [cit. 2018-02-14]. Dostupné z: http://www.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf
28. RUIFROK, Ewoud. The house of tomorrow. In: Faculty of architecture TU Delft [online]. 2015. [cit. 2018-02-14]. Dostupné z: http://bertbon.home.xs4all.nl/hyperbody/student_papers/Ewoud%20Ruifroklitrature&media.pdf
29. Smartphones overtake 'dumb' phones worldwide [online]. Guardian. 2013. [cit. 2018-02-14]. Dostupné z: http://www.guardian.co.tt/business/2013-04-29/smartphonesovertake-%E2%80%98dumb%E2%80%99-phones-worldwide
30. STEINER, Štefan. Moderní a chytrá mesta. In: Parlament, vláda, samospráva [online]. 2011. [cit. 2018-02-14]. Dostupné z: http://www.parlament-vlada.eu/index.php/hlavnitemata-stavebnictvi/211–moderni-a-chytra-msta
31. BLÁHA, Lukáš. Smart Cities – Chytrá města budoucnosti. In: SystémOnLine [online]. 9/2016 [cit. 2018-02-14]. Dostupné z: https://www.systemonline.cz/clanky/smart-cities-chytra-mesta-budoucnosti.htm
32. CIBULKA, Jan. Praha testuje 'chytré' odpadkové koše, půjčení jednoho přijde na 75 tisíc na půl roku. In: *Irozhlas* [online]. 29.8.2017 [cit. 2018-02-14]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/praha-testuje-chytre-odpadkove-kose-pujceni-jednoho-prijde-na-75-tisic-na-pul_1708290600_cib
33. Myslíme na budoucnost [online]. Volvo. 2015. [cit. 2018-02-14]. Dostupné z: http://www.volvocars.com/cz/o-nas/nase-pribehy/inovace-pro-lidi/myslime-nabudoucnost

34. TRCÁLEK, Antonín. Google není jediný, kdo vyvíjí chytrá auta budoucnosti. In: Zive.cz [online]. 2013. [cit. 2018-02-14]. Dostupné z: http://www.zive.cz/clanky/google-nenijediny-kdo-vyviji-chytra-auta-budoucnosti/sc-3-a-170245/default.aspx
35. Best smart clothes: Wearables to improve your life [online]. Pocket-lint. 2016. [cit. 2018-02-14]. Dostupné z: http://www.pocket-lint.com/news/131980-best-smart-clotheswearables-to-improve-your-life
36. Fitbit Ionic Charcoal Smoke-Gray, In: *Alza.cz* [online]. [cit. 2018-02-14]. Dostupné z: https://cdn.alza.cz/ImgW.ashx?fd=f4&cd=SPTFTB002&i=1.jpg
37. HRON, Lukáš, Fitbit dále požírá konkurenci. Koupil výrobce luxusních chytrých hodinek. In: Irozhlas [online]. 19.1.2017 [cit. 2018-02-14]. Dostupné z: https://mobil.idnes.cz/fitbit-koupe-vector-luxusni-chytre-hodinky-fzp-/mob_tech.aspx?c=A170110_153037_mob_tech_LHR
38. Apple Watch Series 3, In: Apple [online]. [cit. 2018-02-14]. Dostupné z: https://store.storeimages.cdn-apple.com/4662/as-images.apple.com/is/image/AppleInc/aos/published/images/4/2/42/alu/42-alu-space-nike-anth-black-nc-gallery1?wid=1000&hei=1000&fmt=jpeg&qlt=95&op_usm=0.5,0.5&.v=1504983237239
39. Samsung Gear S3, In: *Alza.cz* [online]. [cit. 2018-02-14]. Dostupné z: https://cdn.alza.cz/ImgW.ashx?fd=f4&cd=SAAW0013a&i=1.jpg
40. Garmin Fenix 5X, In: *Alza.cz* [online]. [cit. 2018-02-14]. Dostupné z: https://cdn.alza.cz/ImgW.ashx?fd=f4&cd=PP5779d07&i=1.jpg
41. VALEŠ, Miroslav. Inteligentní dum potrebuje inteligentní návrh. In: IQdum [online]. 2013. [cit. 2018-02-14]. Dostupné z: http://www.iqdum.cz/inteligentni-dum-lidovenoviny/
42. Šestý den. In: *CSFD* [online]. 2000 [cit. 2018-02-14]. Dostupné z: https://www.csfd.cz/film/12342-6-den/prehled/
43. PARKER, Mitchell. CES 2015: Inching toward a smarter home. In: Houzz [online]. 2015.[cit. 2018-03-30]. Dostupné z: http://www.houzz.com/ideabooks/37829929/list/ces-2015-inching-toward-a-smarter-home
44. GRIFFITH, Eric. How to Build Your Smart Home: A Beginner's Guide. In: PCMag [online]. 2016. [cit. 2018-03-30]. Dostupné z: http://www.pcmag.com/article2/0,2817,2410889,00.asp
45. PHILIPS HUE [online]. Ledko. 2015. [cit. 2018-03-30]. Dostupné z: http://www.ledko.cz/philips-hue-0/
46. August [online]. August Home. 2016. [cit. 2018-03-30]. Dostupné z: http://august.com/