Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informatiky a kvantitativních metod

Mobilní Cloud Computing

Diplomová práce

Autor: Tomáš Dittrich
Studijní obor: Aplikovaná informatika

Vedoucí práce: doc. Mgr. Tomáš, Kozel, Ph. D.

Hradec Králové listopad 2016

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

Podpis

V Hradci Králové dne 11. 11. 2016 Tomáš Dittrich

Poděkování

Děkuji vedoucímu diplomové práce doc. Mgr. Tomáši Kozlovi, Ph.D. za cenné rady, náměty, připomínky a metodické vedení práce a také za věnovaný čas.

Anotace

Tato diplomová práce se zabývá problematikou mobilního cloud computingu ve vazbě na koncept internet věcí. Práce se snaží o vymezení pojmů mobilní cloud computing a internet věcí a dále pak pojednává o možnostech a oblastech jejich využití. V druhé části práce je pak pojednáváno o problematice zpracování velkého objemu dat a také o problematice bezpečnosti celého konceptu.

Annotation

Title: Mobile Cloud Computing

This diploma thesis deals with the issue of the Mobile Cloud Computing in relation to the concept Internet of Things. This work attempts to define the terms Mobile Cloud Computing and Internet of Things and then deals with the possibilities and areas of their use. In the second part, problems of processing large volumes of data and also the issue of security of the whole concept are discussed.

Obsah

1 Úvod

Fenoménem současnosti informačních a komunikačních technologií se staly pojmy Cloud Computing a Internet věcí (IoT). Do tohoto odvětví jsou investovány nemalé finanční prostředky a do vývoje software, hardware a infrastruktury se zapojily nejen velké nadnárodní IT společnosti, ale také mnoho startupů, open source projektů apod. Celý tento segment se rozvíjí ohromnou rychlostí, a jednotliví účastníci se předhánění ve vydávání nových, lepších, úspornějších zařízení a služeb.

O konceptu internetu věcí slýcháváme každý den a výrobci elektroniky se jej snaží implementovat do stále více svých výrobků. Velmi často bývá internet věcí spojován s konceptem chytrých domácností.

Cílem této práce je objasnit, co jednotlivé pojmy Cloud Computing, mobilní Cloud Computing a Internet věcí znamenají a jak je lze společně propojit. A také poukázat na možnosti a oblasti jejich využití v běžném životě. IoT zařízení bývají často vybaveny senzory umožňující měření a regulaci. V této práci je též pojednáváno o problematice zpracování velkého objemu dat. Kdy objemem samotných dat není myšlena jejich velikost, ale množství. Sběr údajů z jednotlivých senzorů IoT zařízení může generovat značné množství zpráv. Jak se s takovýmto problémem vypořádat a jak je efektivně ukládat a zpracovávat je pojednáváno v druhé části této práce. V neposlední řadě práce pojednává o problematice bezpečnosti celého konceptu. Bezpečný přenos dat, ochrana proti zneužití či kompromitaci zařízení je velmi důležitá, bohužel je velmi často podceňovanou záležitostí.

2 Cloud computing

Cloud computing se stal velmi rozšířeným modelem v IT oblasti. Tato kapitola se zabývá definicí samotného pojmu a také modelem služeb a nasazení, které nabízí. V této kapitole se vychází z bakalářské práce[1] autora.

2.1 Definice pojmu

Definici Cloud Computingu je možné vybírat z celé řady zdrojů. Za uznávanou a často citovanou definici, je považována definice organizace National Institute of Standards and Technology (NIST) [1]:

„Cloud computing je model umožňující pohodlný, síťový přístup na požádání do sdílené paměti konfigurovatelných výpočetních zdrojů (např. sítě, servery, úložiště dat, aplikací a služeb), které lze rychle zásobit a uvolnit s minimálním manažerským úsilím a řízením nebo interakcí s poskytovatelem služeb. Tento cloud model podporuje dostupnost a skládá se z pěti základních charakteristik, tří užitných modelů a čtyř modelů rozmístění.“

V české verzi Wikipedie je pojem Cloud computing definován takto: [2]

„Cloud computing je na internetu založený model vývoje a používání počítačových technologií. Lze ho také charakterizovat jako poskytování služeb či programů servery dostupnými z internetu s tím, že uživatelé k nim mohou přistupovat vzdáleně, kupř. pomocí webového prohlížeče nebo klienta elektronické pošty. Za předpokladu, že služba je placená, uživatelé neplatí za vlastní software, ale za jeho užití.

Principem u služeb a produktů v cloud computingu je to, že uživateli propůjčují výpočetní výkon serverů. V mnoha případech se tak děje formou specializovaných aplikací, jejichž nabídka se pohybuje od kancelářských aplikací přes systémy pro distribuované výpočty až po operační systémy provozované v prohlížečích, jakými jsou např. eyeOS, Cloud či iCloud.“

Další možné vysvětlení pojmu Cloud computing: [3]

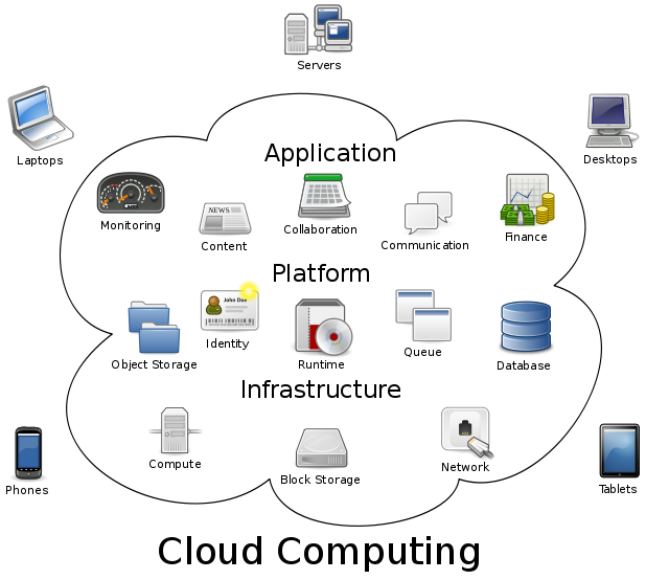
„Představte si svět, kde vaše aplikace již nejsou omezovány hardwarem i softwarem a můžete je využívat bez ohledu na výpočetní výkon, který je třeba, a když je třeba.

[1] Migrace aplikací do prostředí Cloudu

Představte si svět, kde se platí pouze za výpočetní výkon, který jste použili (Pay as You Go). Představte si, že není třeba se starat o správu hardwarové infrastruktury a můžete se zaměřit na software, který se u Vás objeví. V tomto světě můžete posunout svou pozornost od správy serverů na správu aplikace.“

Technologie Cloud computingu se vyznačuje následujícími atributy [2]:

- Multitenancy - jedná se o to, že počítačové zdroje jsou sdílené mezi všemi uživateli.
- Obrovská škálovatelnost a elasticita - umožní uživatelům rychle změnit výpočetní zdroje dle potřeby.
- Pay as you go - tento přístup je založen na principu kolik uživatel spotřebuje, tolik zaplatí.
- Aktuálnost (Up-to-date) - všechen software je automaticky aktualizovaný, uživatel nemusí do tohoto procesu nijak zasahovat, vše zařídí poskytovatel.
- Přístup přes internet - uživatelé se mohou ke svému softwaru připojit kdekoliv po celém světě.



Obrázek 1 - Znázornění cloud computingu (Zdroj: [2])

Za Cloud computing nelze považovat Network computing a Grid computing.

Network computing - aplikace jsou uloženy jen na lokálních firemních serverech a přístupny jen v rámci firemní sítě.

Grid computing - forma distribuovaných a paralelních výpočtů, přičemž "virtuální super počítač" se skládá ze seskupení propojených sítí.

2.2 Model služeb

Model popisuje, co je v rámci služby nabízeno, obvykle software nebo hardware, či jejich kombinace. Znázornění Cloud computingu s vymezenými modely služeb je znázorněna na obrázku 1. Následující text je napsán s využitím zdrojů [2] a [4].

2.2.1 IAAS

Infrastruktura jako služba (angl. Infrastructure as a Service) – je služba nabízející vizualizovanou, hardwarovou infrastrukturu (servery, úložiště, sítě). Poskytovatel služby je odpovědný za správu a provoz. Konzument služby nevlastní hardware, ale jen software či licence k software.

2.2.2 PAAS

Platforma jako služba (angl. Platform as a Service) – je škálovatelná služba, která poskytuje prostředky pro vývoj a následnou údržbu vlastních aplikací prostřednictvím internetu. Příkladem služby může být databázový systém provozovaný jako služba.

2.2.3 SAAS

Software jako služba (angl. Software as a Service) – je služba, kdy je hostovaná aplikace nabízena zákazníkovi formou pronájmu přes internet. Zákazník nekupuje software, ale přístup k němu formou služby. Výhodou tohoto řešení je možnost krátkodobého pronájmu a také aktuálnost (nejnovější verze).

2.3 Modely nasazení

Model nasazení definuje, jak je cloud poskytován. Lze jej rozdělit do čtyř základních oblastí:

- Veřejný
- Privátní
- Hybridní
- Komunitní

2.3.1 Veřejný cloud

Veřejný cloud je model poskytující veřejné služby přes internet. Služby mohou být poskytovány jak bezplatně, tak za úplatu dle konkrétního využití dané služby.

Mezi nejvýznamnější poskytovatele veřejného cloudu patří tyto společnosti:

- Amazon
- Microsoft
- Google
- IBM
- Oracle
- Apple

2.3.2 Privátní cloud

Privátní (soukromý, interní) cloud je provozovaný nějakou organizací (společnost, vládní instituce), která má specifické požadavky na jednotlivé služby. Mezi specifické požadavky se může řadit fyzické uložení dat (místo provozu datového centra), či síťová konektivita (latence) apod. Infrastruktura je spravována samotnou organizací, nebo jiným subjektem.

2.3.3 Hybridní cloud

Hybridní cloud je kombinace veřejného a privátního cloudu. Část služeb je u tohoto modelu provozována v cloudu a část na jiném místě. Za jiné místo lze považovat např. jiné datové centrum, či provozování lokálních služeb na serverech dané organizace (On-premise).

2.3.4 Komunitní cloud

Komunitní cloud je model, u kterého je infrastruktura sdílena více institucemi se stejnými zájmy.

2.4 Historie

Základní myšlenka cloud computingu sahá až do roku 1960, kdy John McCarthy vyjádřil, že by bylo možné výpočetní úlohy organizovat jako veřejnou službu. Název „mrak“ (cloud) byl převzat od telefonních společností, do roku 1990 přednostně nabízejících datové okruhy pro přímé spojení mezi dvěma síťovými uzly, které začaly propagovat svoje privátní virtuální sítě (sdílení pásma). Symbol mraku byl použit jako znázornění bodů, mezi kterými byla oddělena zodpovědnost poskytovatele od uživatele.

Firma Amazon hrála klíčovou roli ve vývoji cloud computingu prostřednictvím modernizace svých datových center, která stejně jako většina počítačových sítí používala v každém okamžiku jen 10% své kapacity a to z důvodu ponechání si prostoru pro příležitostné špičky. Po zjištění, že nová architektura cloud computingu má za následek značné zlepšení vnitřní efektivity, Amazon začal v roce 2005 poskytovat přístup ke svým systémům přes Amazon Web Services. [5]

3 Mobilní Cloud Computing

Mobilita se stala významným pojmem v počítačovém světě. S rozvojem hardware a software mobilních zařízení, se tato zařízení svým výkonem přibližují počítačům s klasickou konstrukcí (desktop). I přes tento pokrok mobilní hardware není primárně určen k náročným a déletrvajícím výpočtům. Mobilní zařízení jsou často limitována napájením z baterie. Proto se nabízí otázka, jak náročné výpočty, práce s daty a jejich trvalé uložení provádět mimo mobilní zařízení Tato kapitola pojednává o možnostech využití mobilního cloud computingu.

3.1 Definice pojmu

Na úvod je nutné říci, že neexistuje žádná přesná definice co je Mobilní Cloud Computing.

Mobilní Cloud Computing (MCC) – je kombinace Cloud computingu, mobilního computingu a bezdrátových sítí pro získání dodatečných výpočetních zdrojů pro mobilní uživatele. [6] Jedná se o infrastrukturu, kde ukládání a zpracování dat se provádí mimo mobilní zařízení.

Mobile Computing (mobilní computing nebo také mobilní počítání) je způsob využívání malých, přenosných a bezdrátových počítačových a komunikačních zařízení, jako jsou například tablety, smartphony, PDA, atd. Tato zařízení jsou pomocí bezdrátové technologie připojena k internetu či podnikové síti. To umožňuje uživatelům mobilních zařízení okamžitý přístup k podnikovému obsahu a k aplikacím daného podniku nezávisle na lokaci. [7]

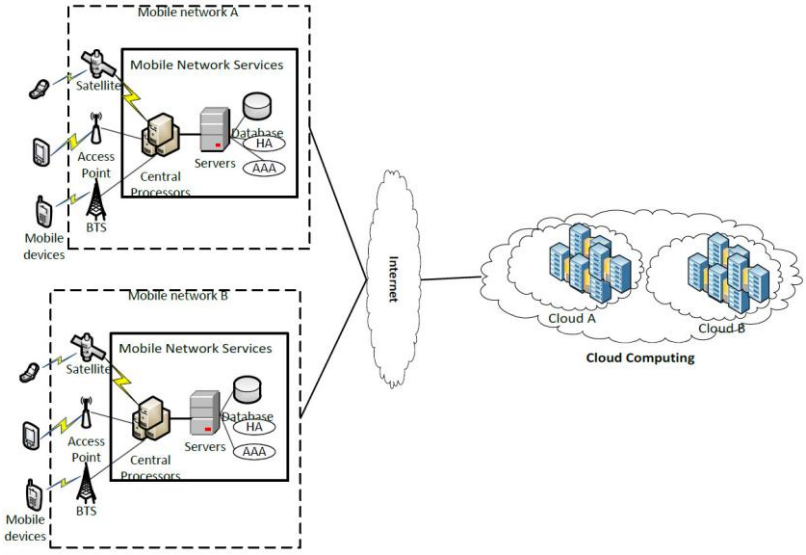
Hlavní rozdíl mezi mobilním computingem a mobilním cloud computingem je v tom, že mobilní computing využívá nativní aplikace v mobilním zařízení, tedy výpočetní výkon i ukládání dat v tomto zařízení. Naproti tomu MCC přenáší výpočetní výkon a ukládání dat mimo mobilní zařízení, tedy do cloudu. V infrastruktuře cloudu je možné provádět výpočetně náročnější operace a ukládání dat. Aplikační data jsou

umístěna v cloudu a výsledky jsou předávány do mobilních zařízení přes mobilní či jiné bezdrátové sítě s přístupem do internetu.

Nabízí se otázka, proč je vlastně vhodné používat MCC místo MC. Hlavním argumentem může být výdrž mobilního zařízení na baterie a s ním spojená úspora, úspora úložiště v mobilním zařízení. Dalším argumentem hovořící pro cloud je pak spolehlivost, dostupnost, bezpečnost a škálovatelnost celého řešení. Data uložená mimo fyzické mobilní zařízení jsou tak chráněna proti ztrátě či poškození zařízení a také přístupna z jiných zařízení či aplikací. Velmi významné kritérium tvoří samotné zabezpečení dat a také případná integrace s jinými systémy. V neposlední řadě použití cloudu přináší dynamické účtování za používání služeb dle konkrétní spotřeby (výpočetní výkon, úložiště, apod.).

3.2 Architektura mobilního cloud computingu

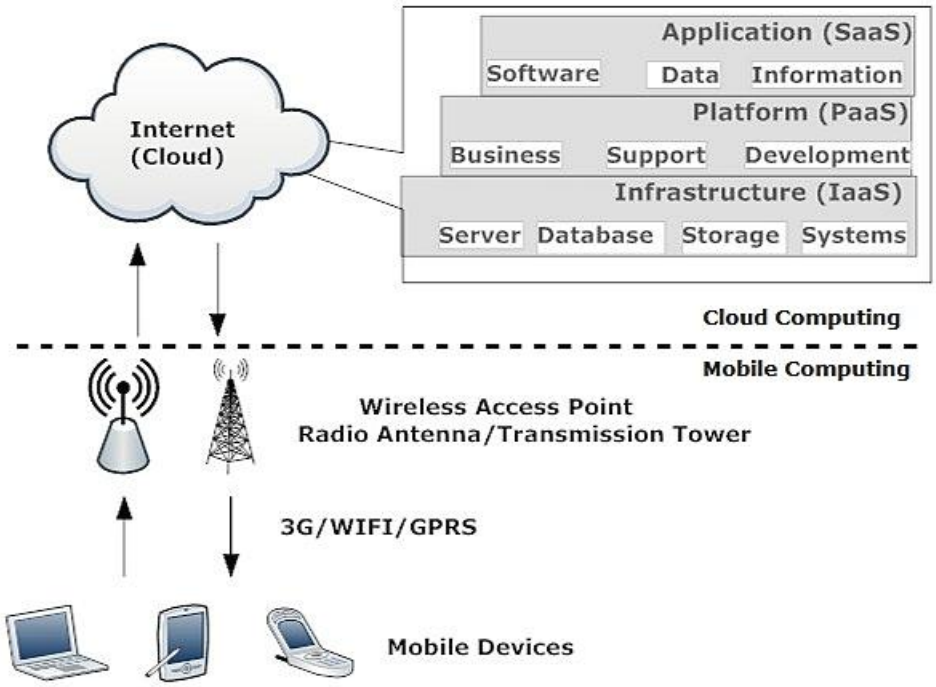
Mobilní zařízení jsou připojena do mobilní sítě prostřednictvím základnových stanic BTS[2], které zajišťují spojení mezi sítěmi a mobilním zařízením. Požadavky mobilních zařízení jsou přenášeny na servery zajišťující mobilní síťové služby. Z těchto serverů jsou požadavky dále doručovány do cloudu přes internetovou konektivitu. V cloudu dochází ke zpracování požadavků na konkrétní cloudové službě. Na obrázku 2 je znázorněna architektura mobilního cloud computingu.



Obrázek 2 - Architektura mobilního cloudu (Zdroj: [6])

[2] Systém základnových stanic (anglicky Base Station S(ubs)ystem, BSS) je část sítě GSM, která je zodpovědná za přenos a příjem radiových signálů z mobilního telefonu. Systém základnových stanic provádí překódování hovorových kanálů, přidělování radiových kanálů mobilním telefonům, paging a mnoho dalších úkolů patřících k radiové síti. [61]

Na obrázku 3 je vyznačena hranice mezi mobilním computingem a cloud computingem.



Obrázek 3 - Architektura MCC s vyznačením hranic MC a CC (Zdroj: [8])

3.3 Aspekty mobilního cloud computingu

Hlavním cílem mobilního cloud computingu je vhodným způsobem zpřístupnit data z cloudu koncovým uživatelům s mobilními zařízeními. Při návrhu mobilních aplikací je zároveň nutné myslet na omezení, které mobilní zařízení mají a také omezení bezdrátové komunikace pro přístup do internetu (WIFI, GSM). V následujícím textu je čerpáno ze zdrojů: [8], [9], [10]

3.3.1 Omezení mobilních zařízení

Přestože výkon hardware mobilních zařízení je neustále zlepšován (CPU, paměť, úložiště, senzory, baterie), stále má velká omezení z pohledu výpočetní schopnosti a také zdrojů energie. V porovnání s hardwarem osobních počítačů a notebooků se jedná o řádově 5-10x pomalejší zařízení ve všech zmíněných oblastech.

3.3.2 Kvalita komunikace

U mobilních zařízení se předpokládá, že budou komunikovat skrze bezdrátové sítě, což přináší velký rozdíl oproti klasickému drátovému připojení. Kvalita spojení je dána několika faktory (signál, síťová odezva, rychlost připojení, vytížení základnových stanic, typ dostupné technologie připojení apod.) a je velmi proměnlivá.

3.3.3 Rozdělení aplikačních služeb

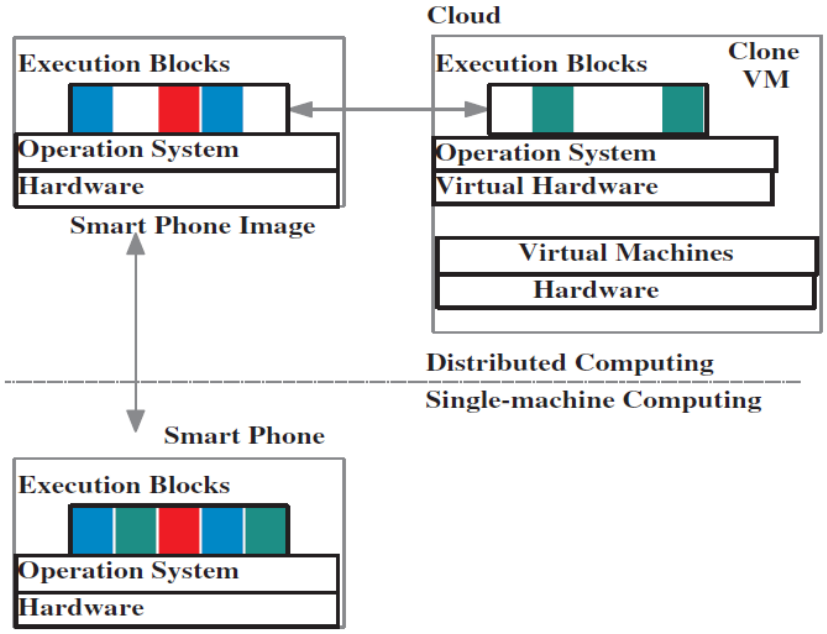
Aplikace náročné na výpočetní výkon, nebo data by neměly být nasazovány do mobilních zařízení. Tyto náročné úkoly by měly být prováděny v cloudu. Mobilní zařízení je tak zodpovědné za vykonání jednoduchých úkolů např. odeslání požadavků či zobrazení výsledků. Jednou z možností posílení výkonu mobilního zařízení je jeho vizualizace v cloudu.

Na eliminaci zmíněných omezení jsou vedeny různé výzkumy průmyslových i vědeckých institucí. Výzkumy se zaměřují na rozdělení úloh do několika podúloh, z nichž některé poběží v cloudu a jiné na mobilním zařízení. Cílem tohoto výzkumu je nalezení optimální strategie nebo algoritmu pro rozdělování úloh.
Směřování výzkumu lze rozdělit do tří hlavních oblastí:

1) Virtualizovaný obraz
2) Klonování mobilního zařízení formou obrazu (VM) v cloudu
3) Weblety

Virtualizovaný obraz (Virtualized Screen) – přesunutí renderování obrazu z mobilního zařízení do cloudu jako služba. Renderování obrazu je tedy prováděno v cloudu a výsledek je doručen do mobilního zařízení formou obrázku. U této metody se počítá s možností, že část úloh může být prováděna v cloudu a část na mobilním zařízení s ohledem na výkon daného zařízení a aktuální konektivitu.

Klonování – jedním z dalších možných směrů je vytvořit klon mobilního zařízení v cloudu. Klonem se rozumí virtuální stroj, který bude mít oproti mobilnímu zařízení výkonnější hardware. Klon rozšiřuje možnosti fyzického zařízení. Ve své podstatě se jedná o zrcadlení snímku mobilního zařízení v cloudu. V cloudu mohou běžet vybrané specifické úlohy. Typickým procesem, kterým je možné spouštět/provozovat v clonu cloudu, je antivir. Výhodou tohoto řešení je provádění náročnějších úkolů mimo zařízení, což výrazně prodlouží běh fyzického zařízení na baterii. Naopak nevýhodou tohoto řešení může být zpoždění plynoucí ze síťové komunikace a rychlosti přenosu dat nutného k zrcadlení. Na obrázku 4 je znázorněna systémová architektura řešení Cloud Clone.



Obrázek 4 - Systémová architektura Cloud Clone (Zdroj: [8])

Weblety – další možností se nabízí rozdělení aplikace do samostatných komponent zvaných Weblety a následně dynamicky nasazovat tyto komponenty na základě konfigurace do cloudu a mobilních zařízení. Nasazením těchto komponent vzniká prodleva mezi komunikací s jednotlivými Weblety. Výzkum v této oblasti se zaměřuje na hledání optimální dynamické konfigurace s cílem minimalizovat prodlevy v komunikaci.

3.4 Základní služby mobilního cloud computingu

Služby mobilního cloud computingu lze rozdělit do tří základních oblastí. První jsou platformové služby, další jsou aplikační služby a poslední služby bohatého obsahu. [9]

3.4.1 Platformové služby

Platformové služby zahrnují výpočetní výkon, úložiště, databáze, cache, fronty zpráv apod. Výpočetním výkonem se rozumí libovolné množství virtuálních strojů, které mohou mít různé parametry dle poskytovatele a zvolené varianty. Služby úložiště poskytují prostor pro dlouhodobé uložení dat. Databázové systémy mohou být nabízeny jako služba, ale lze je instalovat též samostatně do virtuálních strojů. Databázové systémy mohou být relační, in-memory, objektové, nosql, dokumentové apod. Za cache je považována škálovatelná, distribuovaná paměť s rychlým přístupem pro zápis i čtení (Redis, Memcache apod).

3.4.2 Aplikační služby

Mezi aplikační služby lze zařadit zpracování a streamování videí, prezentace, rozpoznání obrazu a řeči, vzdálené notifikace apod.

Zpracováním a streamováním videí se rozumí služby pro zpracování obrazu a konverzi do různých formátů a velikostí. Konverze je výpočetně i kapacitně velmi náročná a proto se hodí pro použití zpracování v cloudu. Velmi užitečnou vlastností je streamování, neboli kontinuální přenos videa a zvuku, aniž by bylo nutné celý záznam nejprve stáhnout do daného zařízení. Existují dva druhy streamovaného vysílání a to přímé přenosy (broadcasting) a videa na vyžádání (video on demand). Při streamování videa dochází k zmenšení velikosti datového toku v závislosti na kvalitě připojení.

Mezi nové služby, na které je v poslední době kladem velký důraz, jsou služby pro rozpoznání a moderování obrazu a řeči. Rozpoznáním obrazu se rozumí specifické operace nad daným obrazem. Může se jednat např. o detekci objektů, osob, gest, nežádoucího/závadného obsahu apod. Služby pro rozpoznání řeči jsou vhodné pro převod mluveného slova na psané. U mobilních zařízení se stávají velkou oblibou hlasové příkazy a rozpoznání řeči je velmi sofistikovanou záležitostí, pro kterou se též hodí zpracování v cloudu.

Velmi oblíbené u mobilních zařízení připojených k internetu se staly push notifikace. Jde o způsob komunikace na internetu, kdy klient (mobilní zařízení) naslouchá a čeká na zprávy, které mu budou zaslány. Iniciátorem komunikace zpráv je tedy server, nikoliv klient. Vzdálené notifikace lze využít k různým účelům a to například k upozornění na nový email, zaslání specifické zprávy do zařízení apod.

3.4.3 Obsahově bohaté podpůrné služby

Obsahově bohaté podpůrné služby (Content-rich support services) jsou podpůrné služby pro vytváření personalizovaných a kontextových aplikací. Mezi tyto služby patří např. služby pro extrahování či doporučení obsahu, služby pro ochranu obsahu apod..

Extrahováním obsahu se rozumí datová analýza mobilních dat společně s daty ze sociálních sítí a senzorů.

Službami pro doporučení obsahu se rozumí analýza dat na základě nějakého kontextu a následné doporučení nějakého obsahu. Příkladem může být, jakou stránku uživatel navštíví, jaké obdobné zboží/video mu lze doporučit apod.

3.5 Možnosti a oblasti využití

Následující text je věnován možnostem a oblastem využití mobilního cloud computingu v praxi. Aplikace rozšířené o možnosti mobilního cloud computingu mohou být např. mobilní komerce, mobilní učení, mobilní zdravotnictví, mobilní hraní her apod. [11]

Mobilní komerce (angl. Mobile commerce) - jde o způsob doručování elektronického obchodování spotřebiteli skrze mobilní zařízení a bezdrátové sítě. Mobilní komerce obsahuje aktivity jako prezentace, platby, obchodování, reklamu atd. Mobilní komerce se musí také vypořádat s mnoha výzvami jako je bezpečnost, nebo rychlost datového spojení apod.

Mobilní učení (angl. Mobile learning) - je založeno na elektronické výuce (e-learning) a navrženo pro použití v mobilních zařízeních. Mobilní učení zahrnuje přístup k výukovým materiálům např. výuka cizích jazyků, přednášky vysokých škol, vědecká přednášky, konference apod. Nemusí se jednat pouze o texty, ale i videa, nahrávky či živá vysílání.

Mobilní zdravotnictví (angl. Mobile Health Care) - účelem aplikování MCC v lékařských aplikacích je nabídnout vhodným, rychlým a bezpečným způsobem zdroje (lékařské záznamy o pacientech). MCC nabízí možnost nemocnicím a zdravotnickým zařízením různé služby namísto provozování vlastních aplikací na lokálních serverech.

Mobilní hraní her (angl. Mobile gaming) - je oblast s velkým potenciálem pro komerční subjekty. Mobilní hraní je možné kompletně zprocesovat (CPU výpočty, renderování grafiky) na serverech v cloudu, kde je výkonnější hardware než v mobilním zařízení. Hráči na mobilních zařízeních pouze interagují s grafickým rozhraním na svém zařízení. Mobilní hraní může výrazně snížit spotřebu energie.

Ostatní využití MCC – existuje mnoho odvětví, kde lze využít potenciál mobilních zařízení v kombinaci s MCC. Může se jednat o aplikace orientovaná na data, mapové podklady, sběr a čtení dat ze senzorů či jiných zařízení, monitoring osob a zboží, doporučení na základě nějakého stavu apod.

4 Internet věcí

Pojem Internet věcí (Internet of Things) je v současné době velmi používaný pojem v oblasti informačních a komunikačních technologií. Není vůbec snadné pochopit, co se pod tímto pojmem či konceptem skrývá.

4.1 Definice

Na úvod je nutné podotknout, že Internet věcí nemá přesnou a jednoznačnou definici stejně jako pojem Cloud computing.

Internet věcí (anglicky Internet of Things, zkratka IoT) je v informatice označení pro propojení vestavěných zařízení s Internetem. Propojení zařízení by mělo být zejména bezdrátové a mělo by přinést nové možnosti vzájemné interakce nejen mezi jednotlivými systémy a též přinést nové možnosti jejich ovládání, sledování a zajištění pokročilých služeb. [12]

Jinou definicí může být například tato:

Internet věcí znamená síť propojených objektů (věcí), které jsou jednoznačně adresovatelné s tím, že tato síť je založena na standardizovaných komunikačních protokolech umožňující výměnu a sdílení dat a informací, jejichž analýzou bude možné docílit vyšší přidané hodnoty. [13] [14]

Slovo síť, nemusí představovat pouze Internet (jak evokuje pojem IoT) – tedy celosvětový systém navzájem propojených počítačových sítí, ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP, ale může znamenat i lokální síť (LAN), v rámci které mohou věci komunikovat, avšak s prostupem do Internetu pro možnost sdílení výsledků. Síť zajišťuje konektivitu. [14]

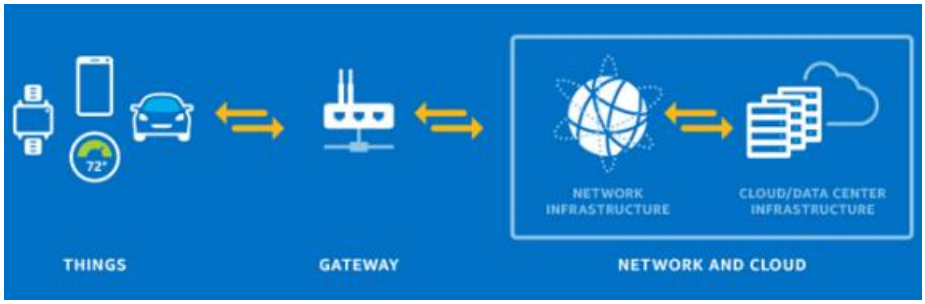
Věc z pohledu IoT představuje neživý objekt (fyzický nebo virtuální) obsahující elektroniku, software a senzory, pomocí kterých snímá určitou veličinu nebo veličiny a poskytuje schopnost sloužit k danému účelu. Jedná se tedy o zařízení (systém), které autonomně poskytuje data (osobní počítač, který neposkytuje data,

nepředstavuje věc z pohledu IoT), která jsou kabelově nebo bezdrátově sdílena s dalšími věcmi nebo systémy. Paradoxem však je, že v rámci Internetu věcí nejsou základem věci, ale data, která tyto věci poskytují. [14]

Internet věcí tedy představuje koncept, v rámci kterého si fyzické a virtuální objekty (věci) vyměňují data přes síť Internet. Věci (systémy) mohou být v rámci Internetu věcí libovolně pospojovány za účelem dosažení vyšších cílů (nových funkčností, složitějších úloh, apod.). [14]

Pojem „Internet věcí" poprvé použil v prezentaci [13] pan Kevin Ashton v roce 1999. V prezentaci autor poukázal na to, že téměř veškerá data na internetu jsou vytvářena lidmi a o co lepší vnímání světa bychom získali použitím propojených senzorů a sdílením dat mezi systémy.
Další důležitý milník z pohledu IoT bylo období mezi roky 2008 a 2009, kdy podle odhadu společnost Cisco překročil počet zařízení (obecně) připojených k internetu počet světové populace a tedy právě mezi roky 2008 a 2009 je datován vznik Internetu věcí. [14]

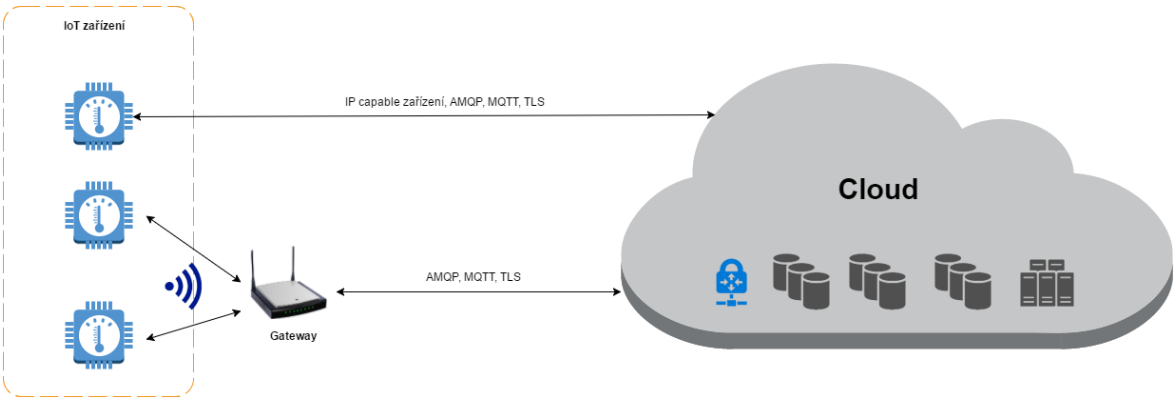
Zároveň je vhodné zmínit, co IoT není, nebo jak by nemělo být vnímáno. Za IoT nelze považovat hardware typu Raspery Pi, Arduirno či jiné vývojové kity, ke kterému se připojí nějaký specifický senzor např. na měření teploty. IoT je o telemetrii, neboli sběru dat a jejich následném zpracování a vyhodnocení mimo daný hardware. IoT zařízení nemusí být přímo připojeno do internetu, ale může být propojeno v rámci lokální sítě. Prostup do internetu pak zpravidla zajišťuje nějaká gateway viz obrázek 5.



Obrázek 5 - Ukázka propojení pomocí Gateway (zdroj: [15])

Gateway – pro zařízení, které nemohou být připojeny přímo do internetu (non ip-capable) je nutné použít Gateway. Tento prvek je prostředníkem mezi IoT zařízením (senzory) a internetem. Gateway je nutné použít i v případech, kdy IoT zařízení neobsahuje hodiny reálného času, nebo není schopné vzhledem k omezenému hardware navázat šifrované spojení, které je vyžadováno při komunikaci s cloudovými službami (málo výkonný procesor, malá operační paměť apod.). Jako Gateway je možné použít v podstatě jakýkoliv hardware splňující výše zmíněné problémy IoT zařízení. Může se tedy jednat o klasický počítač, či o nějakou jeho miniaturní či minimalistickou variantu. V poslední době se řada výrobců snaží vytvářet i specifické Gateway produkty určené přímo na míru k jejich IoT zařízením.

Cloud Gateway – při budování IoT infrastruktury je nutné nejen odesílat data ze senzorů do cloudu, ale také umožnit obousměrnou komunikaci mezi IoT zařízením a cloudem tj. D2C[3] a C2D[4]. Obousměrnou komunikaci je možné využít např. pro notifikaci zařízení (vzor Command / Notification). Zpětný kanál lze využít k posílání různých příkazů danému IoT zařízení. Na obrázku 6 je znázorněna ukázka obousměrné komunikace mezi IoT zařízením a cloudem.



Obrázek 6 - Znázornění komunikace IoT zařízení s Cloudem (Zdroj: vlastní)

[3] D2C – (Device to Cloud) – zařízení posílá zprávy do cloudu (telemetrická data, odpovědi na požadavky)
[4] C2D – (Cloud to Device) – zařízení umožňuje přijít příkazy ke zpracování

4.2 Hardware a vývojové kity

Na úvod této problematiky je vhodné zmínit, že neexistuje žádný standard, jak by mělo IoT zařízení vypadat (velikost, hardware, spotřeba, odolnost atd.). Záleží to tedy na každém výrobci, jaké parametry zvolí. Obecně se lze setkat s kategorií hardware určených pro amatérské či vývojové účely, kde ceny součástek jsou poměrně levné. Pak jsou k dispozici zařízení určená především pro průmysl a obecně odvětví, kde je vyžadována vysoká spolehlivost a běh 24/7. Ceny takovýchto zařízení jsou pak výrazně vyšší.

U IoT zařízení se velmi často očekává, že budou napájeny z baterií, a proto je pro ně velmi podstatná spotřeba. Z tohoto důvodu se ne všechen na trhu dostupný hardware hodí na jakékoliv použití. Obecně lze říci, že zařízení s vysokým odběrem jsou spíše hodná pro účely vývoje a testování. Popřípadě Gateway, která bude sbírat data z jednotlivých mikrokontrolerů se senzory a předávat je dál do internetu.

4.2.1 Arduino

Arduino je otevřená (open source) elektronická platforma, založená na uživatelsky jednoduchém hardware a software. Arduino je v informatice název malého jednodeskového počítače založeného na mikrokontrolerech ATmega od firmy Atmel. Nejedná se o počítač ve smyslu stolního počítače nebo chytrého telefonu. Nelze proto k němu snadno přímo připojit monitor ani klávesnici či myš, ale je připraven na připojení LED diod, displeje z tekutých krystalů, servomotorů, senzorů, osvětlení atd.

Projekt vznikl v roce 2005 v Itálii ve městě Ivrea. Jeho cílem bylo vytvořit jednoduchou prototypovací platformu pro studenty, která umožní rychlý vývoj a jednoduché používání. Projekt zaznamenal velký úspěch a později začaly vznikat jeho další, novější verze. [16]

Arduino je pouze návrhářská deska s mikroprocesorem a není možné na ní provozovat plnohodnotný operační systém typu Linux, Windows apod. Vývojová deska je dostupná v několika modelech. Mezi nejznámější a nejčastěji používané modely patří UNO (Obrázek 7), Nano, Mega apod. Jednotlivé modely se od sebe liší rozměry, počtem pinů, velikostí pamětí FLASH a EEOPROM.

Obrázek 7 - Ukázka Arduino UNO (Zdroj: [17])

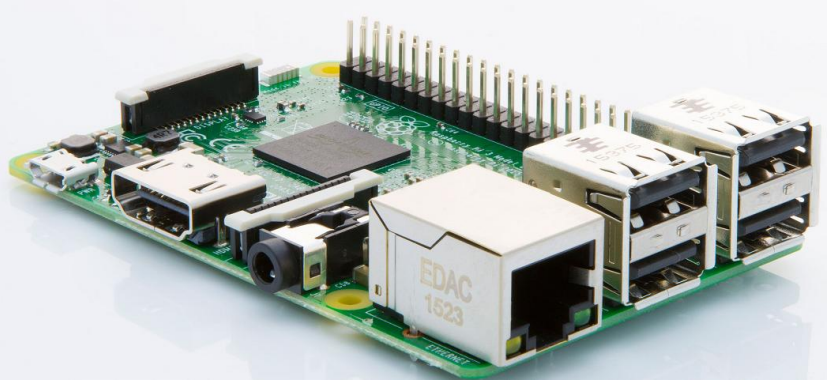
Pro samotný vývoj programu, který poběží na daném zařízení, je možné použít vývojové prostředí Arduino IDE. Toto vývojové prostředí je napsané v jazyce Java a je tedy dostupné pro více platforem. Jedná se o software vzniklý z výukového prostředí Processing., které je upraveno. Na obrázku 8 se nachází ukázka vývojového prostředí. Samotný kód Arduino je možné programovat v jazyce C, C++, nebo je možné používat knihovnu Wiring, která díky své komplexnosti je často označována jako programovací jazyk. Arduino IDE obsahuje podporu „jazyka“ Wiring.

Obrázek 8 - Ukázka vývojového prostředí Arduino IDE (Zdroj: vlastní)

Další možností pokročilejšího vývojového prostředí je Visual Studio s rozšířením Arduino IDE.

4.2.2 Raspberry PI

Raspberry Pi je jednočipový počítač, který je srovnatelný se (slabším) stolním počítačem. Obsahuje vývod pro monitor (HDMI), přes USB je možné připojit klávesnici a myš. Vyvinuto bylo již několik generací tohoto počítače, které se liší výkonem a zamýšleným použitím. Použitý mikroprocesor je z rodiny ARM, takže je srovnatelný s běžným smartphonem. Na počítači Raspberry Pi je možné provozovat jak různé distribuce Linuxu, tak Windows 10 IoT Core od firmy Microsoft [18]. Na obrázku 9 je vyobrazen nejnovější (2016) model Raspberry Pi 3.



Obrázek 9 - Raspberry Pi 3 (Zdroj: [19])

Raspberry PI je dostupné ve dvou základních variantách. Jednak jako standardní model a pak model Zero. Liší se od sebe rozměry, použitým hardware i osazenými porty. Model Zero je navržen pro použití jako mikrokontroler pro robotiku, sondy, offline sběr dat apod.

Vzhledem k hardwarovým parametrům Raspberry Pi je nutné počítat s vyšší spotřebou (viz. Tabulka 1- Srovnání spotřeby modelů Raspberry Pi (Zdroj: [20])) a tudíž toto zařízení není úplně vhodné pro napájení z baterie na delší časové období.

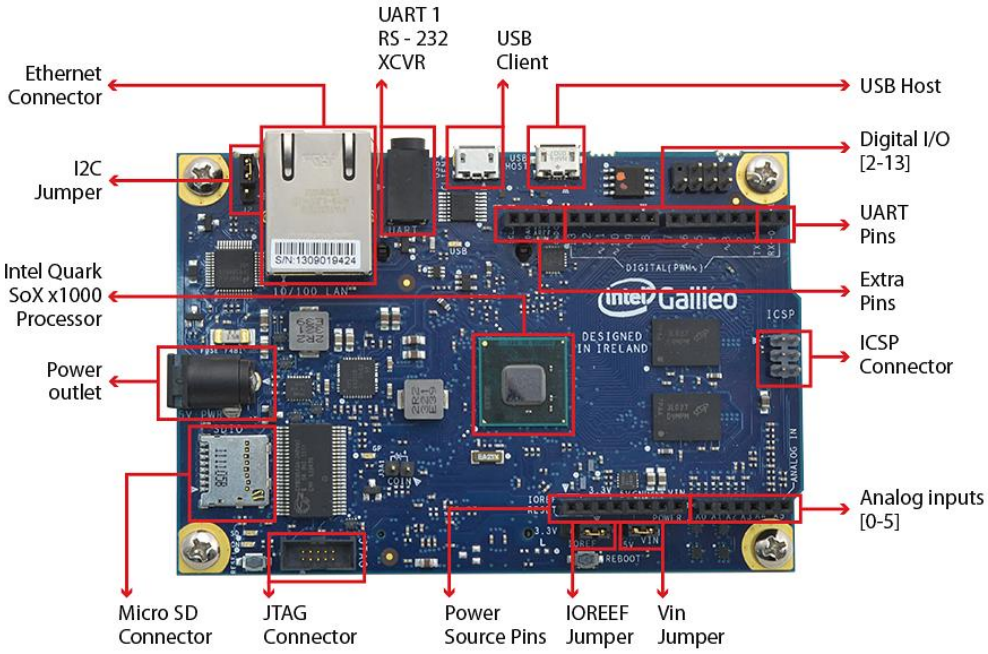
Pi Model	Pi State	Power Consumption
model 3 B	HDMI off, LEDs off	230 mA (1.2W)
model 3 B	HDMI off, LEDs off, onboard WiFi	250 mA (1.2W)
model 2 B	HDMI off, LEDs off	200 mA (1.0W)
model 2 B	HDMI off, LEDs off, USB WiFi	240 mA (1.2W)
Zero	HDMI off, LED off	80 mA (0.4W)
Zero	HDMI off, LED off, USB WiFi	120 mA (0.7W)
B+	HDMI off, LEDs off	180 mA (0.9W)

B+	HDMI off, LEDs off, USB WiFi	220 mA (1.1W)
A+	HDMI off, LEDs off	80 mA (0.4W)
A+	HDMI off, LEDs off, USB WiFi	160 mA (0.8W)

Tabulka 1- Srovnání spotřeby modelů Raspberry Pi (Zdroj: [20])

4.2.3 Intel Galileo

Jedná se o zařízení hardwarově i softwarově kompatibilní s platformou Arduino. Tato deska byla certifikována pro Arduino. Je postavena na x86 architektuře. Lze tak využívat vývojové prostředí, knihovny a shieldy pro Arduino. Vývojová deska běží na operačním systému Linux. Druhá generace této desky nabízí možnost napájení přes Ethernet (PoE – Power over Ethernet). Vyobrazení a rozmístění jednotlivých částí je znázorněno na obrázku 10.



Obrázek 10 - Vývojová deska Intel Galileo (Zdroj: [21])

4.2.4 Ostatní

Na trhu je dostupných spousta zařízení různých výrobců a čínských klonů oficiálních zařízení. Ve své podstatě jde o velmi podobné zařízení k Raspberry Pi. Zpravidla se liší použitým čipem, velikostí pamětí a především cenou. Lze jmenovat např. Intel Edison, Dragonboard, MinnowBoard (opensource projekt společnosti Intel), BeagleBone, Netdruino atd. Rozebírání všech těchto zařízení, by bylo nad rámec této práce.

4.3 Senzory

Senzory jsou nedílnou součástí každého IoT zařízení. Může se jednat jak o velmi jednouché senzory (senzor otevřených dveří), tak o velmi sofistikované, za kterými stojí dlouholetý vývoj a řada patentů např. CO2 senzor. Senzory se tedy u IoT zařízení stávají generátory skutečných dat. Jak již bylo zmíněno, IoT je především o telemetrii a IoT zařízení má primárně za úkol sběr senzorických dat a jejich následné předání dál.

Existuje nespočetné množství senzorů, které není v silách autora zde všechny vyjmenovat a popsat. Následující výčet je tedy omezen na ty nejzákladnější a nejčastěji používané senzory. Kombinací dostupných senzorů na trhu je možné vytvářet technologicky velmi vyspělé projekty.

4.3.1 Senzor teploty

Mezi základní a nejznámější typ senzoru se řadí teplotní senzor. Teplotní senzory existují ve dvou možných provedeních a to analogové nebo digitální. Existuje celá řada typů určených pro různá prostředí. Je nutné si uvědomit, že jiný typ bude použit pro běžně měřitelné hodnoty např. počasí a jiný pro měření v extrémních podmínkách (vysoké mrazy, teploty nad 100 stupňů apod). Od typů použití se také odvíjí jeho cena. Pro neextrémní použití je velmi často v rámci jednoho shieldu dodáván senzor teploty spolu se senzorem vlhkostí a barometrem. Na obrázku 11 se nachází ukázka analogového teplotního senzoru. Velmi důležitým kritériem při výběru konkrétního typu může být též přesnost měření. Jsou velké rozdíly mezi jednotlivými typy. Naměřená teplota se tak může lišit i o několik stupňů což může vyloučit některé typy použití a je nutné hledat senzory s vyšší přesností. Měření se většinou provádí ve stupních Celsia a je možné jej podle vzorce převést na stupně Fahrenheita.

$$F = \frac{9C}{5} + 32, \quad \text{kde C je teplota ve stupních Celsia}$$

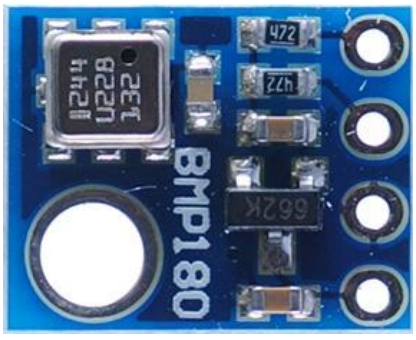
Obrázek 11 – Ukázka analogového teplotního senzoru TMP36 (Zdroj: [62])

4.3.2 Senzor vlhkosti

Senzor vlhkosti je zařízení určené k měření vlhkosti vzduchu. Vlhkost vzduchu udává, jaké množství vody v plynném stavu obsahuje dané množství vzduchu. Podle množství vodních par určujeme tedy vlhkost vzduchu. Vlhkost vzduchu je zpravidla uváděna jako relativní, tedy v procentech. Mezi typické použití tohoto senzoru jsou meteorologické účely.

4.3.3 Barometrický senzor

Barometrický senzor je zařízení určené k měření atmosférického tlaku. Barometrický tlak je definován jako síla působící v daném místě atmosféry kolmo na libovolnou plochu. Měřenou jednotkou jsou pak hektopascal na metr čtverečný. Obrázek 12 obsahuje ukázku senzoru barometrického tlaku.



Obrázek 12 - Senzor barometrického tlaku BMP180 (Zdroj: [22])

4.3.4 Akcelerometr a gyroskop

Akcelerometr je kompaktní zařízení (součástka) určené k měření zrychlení. Je navržen tak, aby při změně z konstantní nebo z nulové rychlosti zaznamenal tuto

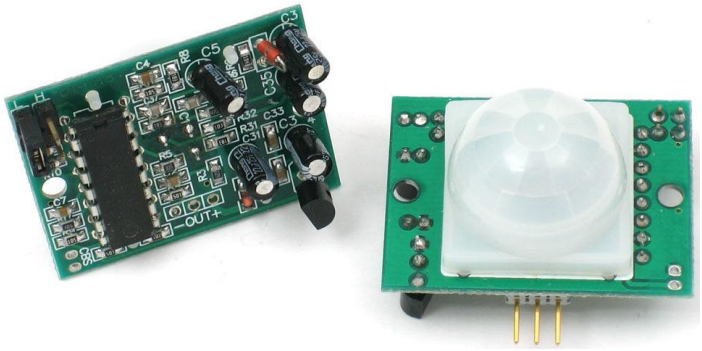
změnu. Při změně dochází k vibracím spojených s tímto pohybem. Akcelerometr využívá mikroskopické krystaly, na kterých se při působení vibrací generuje napětí odpovídající určitému zrychlení. Jedná se o tzv. piezoelektrický jev. Pomocí tohoto jevu lze určit směr gravitace a tedy i natočení přístroje. [23]

K akcelerometru bývá často v mobilních telefonech připojován gyroskopický senzor (gyroskop). Ten slouží podobně jako akcelerometr k tomu, aby určoval naklonění a natočení telefonu. Co však tyto dva druhy odlišuje je fakt, že akcelerometr měří zrychlení, zatímco gyroskop úhlovou rychlost. Je proto výhodné použít jejich kombinaci. Akcelerometr určí směr, kterým se mobilní telefon pohybuje pouze ve dvou osách. Rozpoznání pohybu i ve třetí ose zajišťuje gyroskop. Můžeme tak přesněji určit skutečný pohyb zařízení v prostoru. [23]

4.3.5 Senzor pohybu PIR

Senzor je určen k detekci pohybu. Zkratka PIR je z anglického názvu „passive infrared detector“ - pasivní infračervený detektor. Čidlo funguje na principu pyroelektrického jevu. Na obrázku 13 se nachází ukázka PIR senzoru.

Úkolem optiky PIR detektorů je soustřeďovat infračervené záření vyzařujícího z povrchu objektů, které se nacházejí v detekčních zónách, do PIR elementu. Snímaný prostor je rozdělen na tzv. detekční zóny, jejichž počet je dán počtem segmentů zrcadla nebo čoček, popřípadě geometrií předsazené mřížky. V praxi se používají dva optické systémy - pomocí zrcadel nebo Fresnelovými čočkami [24].



Obrázek 13 - Ukázka PIR senzoru (Zdroj: [25])

4.3.6 Ostatní senzory

Mezi další zajímavé a často využívané senzory vhodné pro vývoj IoT zařízení mohou patřit tyto senzory: senzor intenzity světla, ultrazvukový senzor vzdálenosti, senzor vlhkosti půdy, senzor zaplavení, dešťový senzor, zvukový senzor apod.

4.4 Přenos dat mezi nodem a hubem

V předchozím textu bylo zmíněno, že IoT zařízení se stará o sběr dat ze senzorů. Tato zařízení jsou ve většině případů navrhována s ohledem na spotřebu (low power), aby mohla být napájena delší dobu z akumulátorů. V tuto chvíli nastává problém, jak telemetrická data odeslat do internetu. Většina těchto zařízení není navržena tak, že je přímo připojitelná do internetu. Těch důvodů může být hned několik. Jednak ekonomické, ale také díky použitému hardware. Je nutné si uvědomit, že přenos dat do internetu by měl probíhat v zabezpečeném (šifrovaném) režimu. A tato podmínka se stává pro většinu IoT zařízení překážkou. Dalším faktickým problém může být, že pokud by každé IoT zařízení mělo mít vyhrazenou veřejnou IP adresu, nastal by poměrně velký problém. Adresy IPv4 pomalu docházejí a protokol IPv6 není stále ještě rozšířen. Řešením těchto problémů může být použití gateway, neboli zařízení schopné komunikovat s mikrokontrolery IoT zařízení a následnou možností tyto data posílat do internetu.

Zařízení typu Gateway může být pak jakýkoliv hardware, který se umí připojit k internetu a navázat šifrované spojení. O problematice bezpečnosti přenosu dat bude pojednáváno v jedné z následujících kapitol. Způsobů jakým je možné propojit IoT zařízení s Gateway je více. Mezi nejjednodušší způsoby patří připojení USB kabelem, WIFI, LAN, nebo nějakým jiným typem radiového signálu.

4.4.1 USB

Jde o nejlevnější způsob připojení pomocí usb kabelu. Toto řešení naráží však na několik limitů. Maximální délka usb kabelu je 5 metrů. Znamená to tedy, že IoT zařízení a Gateway musí být blízko sebe. Za hlavní omezení tohoto řešení lze pak považovat množství usb portů, které lze k jedné Gateway připojit. S takovýmto řešením se lze dostat na jednotky maximálně desítky připojených zařízení (nodů). V reálném případě nodů mohou být stovky i tisíce v rámci jednoho řešení. USB je tedy vhodné spíše pro vytváření prototypů či řešení s velmi malým a omezeným počtem nodů.

4.4.2 WIFI

Za velmi ekonomické řešení lze považovat propojení nodů a hubu pomocí WIFI. Toto řešení má však velmi významnou nevýhodu v podobě velkého odběru proudu čili

spotřebu celého zařízení. U prototypů a malých projektů to nemusí být problém, ale u řešení založených na napájení z baterií to představuje zásadní omezení a nelze tento druh komunikace použít.

4.4.3 LAN

Připojení pomocí LAN kabeláže je vhodné pro uzavřené systémy, kde lze tímto způsobem provést propojení. Zařízení je možné připojovat na vzdálenost několika desítek metrů. Při použití aktivních prvků pak i více. Za nespornou výhodu tohoto řešení je možné považovat možnost napájení IoT zařízení z tohoto připojení PoE (Power over Ethernet).

4.4.4 ZigBee

ZigBee je bezdrátová komunikační technologie vystavěná na standardu IEEE 802.15.4. Zigbee je poměrně novým standardem platným od listopadu 2004. Podobně jako Bluetooth je určena pro spojení nízkovýkonových zařízení v sítích PAN (Personal Area Network] na malé vzdálenosti do 75 metrů. Díky použití multiskokového ad-hoc směrování umožňuje komunikaci i na větší vzdálenosti bez přímé radiové viditelnosti jednotlivých zařízení. Primární určení směřuje do aplikací v průmyslu a senzorových sítích. Pracuje v bezlicenčních pásmech (generální povolení) přibližně 868 MHz, 902–928 MHz a 2,4 GHz. Přenosová rychlost činí 20, 40, 250 kbit/s. [26]

4.4.5 Bluetooth

Bluetooth je v informatice proprietární otevřený standard pro bezdrátovou komunikaci propojující dvě a více elektronických zařízení, jako například mobilní telefon, PDA, osobní počítač nebo bezdrátová sluchátka. Vytvořen byl v roce 1994 firmou Ericsson jako bezdrátová náhrada za sériové drátové rozhraní RS-232.

Technologie Bluetooth je definována standardem IEEE 802.15.1. Spadá do kategorie osobních počítačových sítí, tzv. PAN (Personal Area Network). Vyskytuje se v několika verzích, z nichž v současnosti nejvíce využívaná je verze 2.0, která je implementována ve většině aktuálně (2010) prodávaných zařízení, jako jsou např. mobilní telefony, notebooky, televize. V současné době (2011) je nově vyvinuto rozhraní Bluetooth 4.0, u kterého výrobci slibují větší dosah (až 100 metrů), menší spotřebu elektrické energie a také podporu šifrování AES-128. [27]

4.4.6 GSM

Použití GSM sítě pro datové přenosy má svá specifika a úskalí. Výhodou tohoto řešení je velmi solidní pokrytí celého území signálem. Využití této varianty se hodí do míst, kde není možné připojit IoT zařízení či gateway jiným způsobem do internetu. Mezi hlavní a významnou nevýhodu tohoto řešení patří cena. GSM modemy určené pro komunikaci jsou poměrně drahé. K tomu je nutné přičíst další náklady na provoz datového tarifu u nějakého operátora.

4.4.7 Sériový port RS-232, RS-422, RS-485

Sériový port RS-232 byl vyvinut pro komunikaci lokálních zařízení a podporuje jeden vysílač a jeden přijímač. Naproti tomu sériové porty RS-422 a RS-485 se využívají v průmyslovém prostředí a v systémech pro řízení a přenos malého objemu dat. Hlavní rozdíl mezi portem určeným pro komunikaci lokálních a průmyslových zařízení je vzdálenost, na kterou je možné data přenášet. U RS-232 jsou to max. desítky metrů. RS-422 a RS-485 jsou schopny přenášet data až na vzdálenost 1200 metrů. Porty RS-232 a RS-422 jsou určeny pro point-to-point komunikaci. U portu RS-422 mohou být data přenášena v obou dvou směrech současně. U sériového portu RS-485 se používá pro multipoint komunikaci, tzn., že více zařízení může být připojeno k jednomu vedení (obdoba koaxiálního kabelu u sítě ETHERNET). [28]

4.4.8 CAN Bus

CAN (Controller Area Network) je sběrnice, využívaná nejčastěji pro vnitřní komunikační síť senzorů a funkčních jednotek v automobilu, z čehož plyne také použití pro automobilovou diagnostiku. Z této aplikační oblasti se CAN rychle rozšířil také do sféry průmyslové automatizace. Jedná se o sériovou datovou sběrnici, vyvinutou firmou Robert Bosch GmbH. Elektrické parametry fyzického přenosu jsou specifikované normou ISO 11898. Maximální teoretická rychlost přenosu na sběrnici je 1 Mb/s. CAN patří k průmyslovým komunikačním sítím označovaným jako provozní sběrnice, fieldbus. [29]

4.4.9 Rádiový signál

Rádiové vlny (též rádiové záření) je část spektra elektromagnetického záření s vlnovými délkami od 1 milimetru až po tisíce kilometrů. Vzniká mimo jiné v obvodu střídavého proudu, k němuž je připojena anténa. Rychlost šíření rádiových vln je

v prostoru přibližně rovna rychlosti světla ve vakuu. V případě jiných prostředí závisí na indexu lomu. [30]
Pro bezdrátovou komunikaci mezi senzory a gateway se nejčastěji používá frekvence 433, nebo 868 MHz. V USA je pásmo 868 MHz využíváno pro specifické účely, proto se používá pásmo 915 MHz. Dle zvolené frekvence lze dosahovat různých vzdáleností, na kterou je možné komunikovat. Výhodou této komunikace je, že je extrémně nenáročná na spotřebu. Tento typ přenosu se tedy hodí pro řešení založená na napájení z baterie.

Speciálně pro internet věcí se budují nové sítě, využívají frekvenci 868/915 MHz. Jedná se o volné pásmo (Ultra Narrow Band – extrémně úzký frekvenční rozsah), pro které platí povinnost licencování modemů. Mezi nejznámější dvě sítě se řadí Sigfox a LoRA. Cílem těchto sítí je pokrýt celé území (obdoba GSM), tak aby IoT zařízení s modemem mohly komunikovat s nějakou základnou, která předá data do zvolené cloudové služby či úložiště. Princip této komunikace je založen na „datových záblescích“. Jedná se o technologii z druhé světové války. Technologie není vhodná pro použití, kde je vyžadován přenos velkých objemů dat.

Sigfox
Technologie SIGFOX umožňuje IoT zařízením komunikovat levně, bezpečně a na velké vzdálenosti při zcela minimální spotřebě energie. [31]
Modemy komunikují v ultra-narrow band pásmu 868 MHz a se základnovou stanicí se dokážou spojit na přímý dohled v dosahu až 200 km, v členitějším terénu pak 50-60 km a ve městě 2-4 km. Každá zpráva se posílá zhruba dvě sekundy, ale jelikož se vždy odesílá třikrát, aby se zvýšila pravděpodobnost doručení, odeslání může trvat až šest sekund. „Zprávy se posílají na různé BTS a na různých frekvencích, aby se minimalizovala možnost zarušení. [32] Vysílací výkon modemu je 25 mW.
Maximální velikost zprávy je 12 bajtů a za jeden den lze odeslat maximálně 144 zpráv (1 zpráva za 10 minut) vyplývá to z evropské regulace pro bezlicenční pásmo, kdy každé zařízení může vysílat po dobu jednoho procenta z jedné vysílací hodiny.

LoRA

LoRa (Long Range) je modulace patentovaná firmou Semtech, která mj. využívá kódování 4/5, dopřednou korekci chyb a modulaci Chirp. Protokol LoRaWAN zajišťuje transparentní zabezpečený přenos dat mezi koncovým zařízením (internet věcí) a aplikací běžící na serveru a zpět. O standardizaci a rozvoj protokolu LoRaWAN se stará nezisková organizace LoRa Alliance, mezi jejíž členy patří desítky firem. LoRa byla navržena jak pro evropské pásmo 868 MHz, tak pro to americké 915 MHz. Obě pásma mají výhodu a zároveň nevýhodu, že jsou volná a zdarma. Legislativa se pro obě pásma liší, přesto zmíněná technologie dosahuje skvělých výsledků. Citlivost je -136 dB a odolnost vůči rušení -16 dB (pod úrovní šumu), dosah na přímou viditelnost 40 km, v městské zástavbě okolo 2 km. Aby nedošlo k mýlce, hardware a software se pro oba kmitočty liší, nicméně aplikační rozhraní je identické. [33]

Maximální délka zprávy je 255 bajtů. Tuto délku zprávy lze vysílat pro rozsah Spreading Factor 0-7. Pro vyšší hodnoty SF délka zprávy klesá (což souvisí s dobou vysílání jedné zprávy). Zpráva se zkracuje na úkor možnosti přenášet užitečná data – payload. U zprávy standardní délky 255 bajtů je pro užitečná data 240 bajtů. Při nastavení SF 12 je prostor pro užitečná data 51 bajtů, což je ale pro převážnou většinu čidel stále dostatečná kapacita. [34]

LoRA ve srovnání se Sigfox umožňuje přenášet větší objemy dat a má rychlejší obousměrnou komunikaci. Vzdálenost, na kterou je možné komunikovat, je výrazně nižší než u Sigfox.

IQRF

IQRF je platforma pro bezdrátové připojení zařízení určená k budování MESH sítí. Bezdrátový přenos je provozován v bezlicenčním pásmu 433 MHz, 868 MHz nebo 916 MHz. Jedná se o síť s nízkou přenosovou rychlostí, která je navržena na přenos malého objemu dat. Hlavním výhodou této platformy je velmi nízká energetická náročnost při vysílání a příjmu dat. Standardní pokrytí signálem je v řádu desítek až stovek metrů. Tato technologie je vhodná pro budování konceptů pro domácí automatizaci a přenosu senzorických dat.

Stav sítí pro IoT v České republice

V České republice se do budování sítí pro Internet věcí zapojily v tuto chvíli (2016) tři subjekty. První síť Sigfox je budována společnostmi SimpleCell a T-Mobile. Z oficiálních zdrojů plyne, že plánované pokrytí ČR do konce roku 2016 má být 95%. Druhým subjektem na českém trhu je společnost České radiokomunikace, který buduje síť LoRA. Aktuálně (duben 2016) jsou pokryta všechna krajská města a celkové pokryté území ČR je 25%. Posledním subjektem je sdružení Things.cz, které využívá též technologii LoRA. Nestaví však své vlastní vysílače, ale opírá se o lokální poskytovatele internetu. Pokrytí tohoto poskytovatele není zatím známé.

4.5 Oblasti využití

Nabízí se otázka, k čemu to vlastně vše doposud zmíněné je a k čemu by se to dalo využít. Následující text bude věnován možnostem využití výše uvedených technologií v praxi.

Internet věcí je nyní jedna z nejrychleji rostoucích oblastí ve světě IT a telekomunikací. Podle odhadů analytické společnosti IDC bude do roku 2020 zapojeno do internetu věcí až 30 miliard zařízení, dle studie Intelu dokonce až 50 miliard. [35]

Laická veřejnost téměř nemá povědomí o Internetu věcí a jeho využití. Poukazuje na to průzkum, který vznikl ve spolupráci Českých Radiokomunikací (ČRa) a Nielsen Admosphere. Téměř 83 % dotazovaných odpovědělo, že pojem Internet věcí neznají. Obecně lze říci, že Češi očekávají od Internetu věcí zlepšení životní úrovně, především díky tomu, že se v budoucnosti budou i ty nejobyčejnější věci transformovat na tzv. „smart“. [36] Z uvedeného výzkumu nadále vyplývá, že nejvíce zajímavé přijdou Čechům zařízení pro chytré domácnosti a chytré automobily.

4.5.1 Průmysl

V průmyslu se již dlouhá léta pracuje s telemetrickými daty. Co ale nebylo dlouhá léta možné, tak tyto data nějak efektivně využívat ke strojovému učení a předpovídání budoucího stavu. Většinou se jednalo spíše o monitoring, kde pokud hodnota z nějakého senzoru překročila přípustný limit, došlo k aktivaci nějakého události. Se zavedením konceptu IoT přináší této oblasti obrovský potenciál z hlediska analýzy a predikce.

V této souvislosti je často zmiňován pojem Průmysl 4.0[5]. Ve své podstatě se jedná o průmyslovou automatizaci vstupující do nové fáze, kdy digitalizace a robotizace má za úkol zvýšit produktivitu. Inteligentní zařízení by měly převzít činnosti, které doposud vykonávali lidé.

4.5.2 Automobilový průmysl

Automobilový průmysl skýtá též velký potenciál využití internetu věcí. Motivací pro zavedení internetu věcí do tohoto odvětví může být snížení počtu dopravních nehod, zvýšení plynulosti dopravy, autonomní vozidla apod.

Toto odvětví se vyvíjí obrovskou rychlostí. A již dnes jsou automobily vybaveny velkým množstvím senzorů a asistenčních systémů. Většina automobilových koncernů již má v nabídce vozidla umožňující připojení do internetu. Internet ve vozidlech je možné využít nejen pro multimediální využití (navigace, hudba apod.), ale především pro odesílání senzorických dat. Jedním z možných využití těchto dat je predikce poruch či přístup servisního technika k vozidlu na dálku. Nabízí se též využití v případě havárie vozidla a přivolání záchranných složek.

Samostatnou kapitolou jsou pak různé asistenční systémy, které mají za cíl zpříjemnit cestování a také zvýšit bezpečnost přepravy. Může se jednat o rozpoznání únavy řidiče, rozpoznání akutního zdravotního problému, vyhledání vhodného parkovacího místa a zaparkování, hlídání jízdy v protisměru, noční vidění, zmenšení mrtvého úhlu apod.

4.5.3 Chytré domácnosti

Chytré domácnosti patří mezi ty oblasti IoT, které jsou nejvíce vidět. Logicky se na něj zaměřuje i nejvíce výrobců. Ve své podstatě se opět jedná o senzory s využitím pro automatizaci, regulaci a ovládání v domácnosti. Mezi základní vlastnosti chytrých domácností patří automatická regulace teploty (topení, chlazení), řízené větrání, ovládání žaluzií, osvětlení, zabezpečení domácnosti (alarm), multimediální systémy apod. Chytrou domácnost lze též kombinovat s geofencingem. Jedná se o vymezení určité geografické oblasti, u které se mohou na základě vstupu či výstupu z této oblasti aktivovat různé události v domácnosti (regulace topení, osvětlení atd.).

[5] Koncept vychází z dokumentu, který byl představen na veletrhu v Hannoveru v roce 2013. Základní vize tzv. čtvrté průmyslové revoluce se objevily v roce 2011. Podle této myšlenky vzniknou „chytré továrny“, které budou využívat kyberneticko-fyzikální systémy. (Zdroj: [60])

4.5.4 Smart Metering

Smart Metering znamená dálkovou obousměrnou komunikaci mezi měřidlem a datovou centrálou. Umožňuje nejen sběr dat z měření, jejich automatické vyhodnocení, ale např. i řízení sítě, připojení a odpojení měřicího místa, informování zákazníka o aktuální spotřebě apod. [37]

Měřidlo umožňující odečet energií i správu odběrného místa lze považovat za IoT zařízení ve chvíli, kdy je možná komunikace přes internet. Dlouhá léta bránil masovému rozšíření právě přístup měřidel k internetu. Není snadné vybavit odběrná místa internetovou konektivitou. Hlavní příčinou proč tomu tak je, tak jsou náklady a také energetická náročnost potřebná pro komunikaci. Pokud by však komunikace s měřidlem byla založena na radiovém přenosu (Sigfox, LoRA, IQRF), byly by odstraněny zmíněné nedostatky ohledně nákladů na provoz a energetické náročnosti samotné komunikace.

4.5.5 Zdravotnictví

Jedním z nejpřínosnějších využití IoT je pro účely záchrany lidských životů. V této souvislosti je často zmíněn pojem SmartHealth. Jedná se monitoring zdravotního stavu člověka v reálném čase. Prozatím se jedná o chytré náramky, které umožňují měřit krevní tlak, tělesnou teplotu, srdeční tep, rytmus a pravidelnost dechu apod. Je zřejmé, že v této oblasti skýtá obrovský potenciál. Takže měřených fyziologických veličin bude přibývat a budou také vznikat specifické senzory a zařízení pro konkrétní nemoci. A také lze předpokládat, že náramky časem nahradí např. podkožní implantáty.

Na tomto příkladu je vidět reálné využití celého IoT ekosystému tj. od sběru telemetrických dat až po analýzu dat v reálném čase a predikci budoucího stavu (srdeční infarkt, mozková příhoda atd.). V případě zdravotnictví se asi nejvíce otevírá otázka problematiky bezpečnosti a zabezpečení dat před případným zneužitím. Tomuto tématu se bude věnovat následující kapitola.

4.5.6 Zemědělství

V zemědělství je možné internet věcí využít např. pro sledování zvířat (lokace či zdravotní stav). Dále pak pro zavlažovací systémy, monitoring zemědělských strojů apod.

4.5.7 Ostatní

Je velmi mnoho oblastí, kde lze využít internet věcí např. energetika, chytrá města, doprava, logistika zboží, nositelná elektronika apod.

4.6 Identifikace a adresace objektů

Již dnes je zřejmé, že cesta k jednotné sadě standardů pro oblast Internetu věcí bude velmi komplikovaná a to především s ohledem na řadu různých zájmových skupin z oblasti průmyslu nebo standardizačních organizací, které zastupují některé průmyslové sektory. Především v oblasti identifikace zatím není zřejmé, jaká platforma bude v budoucnosti dominantní pro zajištění unikátnosti identifikátorů jednotlivých objektů a zařízení v rámci Internetu věcí. V otázkách adresace objektů a zařízení je však velká naděje směřována k protokolu IPv6, který disponuje dostačující kapacitou pro připojení o několik řádů vyššího počtu komunikujících zařízení. [38]

Protokol	**Adresní prostor**	**Teoretický počet adres**
IPv4	2^{32}	cca 4 miliardy
IPv6	2^{128}	cca $3{,}4\times10^{38}$

Tabulka 2 - Srovnání adres IPv4 a IPv6

5 Zpracování velkého objemu dat

Tato kapitola se zabývá problematikou příjmu a následného zpracování dat z IoT zařízení. Příchozí data z IoT zařízení je možné zpracovávat v reálném čase (hot path), nebo v budoucnu (cold path). U budoucího zpracování se očekává, že data jsou uložena do nějakého úložiště. Tato data mohou být posléze zdrojem pro strojové učení či předpovědní analýzy, o kterých bude dále pojednáváno v této práci.

5.1 Úvod do problému

V závislosti na konkrétním projektu může jedno IoT zařízení generovat určitý počet zpráv. Zmíněným počtem zpráv může být např. 1 zpráva za vteřinu např. údaj o teplotě. Pro jedno či několik takovýchto IoT zařízení nebude problém postavit infrastrukturu (aplikační backend) na relační databázi. Pokud ale takovýchto zařízení bude třeba sto tisíc, tak dříve či později se stane úzkým hrdlem aplikační infrastruktura, která má za úkol přijmout a nějakým způsobem zpracovat přijatá data z IoT zařízení. Nejslabším místem se stane pravděpodobně relační databáze.

Autor této práce se měl možnost podílet na vývoji řešení pro jednu americkou korporátní společnost, kde se jednalo o řešení kde chytré termostaty (IoT zařízení), každých pět minut reportovaly svůj stav (Gateway Live Status). Termostat posílal informaci o tom, že je aktivní a jaké má nastaveny hodnoty. Těch termostatů bylo více jak jeden milion. Vyvíjené řešení bylo testováno na budoucí předpokládaný počet čtyři miliony zařízení. Při tomto počtu se lze snadno dostat k tomu, že za jeden den musí infrastruktura přijmout přes jednu miliardu zpráv. Přestože zpráva není nijak velikostně (datově) obsáhlá, tak se jedná o velké množství, které naráží i na limity klasických relačních databází.

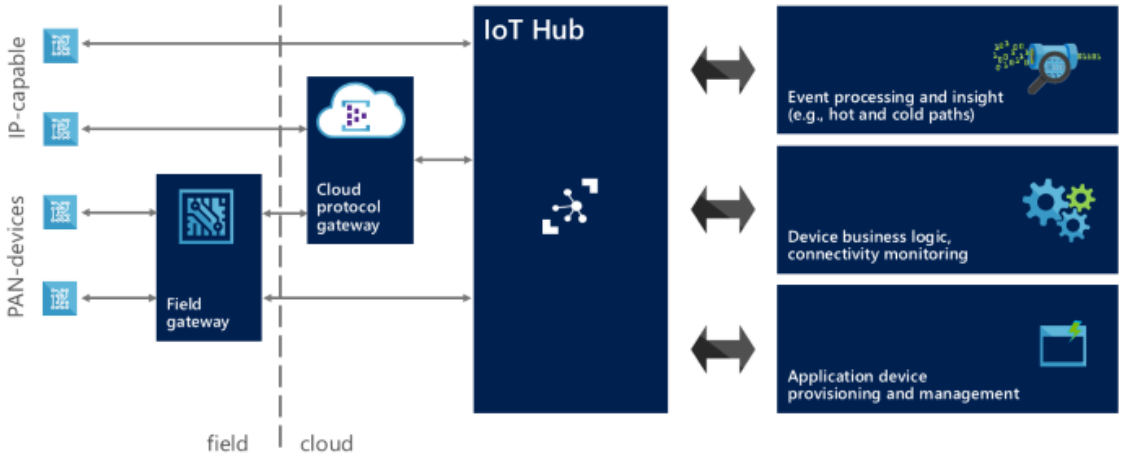
5.2 Dostupné cloudové služby pro IoT

V této části bude pojednáváno o možnosti využití cloudové infrastruktury pro ukládání telemetrických dat z IoT zařízení. Pro menší projekty je možné uvažovat i vlastní infrastruktuře pro poskytování služeb. Avšak tato práce je primárně o mobilním cloud computingu a proto se bude autor zabývat cloudovými řešeními nejvýznamnějších hráčů na trhu a to jsou společnosti Microsoft, Amazon a Google.

5.2.1 Azure IoT Hub

Azure IoT Hub je cloudová, škálovatelná služba umožňující zabezpečené připojení IoT zařízení. Služba umí přijímat zprávy ze zařízení a také je do zařízení odesílat. V rámci IoT hubu je možné provádět kompletní management spravovaného IoT zařízení. (přiřazení bezpečnostních klíčů, zařazení do skupin, blokace zařízení při jeho kompromitaci apod.). Pro komunikaci se zařízením se používá komunikační protokol HTTPS REST, AMQP 1.0 nebo MQTT přes zabezpečenou komunikaci TLS a každý požadavek musí obsahovat SAS (Shared Access Signature – URL požadavek s časovou platností). O komunikačních protokolech bude pojednáváno dále v této práci.

Velikost jedné zprávy je omezena na 4 KB. Na obrázku 14 je znázorněna ukázka komunikačních vrstev v IoT hubu.

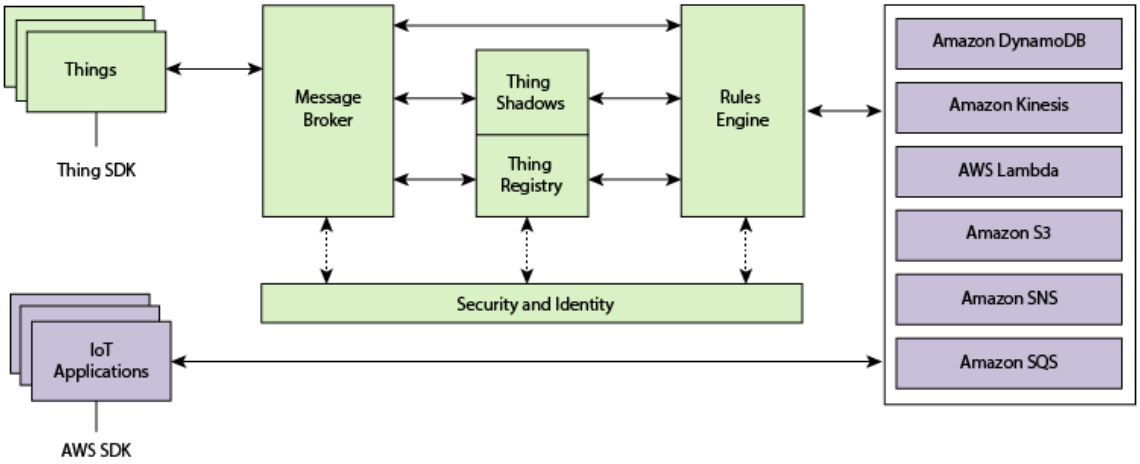


Obrázek 14 - Ukázka komunikačních vrstev IoT hubu (Zdroj: [39])

5.2.2 Amazon AWS IoT

AWS IoT je cloudová infrastruktura, skládající se z několika služeb zaměřených na podporu IoT zařízení, sběru a zpracování telemetrických dat. Zasílání zpráv probíhá ve formátu JSON přes komunikační protokol MQTT.

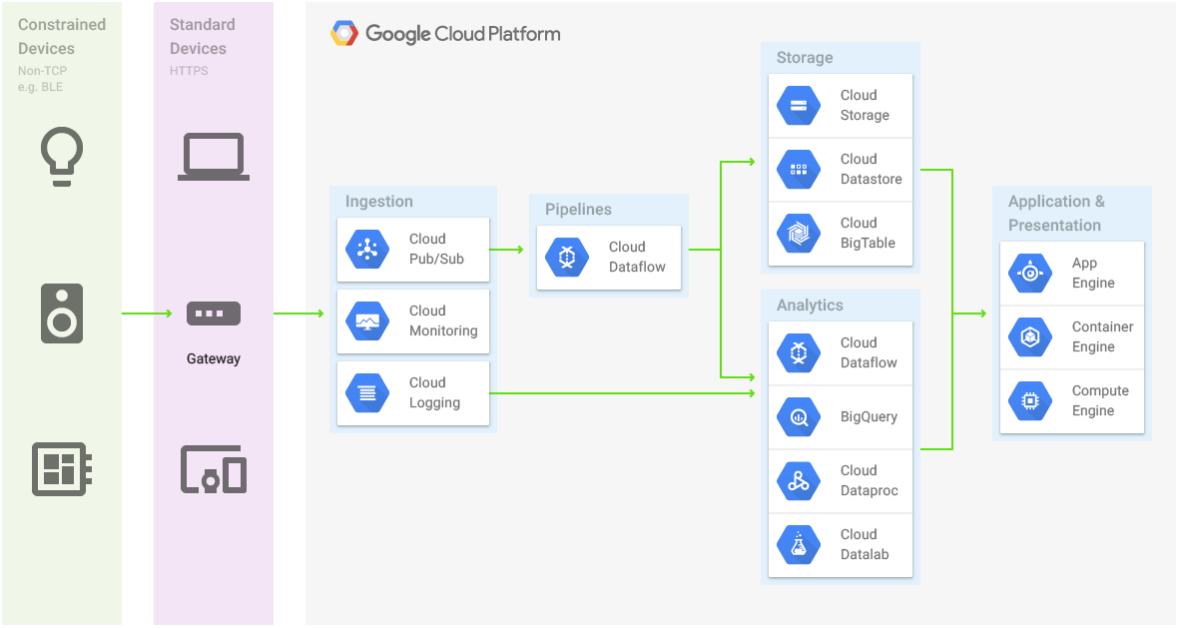
Na obrázku 15 je znázorněna základní architektura služby Amazon AWS IoT. Z obrázku je patrné schéma komunikace mezi jednotlivými komponentami a také možné využití služeb pro ukládání, analýzu dat apod.



Obrázek 15 - Ukázka Amazon AWS IoT infrastruktury (Zdroj: [40])

5.2.3 Google Cloud Platform

Jedná se o sadu cloudových, škálovatelných služeb pro uložení, zpracování a analýzu dat. Na obrázku 16 se nachází základní přehled platformy Google Cloud pro IoT.



Obrázek 16 - Google Cloud Platform (Zdroj: [41])

5.3 Komunikační protokoly pro přenos dat

5.3.1 HTTP

HTTP (Hypertext Transfer Protocol) je internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML. Používá obvykle port TCP/80, verze 1.1 protokolu je definována v RFC 2616. [42]

Rozšířenou možností je použití zabezpečeného protokolu HTTPS. U obou těchto protokolů se často používá REST komunikace. Použití této varianty je vhodné na malé projekty. Není však vhodné pro případy, kdy se odesílají data velmi často např. 4x za vteřinu. Dalším omezením je v tomto případě také použití zpětného kanálu, kdy je potřeba dát zařízení nějakou zprávu. V tomto scénáři je nutné, aby se samo zařízení dotazovalo, zda pro něj není k dispozici nějaká zpráva.

5.3.2 AMQP

AMQP (Advanced Message Queuing Protocol) je standardizovaný protokol pro přenos zpráv. Zprávy (data) jsou přenášena v binární podobě. Protokol obsahuje mechanismy pro bezpečný a spolehlivý přenos zpráv mezi dvěma stranami. Velký důraz je kladen na otevřenost a multiplatformnost (interoperabilita). Obsahuje podporu pro zabezpečenou komunikaci (SASL a TLS). Jedná se o nejrozšířenější komunikační protokol.

5.3.3 MQTT

MQTT (Message Queuing Telemetry Transport) je jednoduchý centralizovaný protokol sloužící zpravidla pro použití s nejrůznějšími senzory. Lze jej však využít i pro přenos mnoha jiných, zejména telemetrických dat. Protokol byl vyvíjen společností IBM v devadesátých letech minulého století. Od té doby se využívá pro sběr a distribuci dat v malých i velkých infrastrukturách. Základem je systém typu zveřejnit/odebírat (publish/subscribe). Zařízení s funkcí zveřejnit odesílají zprávy zprostředkovateli (broker), který na základě přihlášených odběrů provede třídění a přeposlání správným uživatelům. Předávání je pouze jednosměrné (potvrzované), lze však využít QoS. Tento protokol byl vyvíjen pro použití v ekosystému M2M, nicméně dnes je stejně vhodné jej použít i pro IoT a WoT. Od počátku byl protokol koncipován pro sítě TCP/IP. V současnosti, díky rozvoji nových technologií, je možné nalézt např. implementaci MQTT-SN (MQTT for Sensor Networks), kterou je možné

využít i v jiných typech sítí a přenosových soustavách. Důležitým předpokladem je přenos dat v blocích, nelze tedy použít datový proud (streamování). [43]
Protokol MQTT je optimalizován na omezenou kapacitu přenosových linek a používá se především v průmyslovém prostředí.

5.4 Big data

Pojem Big data není přesně vymezen a lze se setkat s různými výklady, co tento termín znamená. Poradenská zveřejnila vlastní definici tohoto pojmu:
Big data je termín aplikovaný na soubory dat, jejichž velikost je mimo schopnosti zachycovat, spravovat a zpracovávat data běžně používanými softwarovými nástroji v rozumném čase. [44]

Pojem „velikost" dat je chápán nejen z hlediska objemu dat měřeného giga-, tera- či petabyty, ale i z hlediska rychlosti jejich tvorby a přenosu a z hlediska různorodosti jejich typů. [44]

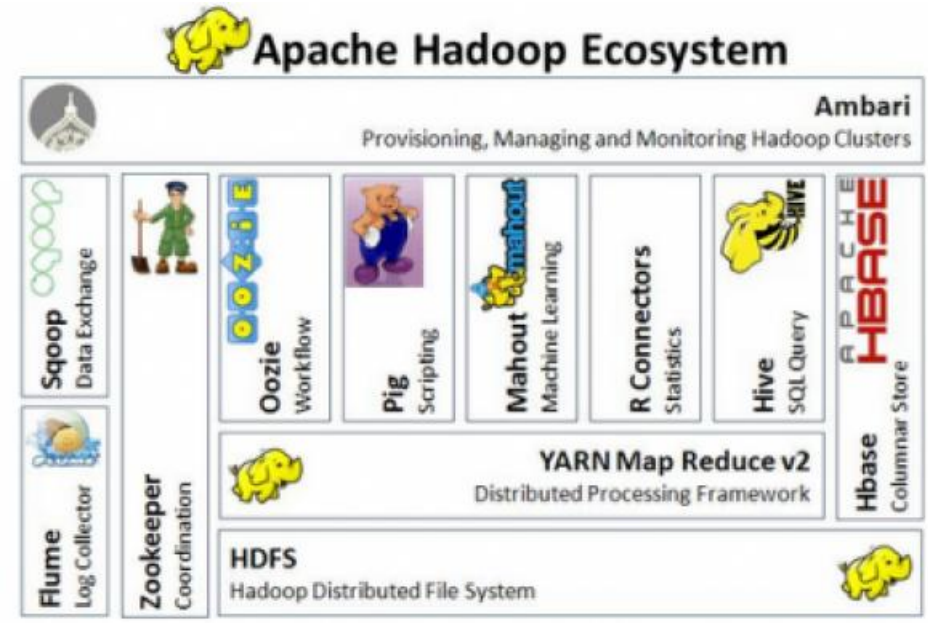
Nástup webu, mobilních zařízení a dalších technologií zapříčinil zásadní změnu charakteru dat a způsobu jejich využití. Již nejsou centralizovaná, vysoce strukturovaná a snadno zvládnutelná, ale více než dříve jsou volně strukturovaná (pokud mají vůbec nějakou strukturu), vysoce distribuovaná a mají vzrůstající objem. Často se v této souvislosti hovoří o trojrozměrnosti velikosti a růstu dat (zkráceně také jako 3V): [44]
Objem (volume) – množství dat vznikajících v rámci provozu firem roste exponenciálně každý rok.
Typ (variety) – různorodost typů dat vzrůstá, například nestrukturované textové soubory, semi-strukturovaná data (XML), data o geografické poloze, data z logů.
Rychlost (velocity) – rychlost s jakou data vznikají a potřeba jejich analýzy v reálném čase vzrůstá díky pokračující digitalizaci většiny transakcí, mobilním zařízením a vzrůstajícímu počtu internetových uživatelů.
Big data mají odlišné vlastnosti, které je odlišují od „tradičních" firemních dat. Tradiční datové sklady a nástroje pro správu dat nejsou připraveny na zpracování a analýzy velkých objemů dat ve velmi krátkém čase (někdy real-time) nebo

nákladově efektivním způsobem. Proto je třeba hledat nové způsoby zpracování a analýzy velkých objemů dat. [44]

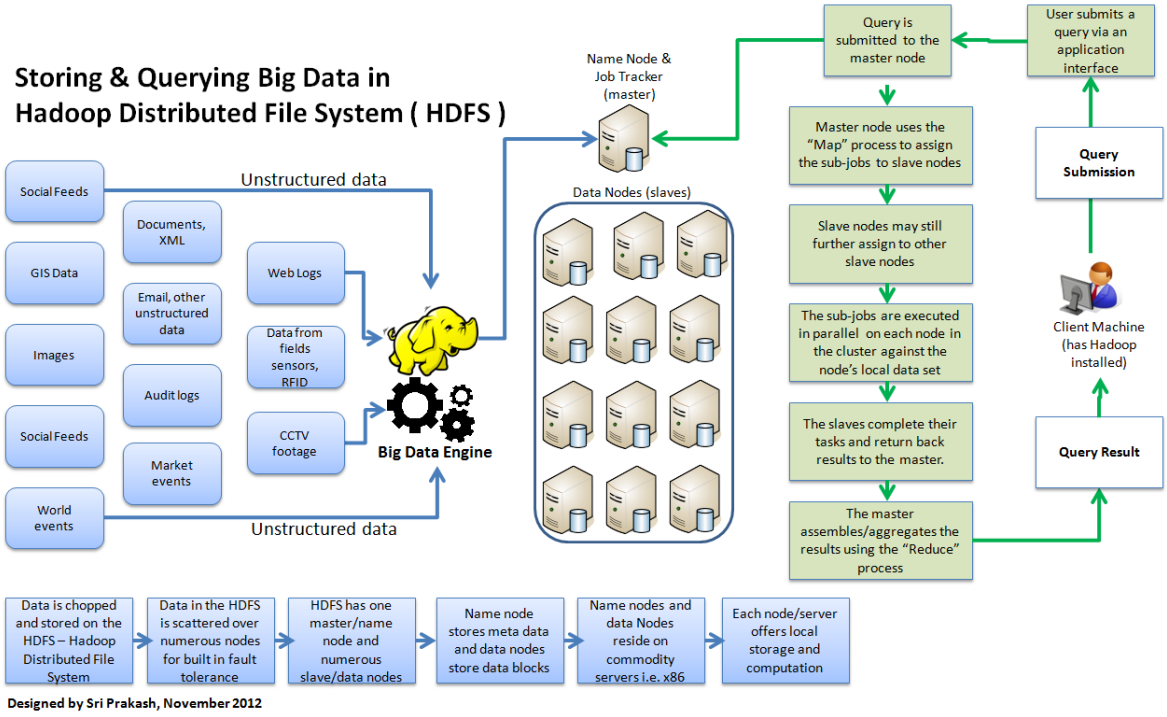
Je nutné si uvědomit o jaké velikosti dat je vlastně pojednáváno v rámci pojmu Big data. Jedná se o vyšší terabajty až petabajty dat. Hlavním z dnešních požadavků je umět pracovat s těmito daty v reálném čase. Tato představa je zcela odlišná od klasických datových skladů u relačních databází. U klasických datových skladů dochází nejčastěji k odlévání dat k určitému datu (konkrétní den, měsíc, kvartál, rok) a nad tímto „snímkem" dat jsou prováděny požadované analýzy včetně OLAP kostek.

Jedním z možných řešení pro Big data je použití nástroje Hadoop. Hadoop je open source framework pro ukládání a následné zpracování distribuovaných a nestrukturovaných dat. Ekosystém nástroje Apache Hadoop je znázorněn na obrázku 17. Existuje mnoho nadstaveb a rozšíření pro Hadoop, za kterými stojí velké společnosti jako IBM, Microsoft, Google apod.

Hadoop je stavěn pro zvládání petabytů a exabytů dat distribuovaných přes více uzlů současně. MapReduce je výpočetní vrstva v rámci Hadoopu. Úlohy MapReduce přistupují k datům, která jsou distribuována na webu nebo v datových centrech, rozdělují je do více replikovaných dílů a jejich zpracování pošlou na jednotlivé uzly. Dotazy a další zpracování pak probíhá v každém uzlu paralelně. Výsledky jsou agregovány a ukládány do úložné vrstvy, jako například Hadoop Distributed File System (HDFS). Odtud jsou data načtena do jednoho z několika analytických prostředí pro analýzu. Ekosystém Hadoop se dále skládá z dalších vzájemně se doplňujících projektů. Mezi ně, kromě výše uvedených HDFS a MapReduce, patří NoSQL datová úložiště, jako Cassandra nebo HBase. [44]
Na obrázku 18 se nachází názorná ukázka ukládání a dotazování do distribuovaného úložiště HDFS.



Obrázek 17 - Ekosystém Apache Hadoop (Zdroj: [45])



Obrázek 18 - Ukázka ukládání a dotazování v HDFS (Zdroj: [46])

5.5 Zpracování streamů v reálném čase

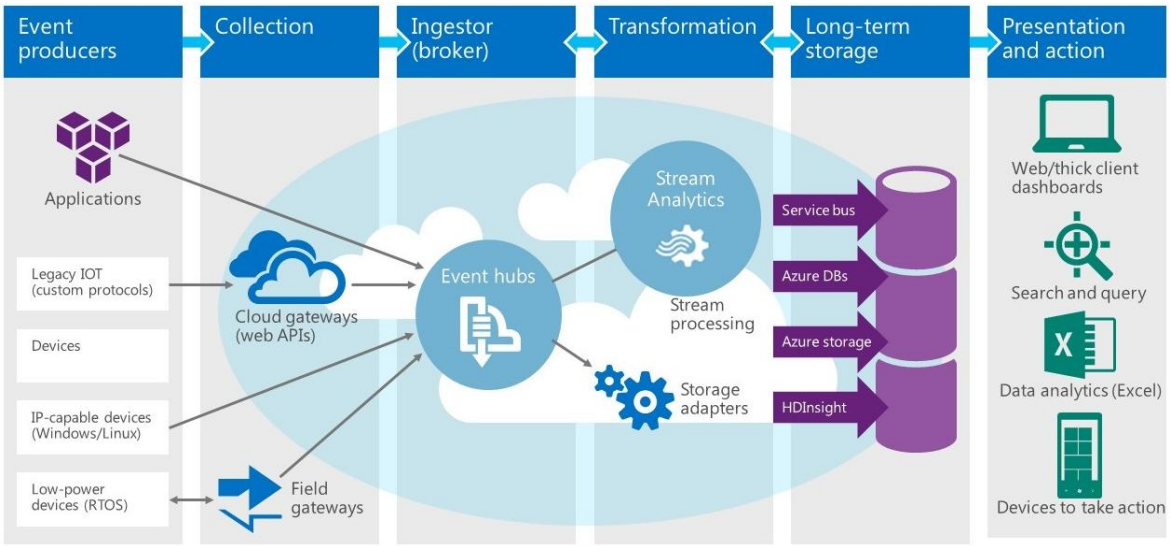
V předcházejícím textu bylo popsáno, jak je možné ukládat a zpracovávat distribuovaná, nestrukturovaná data. Nabízí se ale otázka, zda je možné s příchozími daty něco provést v reálném čase (v okamžiku jejich příjmu). Jako jednoduchý příklad

lze uvést sběr telemetrických dat, kdy nám IoT zařízení budou posílat naměřenou teplotu. V takovém to případě nemusí být každá naměřená hodnota zajímavá, nebo naopak hodnota může dosahovat nějakého extrému a je nutné na ni neprodleně reagovat. Nevýznamné hodnoty je možné zahazovat popř. vkládat do jiné fronty či úložiště.

Pro analýzu streamu v reálném čase existuje celá řada řešení. Jedná se o velmi specifickou záležitost a záleží tedy na konkrétní použité platformě zvoleného dodavatele řešení.

5.5.1 Microsoft Azure Stream Analytics

Služba Stream Analytics umožňuje zpracovávat data v reálném čase. Umožňuje tedy jejich filtrování a agregaci v reálném čase. Na vstupu mohou tedy být data z IoT zařízení, popř. již předpřipravená fronta či jiné datové úložiště. Výstupů může být několik souběžně (permanentní úložiště, jiné služby určené pro další zpracování či vizualizaci). Obrázek 19 obsahuje ukázku možného zpracování zpráv službou Stream Analytics.

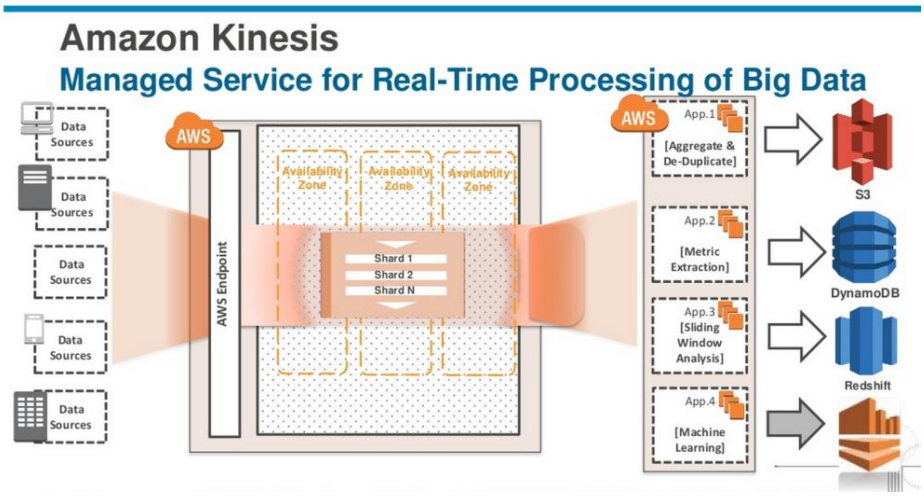


Obrázek 19 - Ukázka toku zpracování zpráv ve Stream Analytics (Zdroj: [47])

5.5.2 Amazon Kinesis

Amazon Kinesis je platforma, která umožňuje zpracování streamů dat v reálném čase. Na vstupu je stream dat a na výstupu mohou být jakékoliv služby Amazonu pro uložení či další zpracování dat. V rámci této platformy je pak možné použít Kinesis

Analytics, který nabízí možnost zpracování streamovaných dat standardním SQL jazykem. Přehled platformy je zachycen na obrázku 20.



Obrázek 20 - Platforma Amazon Kinesis (Zdroj: [48])

5.5.3 Google Analytics

Google Analytics je označení pro sadu komponent pro podporu zpracování streamů v reálném čase. Jedná se o komponenty Cloud Dataflow, Cloud Datalab, CloudDataproc a BigQuery.

Cloud Dataflow umožňuje sjednotit data z více zdrojů a může plně nahradit Apache Hadoop. Pro správu datových toků se používá komponenta Cloud Pub/Sub. Pro analýzy rozsáhlých souborů nestrukturovaných dat je určena komponenta BigQuery. Google Cloud Datalab umožňuje interaktivním způsobem procházení a vizualizaci dat.

5.6 Prediktivní údržba a strojové učení

Tím hlavním důvodem, proč je dobré shromažďovat telemetrická data je provádění analýz a možných předpovědí budoucího stavu. Možností, jak toho dosáhnout je více. Velmi populární se stalo provádět tyto predikce za pomocí strojového učení. Do tohoto odvětví je v poslední době investováno velké množství finančních prostředků mnoha společností včetně velkých IT korporací.

Prediktivní údržba (angl. Predictive maitenance) je analýza historických a současných dat a prediktivních modelů za účelem předpovědi nějakého jevu. Může se tedy např. jednat o předpověď, kdy dojde k poruše stroje na výrobní lince, nebo kdy může dojít k přetížení elektrické rozvodné sítě apod. Hlavním důvodem, proč tyto analýzy provádět je minimalizace vzniku těchto událostí, které mohou mít velmi negativní

finanční dopady. Cílem tedy je včasné zjištění problémů předtím, než nastanou. Mezi základní funkce prediktivní analýzy patří identifikace příčiny, prevence vzniku, úspora nákladů, prodloužení životnosti zařízení apod. Analýza dat může být založena na řadě sofistikovaných metod, jako jsou analýza časových řad, lineární regrese, neuronové sítě, bayesiánské sítě apod.

Strojové učení (angl. Machine learning) je podoblastí umělé inteligence, zabývající se algoritmy a technikami, které umožňují počítačovému systému 'učit se'. Učením v daném kontextu rozumíme takovou změnu vnitřního stavu systému, která zefektivní schopnost přizpůsobení se změnám okolního prostředí. [49]

Algoritmy strojového učení lze podle způsobu učení rozdělit do následujících kategorií: [49]

- **učení s učitelem** (angl. supervised learning) Pro vstupní data je určen správný výstup (třída pro klasifikaci nebo hodnota pro regresi)
- **učení bez učitele** (en:unsupervised learning) Ke vstupním datům není známý výstup
- **kombinace učení s učitelem a bez učitele** (angl. semi-supervised learning) Část vstupních dat je se známým výstupem, ale další data, typicky větší, jsou bez něj. Často se používá EM algoritmus (angl. Expectation–maximization algorithm). Podobný přístup je transdukce
- **zpětnovazebné učení** (angl. reinforcement learning), též učení posilováním

Podle způsobu zpracování lze algoritmy rozdělit na: [49]

- **dávkové** - všechny data požadují před začátkem výpočtu.
- **inkrementální**: dokážou se "přiučit", tj. upravit model, pokud dostanou nová data, bez přepočítání celého modelu od začátku

Mezi základní typy úloh patří: [49]

- **Klasifikace** rozděluje vstupní data do dvou nebo několika tříd
- **Regrese** odhaduje číselnou hodnotu výstupu podle vstupu
- **Shlukování** zařazuje objekty do skupin s podobnými vlastnostmi, typicky při učení bez učitele

6 Problematika bezpečnosti

Nedílnou součástí každého řešení by mělo být řešení otázky problematiky zabezpečení dat proti jejich zneužití, manipulaci či jiné destrukci systému. V této kapitole bude pojednáváno o možnostech zabezpečení a také o hrozbách, které mohou nastat.

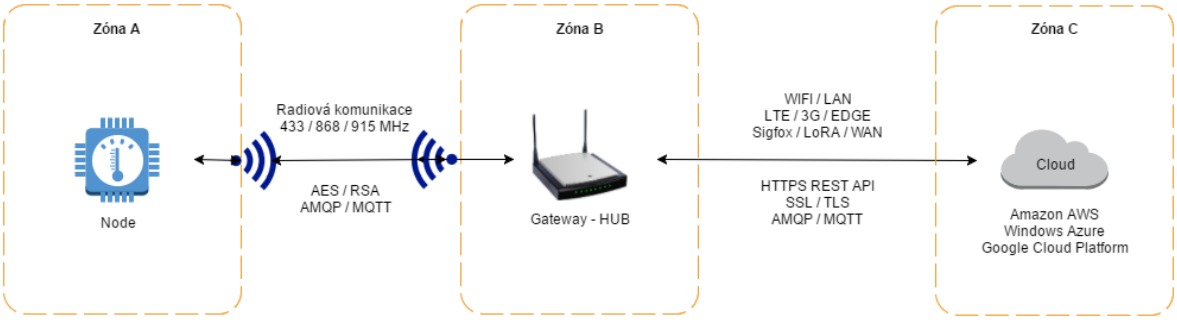
6.1 Úvod do problému

V rámci přenosu a zpracování dat se pracuje se širokým spektrem informací. Některé informace mohou být technického rázu (teplota, vlhkost, výška hladiny, …), jiné zase osobní (GPS pozice apod.). Bez ohledu na povahu dat, by se mělo k těmto datům přistupovat stejně. Zabezpečením se tedy rozumí, že cizí osoba nemá možnost tyto data číst, vkládat, modifikovat a ani je mazat.

Návrh systému musí také počítat s tím, že může dojít ke kompromitaci jednoho či více zařízení. Kompromitací se rozumí fakt, že daného zařízení se zmocní útočník a snaží se prostřednictvím tohoto zařízení provádět útoky na infrastrukturu systému či data.

6.2 Zabezpečení přenosu dat

Přenos dat je možné dle návrhu řešení rozdělit do dvou až tří samostatných zón viz Obrázek 21. Dvě zóny lze použít u řešení, kdy IoT zařízení (node) má vlastní IP adresu a je tedy přímo schopné odesílat zprávy do internetu. Avšak tento scénář není příliš častý. Častějším scénářem je použití tří zón, kdy IoT zařízení je vybavené pouze radiovým zařízením schopným komunikovat s nějakým koncentrátorem (Gateway). V takovémto případě je možné hovořit o třech zónách. První zónu (A) tvoří samotné IoT zařízení se senzory (node). Druhá zóna (B) obsahuje Gateway, která zprostředkovává komunikaci mezi nody a cloudem (zóna C).



Obrázek 21 - Zóny zabezpečení (Zdroj: vlastní)

Na obrázku 21 je znázorněna komunikace mezi zónami A a B radiovým přenosem. Nejedná se samozřejmě o jediný možný způsob. Výčet možných způsobů propojení byl uveden na straně 25 této práce. Jedná se o ilustrativní, ale zároveň nejpoužívanější scénář zapojení. Pro zabezpečení komunikace mezi těmito dvěma zónami je nutné, aby node uměl šifrovanou komunikaci. Z předešlého textu vyplývá, že node zpravidla není schopen výpočetně či paměťově šifrovat. Řešením je vybavit node dodatečným hardware, který se bude starat o šifrování, tzn. neprovádět šifrování softwarově, ale hardwarově.

Komunikace mezi zónami B a C probíhá vždy zabezpečeně. Použití veřejných cloudových služeb přináší tu výhodu, že tyto služby se snaží o maximální míru zabezpečení a drží se doporučených pravidel a postupů. Zpravidla tyto veřejné cloudové služby nedovolují přenášet data nezabezpečeným způsobem. Pokud by v zóně C nebyl Cloud, ale nějaký vlastní datový sklad, měla by pro tuto komunikaci platit stejná pravidla, jak pro komunikaci s veřejným cloudem.

6.2.1 Generátor náhodných dat

Hardwarový generátor náhodných čísel (TRNG, anglicky True Random Number Generator) je v informatice zařízení, které je připojeno k počítači (nebo je obsaženo přímo v procesoru) a které generuje náhodná čísla z fyzikálního procesu. Taková zařízení jsou často založena na mikroskopických jevech, které generují nízkoúrovňové, statisticky náhodné "šumové" signály, například z tepelného šumu či fotoelektrického jevu nebo jiných kvantových jevů. Tyto procesy jsou, teoreticky, zcela nepředvídatelné a teoretická potvrzení nepředvídatelnosti jsou předmětem zkušebního testu. Kvantově založený hardwarový generátor náhodných čísel se typicky skládá z převodníku převádějící některé aspekty fyzikálních jevů na elektrický signál, zesilovač a dalších elektronických obvodů, aby byl výstup snímače přenesen do makroskopické oblasti a nějaký A/D převodník pro konverzi

analogového výstupu do digitální formy (řada binárních čísel 0 a 1). Tím, že opakujeme vzorky náhodně různého signálu, se získá řada náhodných čísel.
Hardwarové generátory náhodných čísel se liší od generátorů pseudonáhodných čísel, které se běžné používají ve většině počítačů. Tyto pseudogenerátory náhodných čísel používají deterministický algoritmus pro výrobu číselné posloupnosti. Proto nejsou vhodné pro kryptografické aplikace, jsou totiž náchylné k dešifrovacímu útoku. Takže bezpečnostních aplikacích, jako jsou produkce náhodných klíčů pro vojenské a obchodní šifrovací systémy, se používají generátory hardwarově náhodné. [50]

6.2.2 Symetrické šifrování

Symetrické šifrování znamená použití stejného klíče (sdíleného tajemství) pro šifrování i dešifrování zprávy. Výhodou symetrického šifrování je nízká výpočetní náročnost. Obecně platí, že čím větší délka klíče sdíleného tajemství je použita, tím obtížnější je prolomení této ochrany. Problematickou částí je však generování klíčů a jejich výměna. Pro generovaný klíč platí zásada, že by měl být náhodný tj. vygenerovaný TRNG, čili opravdové náhodě, nikoliv nějaké sekvenci, která se může opakovat. Při pravidelné obměně klíčů (např. jedenkrát za den) nemusí být použití symetrického šifrování nějakou zásadní bezpečnostní slabinou.
Symetrické šifrování se dělí na dva základní druhy a to proudové a blokové. Proudové šifry zpracovávají text po jednotlivých bitech. Blokové šifry pracují na principu rozdělení textu na jednotlivé bloky. Velikost bloku je dána použitým šifrovacím algoritmem např. 64 či 128 bitů. Existuje celá řada algoritmů pro symetrické šifrování. Mezi nejznámější a v současné době nejpoužívanější patří Triple DES a AES.

Triple DES - (označovaná jako TDES či 3DES) je bloková šifra založená na šifrování Data Encryption Standard (DES), které aplikuje třikrát, čímž zvyšuje odolnost proti prolomení. Původní DES má délku klíče 56 bitů, což se postupem času stalo nedostatečným a klasický DES tak byl ohrožen útoky hrubou silou. Triple DES byl nejjednodušším způsobem, jak odolnost DESu zvýšit díky většímu klíči bez nutnosti přejít na zcela nový algoritmus. Oproti zcela nově navrženým algoritmům (např. AES) je ale TDES mnohem pomalejší, a proto se od jeho používání pomalu ustupuje. [51]

AES (Advanced Ecryption Standard), v překladu pokročilý šifrovací standard, nahrazuje DES, který byl jeho předchůdcem od roku 1977. Novou šifru schválil 26. 11. 2001 americký Národní úřad pro standardizaci (NIST) v publikaci FIPS PUB 197 jako federální standard USA s účinností od 26. 5. 2002. AES je bloková šifra s blokem o délce 128 bitů. Do značné míry vychází z principů užitých v DES, což je jedním z pilířů nastupujícího standardu. Je to z toho důvodu, že algoritmus DES jako takový nebyl dodnes nabourán. S-boxy, které byly stěžejní částí DES algoritmu, se stávají důležitou součástí standardu AES. Druhým pilířem je délka klíče, která může nabývat hodnot 128, 192 nebo 256 bitů. [52]

6.2.3 Asymetrické šifrování

Asymetrické šifrování je metoda, při které se pro šifrování a dešifrování používají odlišné klíče.

Šifrovací klíč pro asymetrickou kryptografii sestává z dvou částí: jedna část se používá pro šifrování zpráv (a příjemce zprávy ani tuto část nemusí znát), druhá pro dešifrování (a odesílatel šifrovaných zpráv ji zpravidla nezná). Je vidět, že ten, kdo šifruje, nemusí s dešifrujícím příjemcem zprávy sdílet žádné tajemství, čímž eliminují potřebu výměny klíčů; tato vlastnost je základní výhodou asymetrické kryptografie. Nejběžnější verzí asymetrické kryptografie je využívání tzv. veřejného a soukromého klíče: šifrovací klíč je veřejný, majitel klíče ho volně uveřejní, a kdokoli jím může šifrovat jemu určené zprávy; dešifrovací klíč je privátní (tj. soukromý), majitel jej drží v tajnosti a pomocí něj může tyto zprávy dešifrovat (existují i další metody asymetrické kryptografie, ve kterých je třeba i šifrovací klíč udržovat v tajnosti). Je zřejmé, že šifrovací klíč a dešifrovací klíč spolu musí být matematicky svázány, avšak nezbytnou podmínkou pro užitečnost šifry je praktická nemožnost ze znalosti šifrovacího klíče spočítat dešifrovací. [53].

Mezi nejznámější asymetrické šifrovací metody patří RSA, Diffie-Hellman a DSA. Z nichž nejrozšířenější se stal algoritmus RSA, který je při použití větší délky klíče (2048 bitů) považován za bezpečný.

6.2.4 SSL a TLS

Pro šifrovanou komunikaci přes HTTPS se používá protokol SSL (Secure Sockets Layer), nebo novější TLS (Transport Layer Security). HTTPS umožňuje zabezpečit spojení mezi klientem a serverem proti odposlouchávání a podvržení dat.

Protokol HTTPS využívá asymetrické šifrování. Obě strany si před zahájením komunikace vygenerují pár klíčů (privátní a veřejný). Při zahájení komunikace si vymění veřejné klíče, které by obě strany měly ověřit pomocí jiného komunikačního kanálu. Ověření může proběhnout kontrolou výtahu (otisk, miniatura, hash) veřejného klíče u protistrany například pomocí telefonu nebo lze použít princip přenosu důvěry, kdy nám protistrana předá veřejný klíč, který je digitálně podepsaný. [54]

TLS zahrnuje tři základní fáze: [55]

1. dohodu účastníků na podporovaných algoritmech
2. výměnu klíčů založenou na šifrování s veřejným klíčem a autentizaci vycházející z certifikátů
3. šifrování provozu symetrickou šifrou

Během první fáze se klient a server dohodnou na používaných kryptografických algoritmech. Současné implementace podporují následující možnosti: [55]

- pro kryptografii s veřejným klíčem: RSA, Diffie-Hellman, DSA
- pro symetrické šifrování: RC2, RC4, IDEA, DES, Triple DES, AES, Camellia
- pro jednosměrné hešování: Message-Digest algorithm (MD2, MD4, MD5), Secure Hash Algorithm (SHA-1, SHA-2)

6.3 Ochrana před zneužitím

Ochrana před zneužitím koncového zařízení (IoT, mobilní zařízení apod.) je velmi složitá záležitost. Obecně platí, že pokud se útočník zmocní koncového zařízení, tak získává obrovskou výhodu. Při návrhu zabezpečení projektu je vhodné pamatovat jak na fyzickou bezpečnost (uzamčené prostory apod.), tak především bezpečnost proti destrukci a manipulaci s daným zařízením.

Zařízení lze rozdělit do dvou základních skupin. Ty co mají operační systém (ořezaná verze Linuxu, Windows, Android apod.) a jednoduché platformy bez operačního systému (např. Arduino). Pro obě tyto skupiny platí pravidlo, že by měli obsahovat vždy nejnovější firmware a aktualizace systému.

Platformy s OS

Na takovýchto zařízení běží plnohodnotný operační systém typu Linux, Windows apod. Výhodou použití této platformy je, že aplikace lze vytvářet v libovolném programovacím jazyce. Tyto zařízení mají zpravidla výkonnější hardware než platformy bez OS. Je využita Von Neumannovská architektura tzn., že se používá stejná paměť pro data i instrukce. Sdílená paměť znamená větší riziko pro případný útok na zařízení. Naopak výhodou těchto operačních systémů jsou standardní kryptografické knihovny. Je tedy možné standardními způsoby používat asymetrickou kryptografii pro zabezpečenou komunikaci apod. U plnohodnotných OS bývá součástí infrastruktura pro aktualizace systému a firmware. Nevýhodou plnohodnotných operačních systémů je naopak zvýšená hrozba útoků na samotný systém či jeho komponenty (attack surface). Pokud se tedy objeví bezpečnostní hrozba v jádře či komponentě operačního systému jedná se o velký problém. Mimoto použití plnohodnotného operačního systému přináší ještě jednu hrozbu v podobě, že pokud se útočník zmocní takového zařízení, je velmi pravděpodobné, že dokáže provádět z takového zařízení útoky na infrastrukturu. Je nutné si uvědomit, že se jedná o počítač připojený do místní sítě.

Jednoduché platformy bez OS

Jednoduché platformy bez operačního systému jako jsou např. Arduino používají Harwardskou architekturu. Znamená to tedy, že mají oddělenou paměť pro kód a data. Výhodou použití takové platformy je menší riziko napadení nějaké komponenty OS a nelze toto zařízení použít jako základ pro další útoky. Získá-li útočník kontrolu nad zařízením, nebude schopen z takového zařízení provádět útoky na infrastrukturu. Pravděpodobně bude moct dané zařízení ovládat a modifikovat odesílaná data. Velmi problematická je aktualizace firmware na takovýchto zařízení. Většinou je nutné si naprogramovat vlastní mechanismus pro vzdálené aktualizace firmware. Takové řešení musí být rezistentní proti modifikaci a podvržení jiného firmware apod. Proces aktualizace firmware by měl být plně automatizovaný, bez zásahu uživatele. Zásadní nevýhodou jednoduchých platforem je velmi omezený hardware, který nelze použít pro asymetrickou kryptografii. Zařízení buď není schopno upočítat dané úkoly, nebo jej nedokáže uložit do operační paměti (např.

velikost kryptografického klíče vs. velikost paměti). Z tohoto důvodu je většinou nutné použít dodatečný speciální hardware, který zvládne asymetrické šifrování.

Typickými problémy IoT zařízení jsou tedy firmware a jeho bezpečná aktualizace, generátor náhodných dat tj. zdroj entropie (TRNG), omezené kryptografické schopnosti a odolnost proti lokálním fyzickým útokům. [56]
Velmi důležitou vlastností při návrhu řešení by mělo být možnost odpojení jednoho konkrétního zařízení, které bylo napadeno. Infrastruktura by tedy měla být navržena formou nějakých klíčů pro každé zařízení nikoliv jednoho klíče pro všechna zařízení. Při kompromitaci jednoho zařízení dojde k jeho zakázání, tzn., že zprávy a příkazy od něj budou zahazovány.
Pro řešení založená na vysoké míře zabezpečení je vhodné dále zvážit samotné fyzické zabezpečení koncového zařízení proti manipulaci s ním. Může se jednat např. o sebedestrukční mechanismus, nebo spuštění alarmu při otevření zařízení apod. Dále je vhodné zvážit použití speciálních typů čipů a pamětí, které neumožňují nakopírování nové verze firmware či vyčtení paměti zařízení.

6.4 Vybrané právní aspekty

Pro výše zmíněné pojmy Cloud computing, Mobilní cloud computing a Internet věcí vyvstává otázka, jak je to s právní legislativou. V úvodu je nutné říci, že neexistuje žádná globální legislativa platná pro celý svět. Problematika bezpečnosti a ochrany dat je velmi citlivou záležitostí. Bohužel se zatím nepodařilo najít celosvětové či evropské řešení. V této souvislosti by se jako vhodné řešení jevilo zastřešení nějakou nadnárodní organizací jako WTO (světová obchodní organizace) či OECD (Organizace pro ekonomickou spolupráci a rozvoj). V současné době však platí, že kde jsou data fyzicky uložena (datový sklad v konkrétní zemi), tam je nutné splňovat legislativu dané země.

Mezi základní právní aspekty patří: [57]

- **Podmínky užívání služeb** (smlouva o užívání, smluvní povinnosti, kvalita služeb apod.)
- **Rozhodné právo** (sídlo poskytovatele a uživatele – jaký právní řád)

- **Ochrana dat, zabezpečení a odpovědnost** (povinnost zajištění dostatečných bezpečnostních opatření)

Rizikem při používání cloudových služeb je, že k datům mohou přistupovat subjekty třetích stran. Zpravidla se může jednat o úřady či jiné bezpečnostní složky dané země, kde se datové centrum a data nachází. Při využívání cloudových služeb nemusí být vždy patrné místo zpracování údajů, a na to se váže problém s určováním rozhodného práva, u sporů se zpracováním údajů.
Na úrovni Evropské unie byla zřízena pracovní skupina pro ochranu údajů podle článku 29, která přijala dne 1. července 2012 „Stanovisko č. 05/2012 ke cloud computingu“ i pracovní skupina pro Internet věcí, která vydala stanovisko „Pracovní dokument útvarů Komise o internetu věcí“.

Legislativa v České republice

Český právní řád nemá žádné vyhrazené zákony pro Cloud Computing či Internet věcí. Vztahují se tak na ně standardní soukromoprávní normy. Základním právním vymezením je tedy Zákon č. 101 o ochraně osobních údajů a o změně některých zákonů ze 4. dubna 2000. V případě Cloud computingu je tedy nutné počítat s tím, že každá země přistupuje jinak k ochraně dat a klade odlišné požadavky na práci s nimi a bezpečnost. Dle stanoviska pracovní skupiny pro ochranu údajů ke cloud computingu je zákazník vybírající si cloudovou službu odpovědný za dodržování právních předpisů.
V souvislosti s použitím bezlicenčních rádiových pásem pro přenos zpráv u IoT zařízení je vhodné dále zmínit zákon č. 127/2005 Sb. O elektronických komunikacích a o změně některých souvisejících zákonů. Činnosti spojené s přidělováním licence a dohlížení na dodržování podmínek má v České republice na starost Český telekomunikační úřad, který vydal opatření obecné povahy „všeobecné oprávnění č. VO-R/10/05.2014-3 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu“.

7 Smart metering s využitím MCC

V této kapitole bude pojednáváno o návrhu konceptu, na kterém bude ukázána možnost využití mobilního cloud computingu a Internetu věcí. Bude se jednat o Smart metering s využitím mobilního cloud computingu.

7.1 Úvod do problematiky

Již několik let je snaha energetických společností po celém světě zautomatizovat odečty měřidel energií a zároveň získat přehled v reálném čase o tom, jaký je aktuální odběr/spotřeba jednoho připojeného odběrného místa. Koncept, který má danou problematiku vyřešit se nazývá Smart metering. Smart metering jako takový je ale primárně určen pro dodavatele energií. Nabízí se otázka, zda by nebylo možné data využít i jinak, než jen k fakturaci. Koncept, který bude v této práci dále rozvíjen, se zabývá možností využití telemetrických dat z měřidel energií s jinými telemetrickými daty z mobilních zařízení. Telemetrická data budou zpracována v cloudu a primárním účelem navrženého konceptu bude využití těchto dat k jiným účelům, než je samotná fakturace.

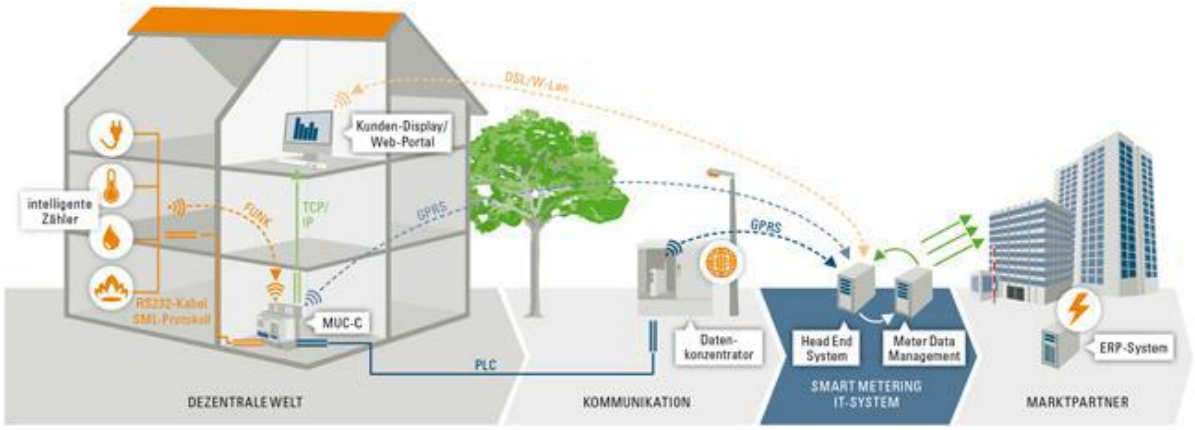
7.2 Smart metering

Smart metering je koncepce pro dálkovou, obousměrnou komunikaci mezi měřidlem a centrálou. V souvislosti s rozvojem dálkové komunikace s měřidlem a jeho inteligencí se používá řada pojmů a zkratek.

AMR (Automated Meter Reading) – automatické odečty (jednosměrná komunikace, efektivní zajištění odečtů).
AMM (Automatic Meter Management) – obousměrná komunikace. V postatě je to AMR s dalšími funkčnostmi, např. řízení tarifu, připojení a odpojení odběrného místa.
Smart metering – chytré měření, AMM + IT podpora pro řízení a vyhodnocování dat.
Smart grid – základem je chytré měření doplněné o čidla v síti pro on-line řízení soustavy a decentralizované výroby.

Komunikaci mezi koncentrátory (měřidly) a datovou centrálou je zajišťována datovými přenosy. Jedná se o datové přenosy jak naměřených dat, tak o povely řídící koncentrátory a měřidla (dálkové připojení/odpojení, mimořádné odečty, informace o stavu měřidla/koncentrátoru). Zde se pro přenos nejčastěji využívá GPRS (General Packet Radio Service – mobilní datové spojení). [58]

Na obrázku 22 je znázorněna ukázka možného zapojení a komunikace konceptu Smart meteringu.



Obrázek 22 - Ukázka Smart meteringu (Zdroj: [59])

Většina konceptů pro přenos dat mezi odběrným místem a centrálou využívá mobilních dat (GPRS). Hlavní nevýhodou tohoto řešení je cena GSM zařízení a jeho provoz, které jsou k těmto účelům nutné. Dalším poměrně komplikovaným faktorem je energetická náročnost GSM modemů, o které již bylo v této práci pojednáváno. Jde o to, že i u měřidel je nutné počítat s možností, že budou napájeny z akumulátorů, kde bude kladen důraz na to, aby vydržely pracovat i několik let bez nutnosti jejich výměny.

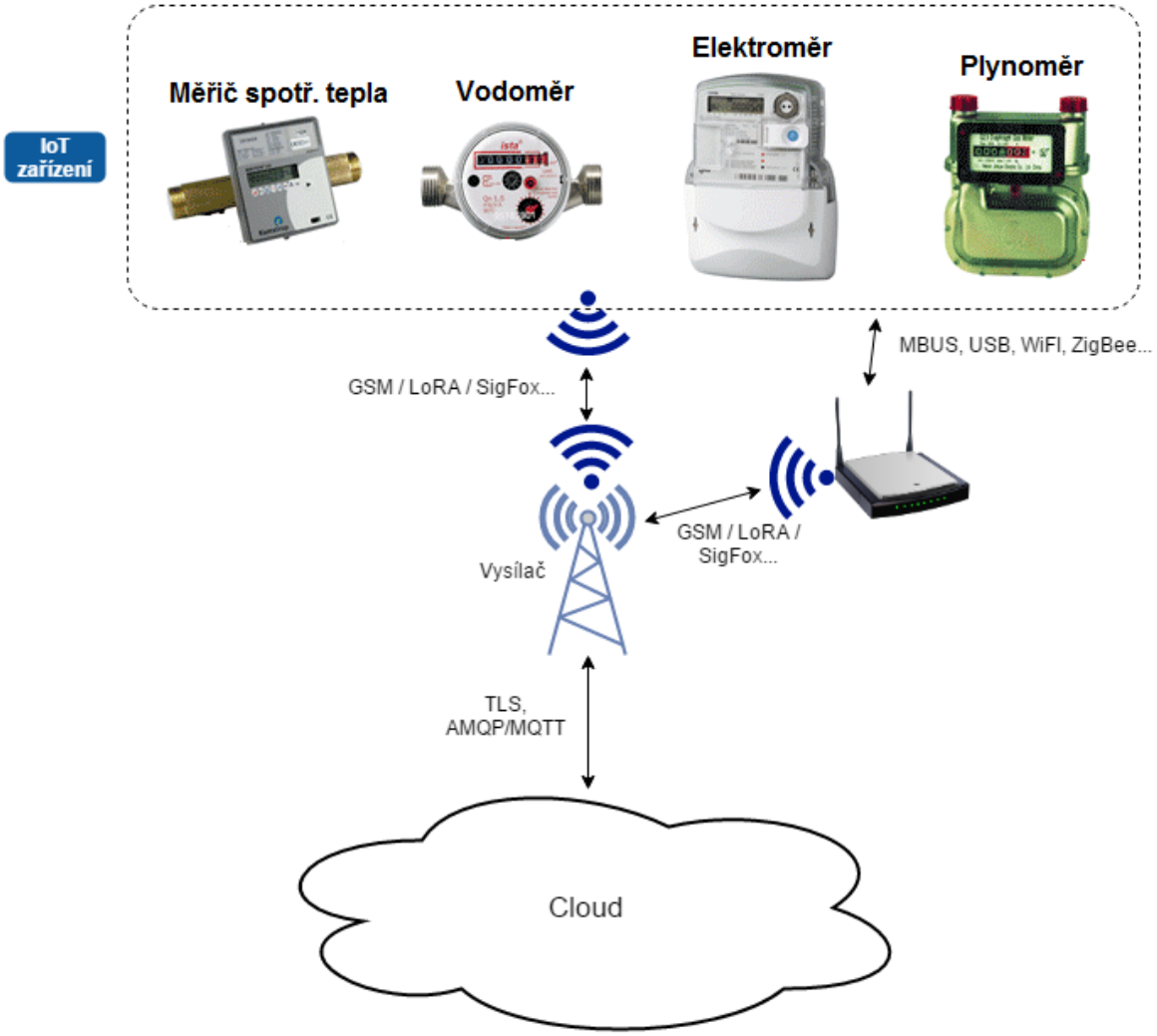
Měřidlo energií jako IoT zařízení

Nabízí se otázka, proč nevnímat chytré měřidlo energií jako IoT zařízení a abstrahovat tak způsob připojení, kterým je připojeno do internetu, zda přímo či nepřímo (Gateway).

Způsobů jak připojit chytré měřidlo k internetu je více a jsou popsány v kapitole 4.4 této práce.

Na obrázku 23 je znázorněn koncept měřidel jako IoT zařízení. Měřidlo (plynoměr, elektroměr, vodoměr, měřič spotřeby tepla) komunikuje buď přímo (IP capable),

nebo nepřímo přes Gateway do internetu. Za vhodnou technologii pro přenos dat lze považovat bezdrátové sítě LoRA, Sigfox, IQRF především kvůli nízké spotřebě a také pořizovacím nákladům. Touto volbou by se odstranila překážka týkající se energetické náročnosti i ceny GSM řešení.



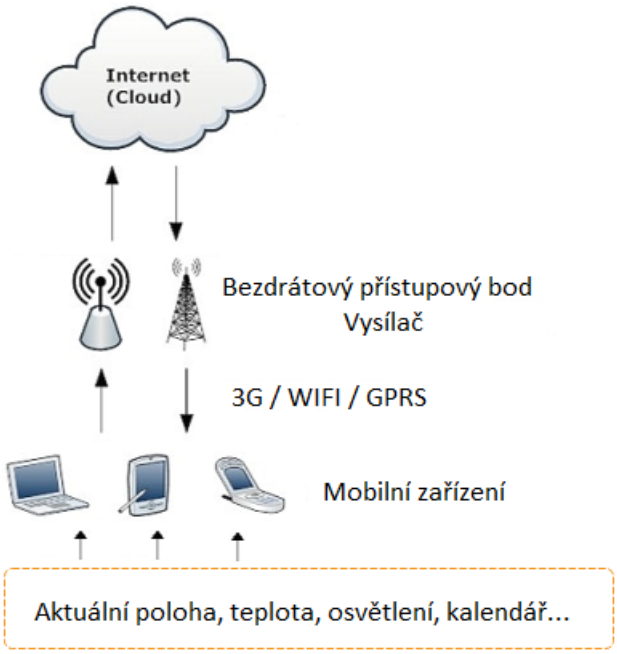
Obrázek 23 - Koncept měřidel jako IoT zařízení (Zdroj: vlastní)

Základní vlastností tohoto zařízení je odesílání údajů tedy telemetrických dat, jako jsou aktuální odběr, údaj o celkové spotřebě, stav zařízení apod. Mimoto je možná obousměrná komunikace se zařízením. Lze jej tedy na dálku ovládat a případně také aktualizovat jeho firmware. Vzdálená správa měřidla je vhodná pro aktivaci a deaktivaci odběrného místa bez nutnosti fyzické návštěvy odběrného místa.

7.3 Data ze senzorů mobilních zařízení

Mobilní zařízení se může stát velmi cenným a užitečným zdrojem informací pro další zpracování. Tato zařízení jsou dnes vybavena množstvím senzorů, které je možné

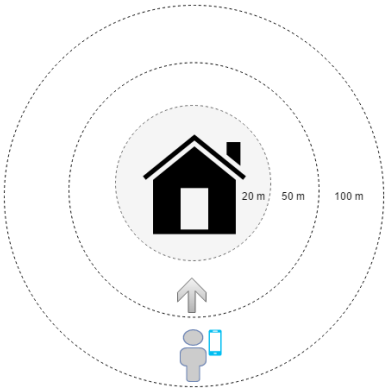
využít při návrhu tohoto konceptu. Mezi užitečné informace z mobilního zařízení, které lze využít, jsou údaje o aktuální poloze, teplotě, osvětlení, kalendáři uživatele apod. I tyto informace lze považovat za telemetrická data, která by bylo vhodné posílat do cloudu k dalšímu zpracování viz obrázek 24.



Obrázek 24 - Přenos telemetrických dat z mobilních zařízení (Zdroj: vlastní)

7.4 Geofencing

Geofencing si lze představit jako monitorovanou geografickou zónu (oblast), ve které se hlídá poloha mobilního zařízení (GPS). Pokud zařízení vstoupí do této vytyčené virtuální zóny, lze na tuto událost nějakým způsobem reagovat. Obdobná je i situace, kdy naopak zařízení z dané zóny vystoupí. Danou vymezující oblastí bývá nejčastěji hranice domu či bytu, ale může se jednat o jakékoliv jiné geografické vymezení. Tento koncept lze využít při návrhu chytrých domácností a domácí automatizaci. Na obrázku 25 je znázorněna ukázka vstupu uživatele do zóny, kde je aktivní Geofencing.



Obrázek 25 - Ukázka Geofenfingu s vyznačenými zónami (Zdroj: vlastní)

7.5 Analýza dat a možnosti jejich využití

Získáním telemetrických dat z měřidel energií a dat z mobilních zařízení se nabízí celá řada možností, jak s těmito daty naložit. Cílem tohoto konceptu je ukázat nové možnosti spojení dat z různých zdrojů a nad těmito daty provádět různé analýzy, predikce apod.

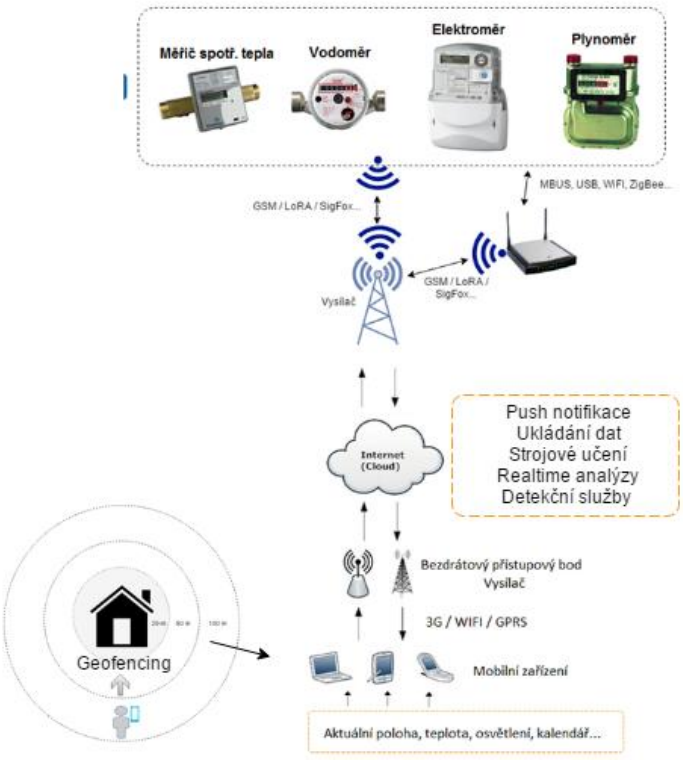
V rámci běžného Smart meteringu jsou již dnes nabízeny služby pro sledování měřeného média. Jedná se zpravidla o aktuální stav celkového odebraného množství a také možnost sledování spotřeby do historie za nějaký časový úsek (den, týden, měsíc apod.). Mezi základní rozšíření této služby je možnost notifikace na mobilní zařízení v případech, kdy hodnota (spotřeba za nějaké období) přesáhne určitý limit. Tato informace může uživateli pomoci k tomu, aby překontroloval, zda je vše v pořádku, nebo zda nedochází k nějakému problému (únik média, černý odběr, vadné měřidlo apod.). Způsobů, jak danou informaci sdělit uživateli je více. Může se jednat o klasické formy doručování informací (email, SMS), nebo je možné využít novější způsob v podobě Push notifikací. V takovém případě se očekává, že uživatel má ve svém mobilním zařízení nainstalovánu aplikaci, která umí tyto zprávy přijmout.

Do této chvíle ale nebylo využito žádných sesbíraných dat z mobilních zařízení (senzory, kalendář apod.) a jejich vzájemné propojení k získání „zajímavějších“ informací. Na tento koncept lze pohlížet ze dvou možných směrů a to z pohledu dodavatele distribuovaného média nebo odběratele média. Z pohledu dodavatele se může jednat o velmi cenná data pro plánování distribuce dodávek i případných odstávek. Jako velmi zajímavá kombinace informací se jeví například vnitřní

a venkovní teplota. Na základě těchto teplot je možné provádět predikce, zda daný objekt bude vytápěn či chlazen. V této fázi je vhodné zapojit i strojové učení, které by na základě dlouhodobě sbíraných dat bylo schopné přesněji predikovat budoucí stav. Např. tepelné čerpadlo za těchto teplot sepne a poběží dvě hodiny a spotřebuje 2 kWh, nebo mezi sedmou a osmou hodinou večerní je v domácnosti X spotřeba vody 200 litrů.
Koncept počítá s větším využitím chytrých služeb u odběratele média. Je to dáno především z důvodu toho, že poskytování „osobních" dat z mobilních zařízení může narážet na etiku, zda by vůbec někdo cizí měl mít přístup k těmto informacím (kalendář, lokace zařízení). Za jinou situaci lze považovat případ, kdy konzumentem chytrých funkcí bude sám uživatel (odběratel).

Velmi přínosnou vlastností tohoto konceptu může být ochrana majetku. Ochranou se rozumí jak minimalizace škod vzniklých havárií či poruchou, tak detekce pokusů o nelegální připojení na přípojku uživatele, detekce vloupání, detekce zapnutých spotřebičů apod. Pro většinu zmíněných případů bude vhodné kombinovat senzorická data z měřidel s geofencingem. Jako informační kanál pro sdělení konkrétní události lze zvolit Push notifikace popř. dle závažnosti i SMS zprávy.

Na základě strojového učení o předpokládané spotřebě v daný okamžik v kombinaci s dalšími informacemi (geofencing, kalendář), je možné vytvořit scénář, který bude reagovat na neobvyklé situace. Lze tak předejít případným škodám na majetku. V tomto scénáři se počítá s případy, kdy odchylka od normálního stavu zahrnující určitou toleranci dosahuje nějaké konkrétní hodnoty. Jinou situací je případ, kdy dle geofencingu či kalendáře není žádná osoba v objektu a je zjištěn mírný odběr média, který může značit nevypnutý spotřebič, nelegální odběr (připojení třetí osoby na přípojku uživatele) apod.
Na obrázku 26 se nachází infrastruktura celého navrženého konceptu.



Obrázek 26 - Architektura konceptu Smart metering s využitím MCC (Zdroj: vlastní)

Bezpečnost a ochrana dat

Data z IoT zařízení i mobilních zařízení jsou do cloudu přenášena v zabezpečeném šifrovaném formátu. Mezi zařízením a cloudem je použito TLS zabezpečení. Přenosový protokol pro zasílání zpráv je MQTT. Každé zařízení podléhá registraci a je při každém požadavku verifikováno (párové klíče s obměnou 1x za 24 hodin), aby nemohlo dojít k podvržení dat neoprávněnou osobou. Pokud by už došlo ke kompromitaci zařízení, je možné dané zařízení zablokovat, bez nutnosti blokace všech zařízení uživatele.

Aplikace pro mobilní zařízení

Nedílnou součástí tohoto konceptu je aplikace pro mobilní zařízení. Aplikace resp. služba na pozadí systému odesílá v pravidelných intervalech povolené údaje z mobilních zařízení. Mimo jiné musí být také schopna přijímat Push notifikace z cloudu, které informují formou notifikací o nastalých událostech. Mezi základní funkce pak patří zobrazení dat o spotřebě médií vhodnou formou (tabulky, grafy apod.).

Náměty na rozšíření a zlepšení

Nelze očekávat, že již první vytvořená verze bude dokonalá. V prvních verzích je nutné počítat s případnými falešnými či nesprávnými vyhodnoceními. Jednotlivé detekční algoritmy bude nutné dále rozvíjet a zdokonalovat. Je nutné si uvědomit, že se nejedná o triviální záležitost a faktorů vstupujících do rozhodovacích algoritmů a strojového učení je mnoho. Bude nutné stanovit jejich váhy a priority. Za další možné rozšíření lze považovat propojení s dalšími senzory a daty z externích zdrojů (meteorologické předpovědi apod.).

8 Závěr

Cílem této teoretické práce na téma Mobilní cloud computing ve vazbě na koncept Internet věcí bylo vymezit, co tyto pojmy znamenají a jak je lze v praxi využít v jednotlivých odvětvích.

Mobilní cloud computing přináší rozšíření cloudových služeb pro mobilní zařízení, která jsou často limitována svým hardwarem i výdrží na baterii. Smyslem tohoto spojení je dát mobilním zařízením přístup ke specifickým a často sofistikovaným službám, které se nachází v cloudu. Dalším významným argumentem používání mobilního cloud computingu je práce s daty a jejich zabezpečení. Ponechávat data pouze v mobilním zařízení není doporučeno z důvodu možné ztráty dat (poškození, ztráta, krádež). Velmi zajímavou oblastí, jak podpořit výkon mobilních zařízení, je technologie pro klonování obrazů fyzického zařízení do cloudu.

Velmi diskutovaným tématem dnešní doby se stává Internet věcí. V této práci je podrobněji rozebráno, co to je, jak se dá sestavit a jak se dá využít. V souvislosti s Internetem věcí jsou budovány speciální sítě, přes které je možné levně a energeticky úsporně komunikovat (Sigfox, LoRA, IQRF). S ohledem na omezený hardware, je často podceňována problematika zabezpečení komunikace IoT zařízení s Gateway.

Zabezpečení komunikace a obecně problematika bezpečnosti je v této práci podrobněji řešena. Problematika zabezpečení bývá velmi podceňovaným tématem. Většina výrobců IoT ji ani neřeší při návrhu svých řešení, ale spíše ji „dolepují“. V této souvislosti je nutné vyzdvihnout řešení české společnosti BigClown spadající do skupiny Jablotron, která jako první přichází s hardwarem, u kterého se na bezpečnost pamatovalo již od samotného počátku. Dle různých průzkumů se uvádí, že v roce 2020 bude na světě až několik desítek miliard IoT zařízení. Ať už výsledný počet bude jakýkoliv, tak s tímto počtem souvisí jedno zásadní omezení a to nemožnost použití stávajícího IPv4 protokolu. Bude nutné použít protokol IPv6, nebo najít nový standard adresace pro IoT zařízení.

V této práci je dále podrobněji řešena problematika zpracování velkých objemů dat. Zpracování velkého objemu dat je problematické jak u IoT zařízení, tak u velkého

počtu mobilních zařízení. Velmi diskutovaným pojmem v této oblasti je dnes BigData. Klasické relační databáze nejsou stavěny na tak velké množství dat, které je navíc nutné zpracovávat v reálném čase při příjmu a provádět nad těmito daty různé analytické úlohy apod.

Autor práce si vybral koncept Smart metering v kombinaci s mobilním cloud computingem na ukázku toho, jak je možné propojit mobilní cloud computing a Internet věcí. Za přidanou hodnotu lze pak považovat „chytré“ funkce, na které jsme doposud nebyli zvyklí. Cílem konceptu bylo předvést možnosti a směry, které je možné využít i na jiných projektech. V rámci cloudu je nabízena celá řada zajímavých a užitečných služeb, které lze využít k budování pokročilých a technologicky vyspělých projektů. Na podobném principu jako byl předveden koncept Smart metering v kombinaci s mobilním cloud computingem, by bylo možné postavit i jiné projekty např. monitoring pohybu dětí, zdravotní náramky s možností predikce určitých stavů (nevolnost, infarkt, epileptický záchvat, mozková příhoda apod.).

Dle autora byly cíle této práce splněny. Autor vidí velký potenciál v oblasti Internetu věcí, cloud computingu i mobilního cloud computingu. Díky těmto technologiím se otevírají nové možnosti v oblasti vývoje a výzkumu nových zařízení, které mohou sloužit lidem v různých oblastech života. IoT je často spojováno s chytrými domácnostmi a zařízeními určenými pro zábavu. Nicméně uplatnění nalezne ve všech oblastech lidské činnosti a především v oblastech, kde je možné zachraňovat lidské životy či je zkvalitňovat např. u nevidomých či jinak postižených lidí.

Úplným závěrem, jsem velmi rád, že jsem měl možnost se tomuto tématu věnovat a posunout se tak vědomostmi zase o velký kus dále.

Seznam použité literatury

[1] NIST, „Cloud Computing Synopsis and Recommendations," [Online]. Dostupné z: http://www.nist.gov/itl/cloud/. [Přístup získán 18. 06. 2012].

[2] Wikipedie, „Cloud computing," [Online]. Dostupné z: http://cs.wikipedia.org/wiki/Cloud_computing. [Přístup získán 20. 01. 2012].

[3] H. Chris a B. Prince, Azure in Action, Stamford: Manning Publications, 2010.

[4] J. Rosenberg a A. Mateos, The Cloud at Your service, Greenwich: Manning Publications, 2010.

[5] Wikipedia, „Cloud Computing," [Online]. Dostupné z: http://en.wikipedia.org/wiki/Cloud_computing#History. [Přístup získán 03. 02. 2012].

[6] Wikipedia, „Mobile Cloud Computing," [Online]. Dostupné z: https://en.wikipedia.org/wiki/Mobile_cloud_computing. [Přístup získán 20. 09. 2016].

[7] M. Antony, „Mobilní aplikace, Mobile Computing," [Online]. Dostupné z: http://mbi.vse.cz/public/cs/obj/FACTOR-133. [Přístup získán 23. 09. 2016].

[8] H. Qi a A. Gani, „Research on Mobile Cloud Computing: Review, Trend and Perspectives," University of Malaya, [Online]. Dostupné z: https://arxiv.org/ftp/arxiv/papers/1206/1206.1118.pdf. [Přístup získán 23. 09. 2016].

[9] P. Bahl, R. Y. Han, L. Erran Li a M. Satyanarayanan, „Advancing the State of Mobile Cloud Computing," [Online]. Dostupné z: http://research.microsoft.com/en-us/um/people/bahl/Papers/Pdf/mcs12_cloud.pdf. [Přístup získán 23. 09. 2016].

[10] M. Schüring, „Mobile cloud computing – open issues and solutions," University of Twente, [Online]. Dostupné z: http://referaat.cs.utwente.nl/conference/15/paper/7247/mobile-cloud-computing-open-issues-and-solutions.pdf. [Přístup získán 24. 09. 2016].

[11] P. Dharmale. a P. Ramteke, „Mobile Cloud Computing,“ [Online]. Dostupné z: https://www.ijsr.net/archive/v4i1/SUB15767.pdf. [Přístup získán 22. 09. 2016].

[12] Wikipedia, „Internet věcí,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Internet_v%C4%9Bc%C3%AD. [Přístup získán 20. 06. 2016].

[13] K. Aston, „Internet of Things in 2020 - A roudmap for the future,“ 2008. [Online]. Dostupné z: http://www.smart-systems-integration.org/public/documents/publications/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf. [Přístup získán 22. 06. 2016].

[14] P. Pohanka, „Internet věcí,“ [Online]. Dostupné z: http://i2ot.eu/internet-of-things/. [Přístup získán 22. 06. 2016].

[15] Intel, „Transform Business with Intelligent Gateway Solutions for IoT,“ [Online]. Dostupné z: http://www.intel.com/content/www/us/en/internet-of-things/gateway-solutions.html. [Přístup získán 01. 07. 2016].

[16] Wikipedia, „Arduino - Wikipedia,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Arduino. [Přístup získán 05. 07. 2016].

[17] Arduino.org „Arduino UNO,“ [Online]. Dostupné z: http://www.arduino.org/products/boards/arduino-uno. [Přístup získán 05. 07. 2016].

[18] Wikipedia, „Raspery Pi,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Raspberry_Pi. [Přístup získán 05. 07. 2016].

[19] HifyBerry, „The new Raspery Pi 3 is out,“ [Online]. Dostupné z: https://www.hifiberry.com/2016/02/the-new-raspberry-pi-3-is-out/. [Přístup získán 20. 07. 2016].

[20] P. Dramble, „Power Consumption | Raspberry Pi Dramble,“ [Online]. Dostupné z: http://www.pidramble.com/wiki/benchmarks/power-consumption. [Přístup získán 22. 07. 2016].

[21] Cooking Hacks, „Using Intel Galileo with the Arduino and Raspberry Pi shields designed by Cooking Hacks,“ [Online]. Dostupné z:

https://www.cooking-hacks.com/documentation/tutorials/intel-galileo-tutorial-using-arduino-and-raspberry-pi-shields-modules-boards/. [Přístup získán 27. 07. 2016].

[22] Santy, „Barometrický senzor BMP180," [Online]. Dostupné z: http://www.santy.cz/senzory-c24/sensor-bmp180-i179/. [Přístup získán 26. 07. 2016].

[23] Beryko, „Senzory v mobilních telefonech od A do Z," [Online]. Dostupné z: https://www.beryko.cz/blog/recenze/senzory-v-mobilnich-telefonech-od-a-do-z.html. [Přístup získán 03. 08. 2016].

[24] L. Michalec, „PIR detektor: skvělý sluha, ale zlý pán," [Online]. Dostupné z: http://vyvoj.hw.cz/automatizace/pir-cidlo-skvely-sluha-ale-zly-pan.html. [Přístup získán 29. 07. 2016].

[25] Adafruit, „PIR Motion Sensor Tutorial," [Online]. Dostupné z: http://www.instructables.com/id/PIR-Motion-Sensor-Tutorial/. [Přístup získán 02. 08. 2016].

[26] Wikipedia, „ZigBee," [Online]. Dostupné z: https://cs.wikipedia.org/wiki/ZigBee. [Přístup získán 05. 08. 2016].

[27] Wikipedia, „Bluetooth," [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Bluetooth. [Přístup získán 05. 08. 2016].

[28] J. Valter, „Co je RS 422, RS 485 a srovnání s RS 232," [Online]. Dostupné z: http://valter.byl.cz/co-je-rs422-rs485-a-srovnani-rs232. [Přístup získán 08. 08. 2016].

[29] Wikipedia, „CAN bus," [Online]. Dostupné z: https://cs.wikipedia.org/wiki/CAN_bus. [Přístup získán 05 08 2016].

[30] Wikipedia, „Rádiové vlny," [Online]. Dostupné z: https://cs.wikipedia.org/wiki/R%C3%A1diov%C3%A9_vlny. [Přístup získán 20. 08. 2016].

[31] SimpleCell, „Technologie SIGFOX," [Online]. Dostupné z: https://www.simplecell.eu/?gclid=CImx6rWwlM8CFUSVGwodufYNmg. [Přístup získán 29. 08. 2016].

[32] J. Mazal, „Síť pro internet věcí v ČR otevírá nové obchodní příležitosti,"

[Online]. Dostupné z: http://channelworld.cz/rozhovory/sit-pro-internet-veci-v-cr-otevira-nove-obchodni-prilezitosti-16582. [Přístup získán 12. 09. 2016].

[33] M. Mácha, „LoRa Technology," [Online]. Dostupné z: http://www.osel.cz/8732-lora-technology.html. [Přístup získán 13. 09. 2016].

[34] České radiokomunikace, „Technické aspekty technologie LoRa," [Online]. Dostupné z: http://pripoj.me/technicke-aspekty-technologie-lora/. [Přístup získán 15. 09. 2016].

[35] Vodafone, „Vodafone si pro rozšíření služby Internet věcí vybral technologii NB-IoT," [Online]. Dostupné z: https://www.vodafone.cz/o-vodafonu/o-spolecnosti/pro-media/tiskove-zpravy/detail/vodafone-si-pro-rozsireni-sluzby-internet-veci-vyb/. [Přístup získán 16. 09. 2016].

[36] České radiokomunikace, „PRŮZKUM: 8 Z 10 ČECHŮ NIKDY NESLYŠELO POJEM INTERNET VĚCÍ," [Online]. Dostupné z: https://www.radiokomunikace.cz/pruzkum-8-z-10-cechu-nikdy-neslyselo-pojem-internet-veci. [Přístup získán 15. 09. 2016].

[37] S. Netoličková, „Fyzika a klasická energetika - Smart Metering," [Online]. Dostupné z: http://www.3pol.cz/cz/rubriky/fyzika-a-klasicka-energetika/699-smart-metering. [Přístup získán 15. 09. 2016].

[38] L. Vojtěch a D. Lopour, „Internet věcí – kam kráčíme," [Online]. Dostupné z: http://www.dps-az.cz/zajimavosti/id:6700/internet-veci-kam-kracime. [Přístup získán 02. 10. 2016].

[39] S. Kimple, „Why Should You Use Azure IoT Suite Over Event Hub?," [Online]. Dostupné z: https://blog.tallan.com/2015/12/08/azure-iot-hub-vs-event-hub/. [Přístup získán 02. 10. 2016].

[40] Amazon, „How AWS IoT Works," [Online]. Dostupné z: http://docs.aws.amazon.com/iot/latest/developerguide/aws-iot-how-it-works.html. [Přístup získán 02. 10. 2016].

[41] Google, „Architecture: Real-Time Stream Processing for IoT," Google, [Online]. Dostupné z:

https://cloud.google.com/solutions/architecture/real-time-stream-processing-iot. [Přístup získán 03. 10. 2016].

[42] Wikipedia, „Hypertext Transfer Protocol,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Hypertext_Transfer_Protocol. [Přístup získán 03. 10. 2016].

[43] Z. Břicháček, „Využití protokolu MQTT nejen pro M2M a IoT,“ [Online]. Dostupné z: https://blog.brichacek.net/vyuziti-protokolu-mqtt-nejen-pro-m2m-a-iot/. [Přístup získán 03. 09. 2016].

[44] O. Dolák, „Big data - Nové způsoby zpracování a analýzy velkých objemů dat,“ [Online]. Dostupné z: http://www.systemonline.cz/clanky/big-data.htm. [Přístup získán 06. 09. 2016].

[45] S. Bappalige, „An introduction to Apache Hadoop for big data,“ [Online]. Dostupné z: https://opensource.com/life/14/8/intro-apache-hadoop-big-data. [Přístup získán 03. 09. 2016].

[46] S. Prakash, „Storing and Querying Big Data in Hadoop (HDFS),“ [Online]. Dostupné z: http://ecomcanada.org/blog/tag/hadoop-architecture/. [Přístup získán 04. 09. 2016].

[47] Microsoft, „The Ins and Outs of Azure Stream Analytics – Real-Time Event Processing,“ [Online]. Dostupné z: 06.

[48] M. Vattipulusu, „AWS Kinesis,“ [Online]. Dostupné z: https://madhuvattipulusu.wordpress.com/2014/10/16/aws-kinesis/. [Přístup získán 08. 09. 2016].

[49] Wikipedia, „Strojové učení“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Strojov%C3%A9_u%C4%8Den%C3%AD. [Přístup získán 10. 09. 2016].

[50] Wkipedia, „Hardwarový generátor náhodných čísel,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Hardwarov%C3%BD_gener%C3%A1tor_n%C3%A1hodn%C3%BDch_%C4%8D%C3%ADsel. [Přístup získán 20. 09. 2016].

[51] Wikipedia, „Triple DES,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Triple_DES. [Přístup získán 20. 09. 2016].

[52] Mendelova univerzita, „Symetrická kryptografie,“ [Online]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7026. [Přístup získán 20. 09. 2016].

[53] Wikipedia, „Asymetrické šifrování,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie. [Přístup získán 21. 09. 2016].

[54] Wikipedia, „HTTPS,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/HTTPS. [Přístup získán 22. 09. 2016].

[55] Wikipedia, „Transport Layer Security,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Transport_Layer_Security. [Přístup získán 22. 09. 2016].

[56] M. Valášek, „Představení IoT platformy BigClown,“ [Online]. Dostupné z: https://channel9.msdn.com/Events/Czech-Devs/predstaveni-iot-platformy-bigclown. [Přístup získán 02. 09. 2016].

[57] J. Zahradníček, „Právní aspekty cloud computingu,“ [Online]. Dostupné z: www.cssi.cz/cssi/system/files/all/SI_2015_01_Zahradnicek.pdf. [Přístup získán 05. 10. 2016].

[58] MFF UK, „Smart metering – nová koncepce měření,“ [Online]. Dostupné z: artemis.ms.mff.cuni.cz/main/tiki-download_file.php?fileId=47. [Přístup získán 4. 11. 2016].

[59] Gasag, „Smart metering - GASAG,“ [Online]. Dostupné z: https://www.gasag.de/geschaeftskunden/loesungen/energiedienstleistungen/smart-metering/seiten/default.aspx. [Přístup získán 01. 05. 2015].

[60] Wikipedia, „Průmysl 4.0,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Pr%C5%AFmysl_4.0. [Přístup získán 17. 09. 2016].

[61] Wikipedia, „Systém základnových stanic,“ [Online]. Dostupné z: https://cs.wikipedia.org/wiki/Syst%C3%A9m_z%C3%A1kladnov%C3%BDch_stanic. [Přístup získán 22. 09. 2016].

[62] Analog Devices, „Temperature Sensor - TMP36,“ [Online]. Dostupné z: https://www.sparkfun.com/products/10988. [Přístup získán 22. 09. 2016].

Seznam obrázků

Seznam tabulek