

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

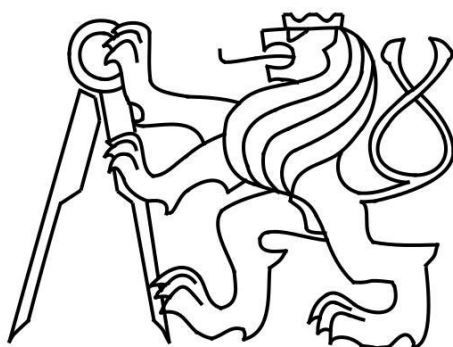
BAKALÁŘSKÁ PRÁCE

2017

Tomáš Straka

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická
Katedra telekomunikační techniky



Bakalářská práce

Cloudové služby v prostředí technologické firmy

Cloud services in a technology company

Květen 2017

Bakalant: Tomáš Straka
Vedoucí práce: Ing. Bc. Marek Neruda, Ph.D

Čestné prohlášení

Prohlašuji, že jsem zadanou bakalářskou práci zpracoval sám s přispěním vedoucího práce a konzultanta a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé bakalářské práce nebo její části se souhlasem katedry.

V Praze dne 26. 5. 2017

.....

Podpis bakalanta

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Straka** Jméno: **Tomáš** Osobní číslo: **426065**
Fakulta/ústav: **Fakulta elektrotechnická**
Zadávající katedra/ústav: **Katedra telekomunikační techniky**
Studijní program: **Komunikace, multimédia a elektronika**
Studijní obor: **Sít'ové a informační technologie**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Cloudové služby v prostředí technologické firmy

Název bakalářské práce anglicky:

Cloud services in a technology company

Pokyny pro vypracování:

Zhodnoťte dostupné cloudové služby pro ukládání a vizualizaci dat z připojené senzorové sítě a procesů technologické firmy. Uvažujte nákladovost, spolehlivost, prostředí malých podniků a bezpečnost. Zrealizujte demo sestávající se z vybraných senzorů, mini PC a cloudové služby a zhodnoťte navržené řešení z pohledu výše uvedených parametrů.

Seznam doporučené literatury:

[1] Weber, R. H.; Weber, R.: Internet of things. Vol. 12. New York, NY, USA.: Springer, 2010. ISBN: 978-3-642-11709-1.
[2] Krutz, R. L.; Russell, D. V.: Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing, 2010. ISBN: 978-0-470-58987-8.

Jméno a pracoviště vedoucí(ho) bakalářské práce:

Ing. Marek Neruda Ph.D., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **17.02.2017** Termín odevzdání bakalářské práce: **26.05.2017**

Platnost zadání bakalářské práce: **30.09.2018**

Podpis vedoucí(ho) práce

Podpis vedoucí(ho) ústavu/katedry

Podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student bere na vědomí, že je povinen vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

Datum převzetí zadání

Podpis studenta

Poděkování

Rád bych tímto poděkoval Ing. Bc. Marku Nerudovi, Ph.D. za cenné rady a konzultace týkající se bakalářské práce v průběhu semestru.

Abstrakt:

Tato práce se zabývá zhodnocením cloudových služeb z pohledu nákladovosti, spolehlivosti a bezpečnosti pro využití technologickou firmou. V teoretické části je obecně popsána problematika cloudových služeb, sensorových sítí a služeb spojených s procesy technologické firmy. V praktické části jsou cloudové služby porovnávány z hlediska výše zmíněných pohledů podle toho, jestli jsou umístěny v cloudu, nebo v serveru firmy. Závěr praktické části je věnován zhodnocení dema, které představuje službu v obou variantách umístění.

Klíčová slova:

Cloudové služby, internet věcí, procesy technologické firmy, sensorová síť

Abstract:

This thesis deals with the evaluation of cloud services from the point of costs, reliability, and security for a technological company. In theoretical part the problematic of cloud services, sensor networks, and services accompanying the processes of a technological company is described. In practical part, the cloud services are compared from the aforementioned standpoints based on being situated in a cloud, or on company servers. Ending of the practical part is dedicated to rating a demo, that presents the service in both variants of situation.

Index Terms:

Cloud services, Internet of Things, processes of the technology company, sensor network

Obsah

1 Úvod.....	1
2 Internet věcí.....	3
2.1 Cloudové služby.....	5
2.1.1 Základní charakteristické vlastnosti cloudových služeb.....	6
2.1.2 Modely nasazení.....	7
2.1.3 Distribuční model cloudu.....	8
2.1.4 Výhody a nevýhody cloudových služeb.....	10
2.1.5 Bezpečnost a rizika cloudových služeb.....	11
3 Senzorová síť.....	13
3.1 Senzory.....	13
3.1.1 Drátové senzory.....	15
3.1.2 Bezdrátové senzory.....	16
3.1.3 Optické senzory.....	18
3.2 Datalogery.....	20
3.2.1 Jednoúčelové.....	20
3.2.2 Víceúčelové.....	21
3.3 Úložiště dat.....	21
3.3.1 Lokální souborový systém.....	22
3.3.2 Lokální databáze.....	22
4 Procesy technologické firmy.....	23
4.1 Plánování podnikových zdrojů.....	24
4.1.1 Funkce ERP systémů.....	25
4.1.2 Charakteristiky firemního ERP systému typu cloud.....	25
4.2 Správa dokumentů.....	27
4.2.1 Funkce DMS systémů.....	28
4.2.2 Charakteristiky DMS systému typu cloud.....	29
5 Zhodnocení cloudových služeb.....	30
5.1 Nákladovost.....	31
5.1.1 Ze sensorové sítě.....	31
5.1.2 Z procesů technologické firmy.....	36

5.2 Spolehlivost.....	42
5.2.1 Ze sensorové sítě.....	43
5.2.2 Z procesů technologické firmy.....	45
5.3 Bezpečnost.....	47
5.3.1 Ze sensorové sítě.....	49
5.3.2 Z procesů technologické firmy.....	50
6 Demo.....	53
6.1 Použité prostředky.....	53
6.1.1 Hardware.....	53
6.1.1 Software.....	56
6.2 Princip činnosti.....	58
6.2.1 Demo jako lokální řešení.....	59
6.2.2 Demo jako řešení v cloudu.....	60
6.3 Zhodnocení řešení.....	61
6.3.1 Nákladovost.....	61
6.2.2 Spolehlivost.....	63
6.2.3 Bezpečnost.....	63
7 Závěr.....	65

1 Úvod

Cloudové služby jsou posledních několik let často skloňovány ve spojitosti s ulehčováním činností v mnoha oblastech jako jsou chytré domácnosti, průmysl, podnikové systémy, a především internetu věcí. V této práci bych se rád zaměřil především na zhodnocení dostupných cloudových služeb, které by mohly být přínosné při využití v technologické firmě. Zaměřil jsem se především na využití senzorových sítí, podnikových informačních systémů a systémů pro správu dokumentace.

Pojem cloudová služba si lze představit jako službu pro ukládání dat mimo vlastní fyzické uložení, ale to je jen jedna z mnoha možností, kterou tyto služby představují. Jednou z oblastí působení cloudů jsou tzv. IoT cloudy. Tyto cloudy, resp. jejich platformy a aplikace ulehčují sběr dat ze senzorových sítí. Při množství dat, které dnešní rozsáhlé senzorové sítě generují mnohdy obyčejný PC, nebo server pro zpracování a uložení dat nestačí. Proto firmy přistupují ke cloudovým řešením, které představují téměř neomezený výpočetní a úložný prostor.

Další možností využití cloudových služeb je v oblasti správy procesů firmy. Cílem každé firmy je, aby se vnitřní i vnější procesy zrychlovaly a zkvalitňovaly, a tím se dosáhlo úspory času a financí. Za tímto účelem byly vytvořeny cloudové služby, resp. systémy běžící v cloudu, tzv. systémy pro plánování podnikových zdrojů. Každá firma má svá oddělení (financí, výroby, marketingu, prodeje atd.), které pracují odděleně. Ve chvíli, kdy je potřeba, aby spolu tyto oddělení spolupracovali však může nastat problém v podobě rozdílných systémů, které oddělení využívají. Toto se snaží služba eliminovat tím, že v sobě kloubí veškeré funkce, které jednotlivá oddělení vyžadují. Mezi další funkce těchto služeb patří např. sdružování veškerých podnikových dat, automatizace procesů apod. Výhodou se jeví jejich rozšiřitelnost o další služby podle potřeb firem.

Jako další využitelná služba se jeví služba, resp. systém pro správu dokumentace. Mnohdy mají firmy dokumenty pouze v papírové podobě, nebo v souborech v jednotlivých PC, které nemají jednotné uložení. Při snaze zaměstnanců dokumenty nalézt a pracovat s nimi tak mnohdy stráví mnoho času navíc. Systémy pro správu dokumentů umožňují sjednotit veškerou dokumentaci pod jeden systém. Kromě této funkce mnohdy umožňují také digitalizaci papírových dokumentů a umožňují nastavení workflow pro oběh dokumentů ve firmě.

Všechny tyto služby mají něco společného, a to je citlivost firemních dat. Proto se v práci zaměřuji na porovnávání cloudových služeb, tedy služeb běžících v cloudu a

„On-premises“ služeb, tedy služeb, které běží v serveru firmy. V teoretické části jsou popsány cloudové služby, senzorová síť a procesy technologické firmy. V praktické části je popsán průzkum trhu se zmíněnými cloudovými službami a následné porovnávání vybraných služeb z pohledu nákladovosti, spolehlivosti a bezpečnosti pro firmy. V závěru praktické části je prezentována demo ukázka, která představuje službu jak běžící v cloudu, tak v lokálním serveru a tyto dvě varianty bych porovnal z výše zmíněných pohledů.

Přínosem této práce jsou odpovědi na otázku, jestli se hodí pro firmu více umístění služby v cloudu nebo v lokálním serveru, či kombinace obojího. Práce může být nápomocna lidem, kteří se o tuto problematiku zajímají a mohli by v ní nalézt odpovědi na některé své otázky, případně by jim mohla pomoci s volbou vhodné služby.

2. Internet věcí

Definice pojmu „internet věcí“, dále jen IoT (Internet of Things), není striktně dána a těžko jí tak lze obecně vyjádřit. Podle Pavla Buriana, autora knihy „Internet inteligentních aktivit“ lze Internet věcí definovat jako: *„Dynamická globální síťová infrastruktura s vlastními možnostmi konfigurace, založena na standardních komunikačních protokolech a interoperabilitě, kde fyzické a virtuální „věci“ mají vlastní identitu, fyzické atributy a virtuální inteligentní programové agenty, které jsou integrovány do informační sítě.“* [1].

Podobnou definici například uvádí Pavel Pohanka jako: *„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.“* [14]. Taková krátká, ale výstižná definice je od Libora Michalce, autora článku „Velký přehled cloudů pro IoT“ který říká, že: *„IoT (Internet věcí) můžeme nazvat vše, co komunikuje, a to nejen bezdrátově.“* [2].

Poprvé byl tento pojem použit v roce 1999 jistým Kevinem Ashtonem v jeho prezentaci [14]. Další důležité období pro IoT je mezi roky 2008 a 2009, na které se datuje vznik označení „Internet věcí“, tedy označení pro definici, která je uvedena výše [15]. Společnost Cisco předpovídala, že kolem roku 2015 bude k internetu připojeno okolo 25 miliard zařízení a do roku 2020 až 50 miliard zařízení [15]. Nutno podotknout, že tento předpoklad je z roku 2011, podle statistik uvedených na webu statistica.com z roku 2015, bylo ve stejném roce dosaženo 15 miliard zařízení a pro rok 2020 se předpokládá nárůst na necelých 31 miliard zařízení [14].

Pro úplné pochopení konceptu IoT je třeba si říct, co znamená označení „věc“. Je tak označován neživý objekt (fyzický, nebo virtuální), který se skládá z hardwaru a softwaru a je schopen snímat určitá data (fyzikální veličiny, polohy strojů apod.). Jedná se tak o zařízení, které autonomně poskytuje získaná data, která jsou dále sdílena s dalšími zařízeními, tj. „věcmi“ podle druhu jejich připojení do sítě (drátově, bezdrátově, opticky) [14]. Příkladem mohou být např. senzory teploty, vlhkosti a další. Podle druhu připojení se využívají také různé druhy komunikačních protokolů, o kterých se budu detailněji zmiňovat v kapitole 3. IoT tedy označuje síť fyzických objektů, které jsou vybavené technologií umožňující zachytit jejich vnitřní stavy a dále získaná data pomocí komunikace poskytovat svému okolí [17].

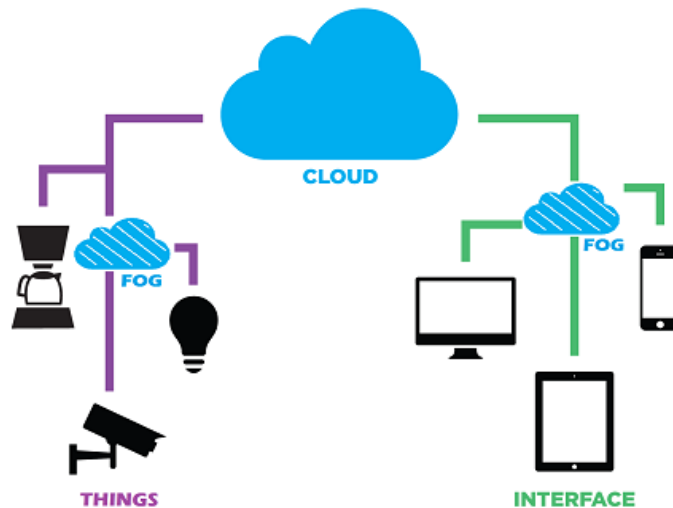
„Cílem IoT je propojení zařízení, systémů a služeb za účelem poskytnutí více dat, která mohou být převedena na informace a informace na znalosti, které lze následně aplikovat.“ [14]. To znamená, že čím víc dat budeme schopni získávat a analyzovat, tím víc lze nově získané informace využít k rozvoji a pokroku. Obecné označení IoT se dá dále rozdělit podle oblastí jeho využití, nejčastěji se ale uvádí rozdělení na „spotřebitelský internet věcí“ (CloT – Consumer IoT) a „průmyslový internet věcí“ (IIoT – Industrial IoT). Dohromady představují vše, Co se od IoT očekává [18].

CloT lze charakterizovat jako odvětví ve kterém jsou aplikace orientované na spotřebitele, především tak na spotřebitelská zařízení. Tyto zařízení, často označovaná jako inteligentní denně usnadňují životy lidí v podobě automatizace procesů v domácnosti, různých fitness náramků a jim podobným zařízením. Selhání těchto aplikací nemá kritické následky, například selhání chytrého náramku nezpůsobí jiné škody krom finančních [18]. Oproti tomu selhání zařízení v IIoT může mít výrazný vliv na bezpečnost, jelikož se jedná o zaměření na průmyslové aplikace, tedy zařízení pro chytrá města, průmysl, dopravu a energetiku. Selhání komunikace s dopravním značením, nebo výrobním pásem by tak mohlo vést k závažným haváriím [18].

Aby IoT bylo efektivním řešením, musí splňovat základní požadavky. Prvním a nejmíc diskutovaným je bezpečnost přenosu dat. Při jejich přenosu musí být nutně zajištěno šifrování, a to především při bezdrátovém přenosu, aby nedošlo k odposlechnutí či jinému zneužití dat neoprávněným prostředkem/uživatelé. Dalšími požadavky jsou například interoperabilita, efektivní přenos a zpracování dat [17]. Ze strany zhotovitele je pak důležité snadné nasazení řešení a jednoduchá integrace do již hotového řešení [17].

V této práci se budu především snažit o popsání spojení a následného využití IoT a cloudových služeb, proto je třeba zmínit, jaké jsou možnosti tohoto spojení. Jedno řešení je tzv. „**Fog computing**“, které říká, že zařízení (věci) komunikují mezi sebou, dochází tak k lokálnímu sběru dat, která jsou vyhodnocena lokálně a poté putují do cloudu [17]. Příkladem může být semafor, který kamerou vidí příjezdějí sanitku a reaguje svým nastavením na vzniklou situaci. Nicméně zpoždění v přenosové síti by mohlo být takové, že by informace, rozhodovaná v cloudovém řešení, mohla být irelevantní. Rozhodující logika se tak v tomto řešení přesouvá na rozhraní mezi koncové zařízení a cloud, situace je vyřešená lokálně a sanitka dostává okamžitou přednost [19]. Jde tak o řešení umožňující rychlejší odezvu, vyšší spolehlivost a snížení nákladů.

Druhým řešením je **přímá komunikace zařízení a cloudu**. Využívá se především v oblastech, kde se neklade velký důraz na rychlou odezvu a na případné následky při výpadku spojení. Veškeré zpracování a vyhodnocování je tedy úkolem cloudové služby, zařízení se stará pouze o sběr a přenos dat [17].



Obr. 2.1 Fog a cloud řešení, převzato z [21].

2.1 Cloudové služby

Význam slova cloud neboli v českém překladu mrak nelze jednoznačně definovat. Existuje mnoho podob, jak lze cloud charakterizovat, nejvíce se však vychází z definice, která je uvedena v dokumentu „The Nist Definition of Cloud Computing“ [11] z roku 2011, který vydal Národní institut standardů a technologie (dále jen NIST). Pojem cloud zahrnuje nespočetný počet aplikací a služeb poskytovaných prostřednictvím internetu. Poskytovatel disponuje vlastními výpočetními prostředky (servery, úložiště, aplikace), které lze rychle poskytnout s minimálním úsilím a interakcí s poskytovatelem [11]. Tyto služby jsou pomocí internetu zpřístupněné zákazníkovi za nízké poplatky s možností okamžité škálovatelnosti dle potřeby zákazníka.

Základem tak je, že veškeré nabízené prostředky jako infrastruktura, vývojové platformy a software jsou poskytovány formou služby, ke které uživatel přistupuje přes internet pomocí webového rozhraní, nebo předem připravené aplikace. Tyto služby jsou zpoplatněné dle různých tarifů, nejčastěji se objevuje tzv. „pay as you go“ tarif, tedy platba za to, co doopravdy využíváte, nebo tzv. „pay per user“, tedy platba za jednoho uživatele služby. Vyúčtování probíhá většinou v měsíčních intervalech, ale objevují se řešení s roční platbou. Dnes již mnoho poskytovatelů cloudových služeb

nabízí tzv. „Free-trial“, tedy uživatelský účet, který na omezenou dobu zpřístupní všechny služby, aby si mohl zákazník službu nejdříve vyzkoušet a někteří dokonce poskytují balíčky služeb, které jsou doživotně zdarma s určitým omezením.

2.1.1 Základní charakteristické vlastnosti cloudových služeb

Podle definice NIST by měl cloud splňovat pět nezbytných charakteristických vlastností. První takovou charakteristickou vlastností je **široká dostupnost přes síť**. Přístup ke službám je tak přes internet dostupný z velké škály zařízení jako jsou stolní počítače, notebooky, tablety a mobilní telefony [11]. Společnosti, které využívají tento přístup ke cloudovým službám, musí často řešit problémy spojené s ukládáním citlivých dat, a tak se nejčastěji uchylují k řešení v podobě privátního cloudu [12].

Další charakteristickou vlastností je **samoobsluha podle potřeby**. Zákazník tak dostává možnost pomocí uživatelského rozhraní samostatně upravovat a dle potřeb flexibilně rozšířit využívané služby bez nutnosti komunikace s jejich poskytovatelem [11].

Aby se plně využíval potenciál poskytované infrastruktury, využívá se tzv. **sdílení a slučování prostředků**. Výpočetní prostředky poskytovatele jsou slučovány tak, aby obsloužili několik zákazníků pomocí tzv. multi-tenant modelu ve sdíleném prostředí a docházelo tak k dynamickému přiřazování, nebo odebrání těchto prostředků dle aktuální potřeby [11]. Virtualizace umožňuje přidělit každému zákazníkovi část prostředků, které se tváří jako virtuální stroj. Tyto virtuální stroje se nachází na sdílených discích, ke kterým přistupuje i několik uživatelů, ale jsou od ostatních strojů virtuálně oddělené a tím je zajištěno, že žádný uživatel nemá možnost přistupovat k datům jiného uživatele [1].

„Rapid elasticity“, doslova přeložené jako **rychlá pružnost** je další charakteristickou vlastností. Znamená to schopnost cloudu rychle a jednoduše vytvářet, přidávat, navyšovat, snižovat a rušit využití prostředků podle potřeb zákazníka. Dochází tak ke snižování nákladů na provoz a rychlejšímu nasazení služby. Poskytovatel většinou disponuje rozsáhlou, dobře spolupracující infrastrukturou, a tak se můžou uživatelé jevit dostupné služby jako neomezené [11].

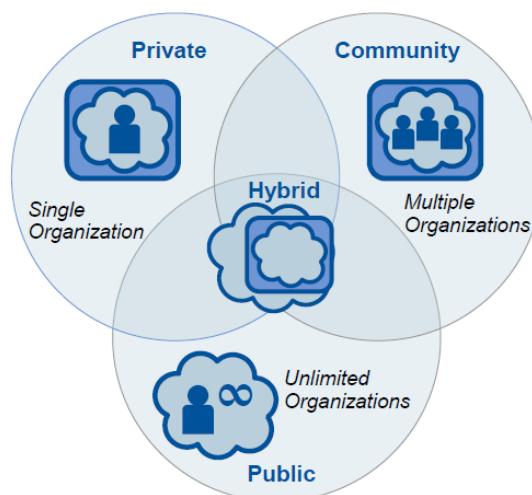
To, co zákazník využívá z nabídky poskytovatele, musí být měřitelné, tedy poslední vlastností je **měřitelnost poskytovaných služeb**. Jedná se o schopnost sledovat a měřit vytíženost a využívanost konkrétní služby [11]. Lze měřit například výpočetní prostředky, které byly na její provoz vynaloženy, nebo různé úrovně výkonů a dostupnosti [13].

2.1.2 Modely nasazení

Model nasazení cloudu udává, jakým způsobem je služba využívána uživatelem, kde jsou data uložena a kdo je provozovatelem a správcem zvoleného řešení. Podle NIST lze dělit modely nasazení na [11]:

- Veřejný
- Privátní
- Komunitní
- Hybridní

Každý z těchto modelů má své specifické vlastnosti a platí pro něj určitá pravidla.



Obr. 2.2 Modely nasazení cloudu, převzato z [20].

Veřejný

Veřejným cloudem je dnes označován cloud tak, jak je nejvíce chápán. Veřejné cloudy jsou provozované na sdílené platformě poskytovatele, který dodává výpočetní prostředky jako jsou servery a datová úložiště [1]. Jak napovídá název, služby jsou dostupné nejširší společnosti, tedy veřejnosti a uživatelé k nim přistupují pomocí webového rozhraní, nebo aplikace k tomu určené. U veřejného cloudu je veškerý software i hardware vlastněn poskytovatelem [6]. Služby jsou většinou uzpůsobené tak, aby nabízely stejné funkce pro všechny uživatele a uspokojily co nejvíce společných požadavků veřejnosti. Mezi nejvíce užívané služby ve veřejném cloudu se řadí například „Microsoft Azure“ a „Google G Suit“ [7].

Privátní

Privátní cloud je alternativou k veřejnému cloudu, poskytuje tedy infrastrukturu se stejnými službami, ale pouze v rámci jedné organizace [1]. Privátní cloud lze dělit podle jeho umístění, a to buď v datovém centru (zázemí pro uložení a provoz serverů) organizace, nebo v datovém centru třetí strany. Výhodou vlastního datového centra je především bezpečnost citlivých dat. Při využívání privátního cloudu je kladen důraz především na stabilní internetové připojení, vysokou dostupnost a škálovatelnost [8].

Komunitní

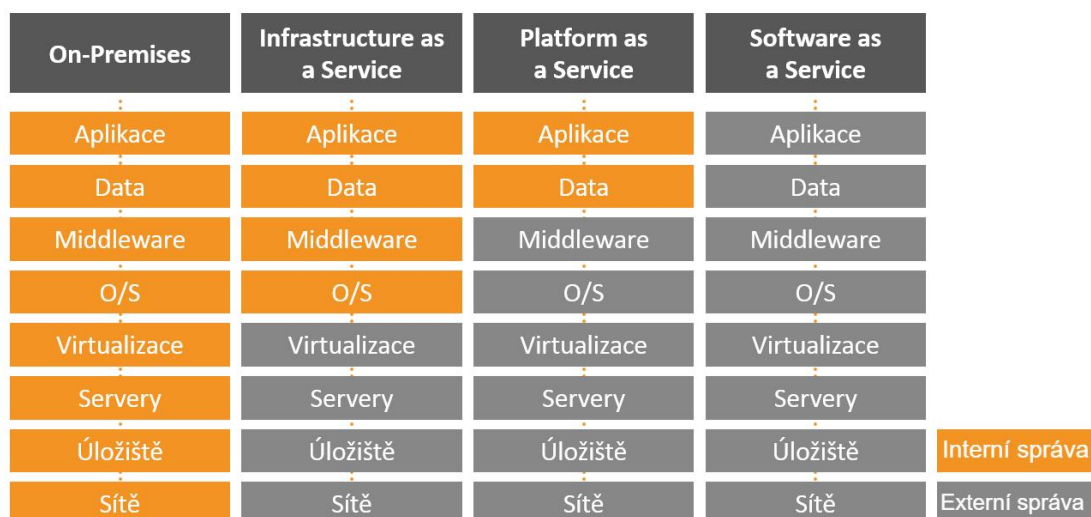
Jako komunitní cloud se označuje cloud, který je dostupný a přizpůsobený pro určitou skupinu lidí se stejnými zájmy a požadavky na poskytované služby [1]. Cloud vzniká po dohodě více subjektů, které si předem stanoví podmínky a politiku fungování. Jedná se například o státní organizace nebo o více společností, které spolupracují.

Hybridní

Kombinací modelů privátního a veřejného cloudu vznikl cloud označovaný jako hybridní, který navenek působí jako jeden konzistentní model [1]. Hlavní výhodou takového řešení je, že v sobě snoubí rychlost veřejného modelu s kontrolou a zabezpečením privátního modelu [10]. Tento model se nejvíce hodí pro firmy, které potřebují svá citlivá data, která podléhají přísným bezpečnostním požadavkům uchovávat mezi čtyřmi stěnami a zároveň vzdáleně přistupovat a pracovat s jinými daty.

2.1.3 Distribuční model cloudu

Distribuční model reprezentuje, co je v rámci poskytované služby nabízeno. Obvykle se jedná o hardware, software anebo jejich kombinaci. [2] Jednotlivé modely se od sebe liší také podle poměru kontroly a vlastnictví uživatele a poskytovatele.



Obr. 2.3 Distribuční modely cloudu, převzato z [5].

Infrastructure as a Service – IaaS

Základním typem distribučního modelu je infrastruktura jako služba. Ta představuje připravenou výpočetní infrastrukturu, kterou zajišťuje poskytovatel služby. Jedná se typicky o virtuální stroje s možnostmi rozsáhlé škálovatelnosti, ke kterým lze vzdáleně přistupovat a spravovat je bez nutnosti vlastnit hardware, na kterém tyto stroje běží. Jde tak o ekonomickou volbu, kterou lze eliminovat vysoké počáteční náklady spojené s nákupem a provozem vlastního hardwaru [1, 2]. Mezi nejvíce využívané služby IaaS patří „Microsoft Azure“, nebo „Amazon Web Services“ [3].

Platform as a Service – PaaS

Další typ distribučního modelu je platforma jako služba, kterou lze charakterizovat jako úplné prostředí pro vývoj a nasazení v cloudu [2]. Podobně jako v IaaS je zde zahrnuta infrastruktura (virtuální stroje, úložiště a sítě), ale také tzv. solution stack, tedy software, který poskytuje uživateli možnost využívat vývojářské nástroje ke tvorbě vlastních cloudových aplikací. Uživatel se tak zabývá pouze instalací, provozem a údržbou své aplikace, zatímco poskytovatel se stará o infrastrukturu a správu vývojářských nástrojů [1]. Typickým poskytovatelem této služby je například „Google App Engine“ nebo „Force.com“.

Software as a Service – SaaS

Zatímco model PaaS nabízí uživateli prostředí pro tvorbu a běh jeho aplikací, model „Software jako služba“ nabízí již hotové aplikace, které jsou licencovány a pronajímány jako služby uživateli [1]. Aplikace jsou provozované v cloudovém prostředí, odpadá tak nutnost jakékoliv instalace na lokální hardware. K aplikaci se přistupuje z webového prohlížeče, nebo speciální klientské aplikace, tím je zajištěna nezávislost na platformě zákazníka [4]. Dnes je takto nabízeno široké portfolio aplikací. Mezi nejznámější produkty se řadí například firemní sada aplikací „Google G Suite“, či „Microsoft Office 365“.

On-premises

Jedná se o model, ve kterém je hardware i software ve vlastnictví zákazníka a je provozován interně, nikoliv na externím zařízení, nebo v cloudu. Veškerá správa je tak v kompetenci zákazníka a poskytovatel služby zde figuruje pouze jako dodavatel určitého softwaru [5]. Toto řešení umožňuje přímý dohled nad spravovanými daty, ale má i mnoho úskalí jako je nebezpečí ztráty dat v důsledku žádného, nebo malého zabezpečení a výrazně velká počáteční investice do hardwaru. Řešení „On-premises“ nabízí například společnost Microsoft jako produkt „Azure Stack“, či společnost SAP s produktem „SAP HANA“.

2.1.4 Výhody a nevýhody cloudových služeb

Výhody

Všechny charakteristické vlastnosti uvedené v kapitole 2.1.1 jsou zároveň také silné výhody, kterými cloudové služby disponují oproti „On-premises“ řešení. Tyto služby jsou dnes dostupné téměř komukoliv a pro jejich zřízení často stačí pouze pár minut času, který je třeba strávit vyplněním zřizovacího formuláře bez nutnosti interakce s poskytovatelem. Jelikož se jedná o předpřipravenou infrastrukturu, může tak zákazník ke službě **přistoupit téměř okamžitě po jejím zřízení**. Další výhodou je, že zákazník může k datům přistupovat v podstatě odkudkoliv, **nezávisle na platformě**, kterou využívá. Rozhraní pro správu služeb bývá uzpůsobeno tak, aby jej zvládl **zákazník ovládat sám**, a tak byl ušetřen čas, který by museli oba, zákazník i poskytovatel, věnovat společné komunikaci.

Z finančního hlediska lze díky celkové infrastruktuře od poskytovatele snížit **počáteční náklady** [1]. Velikou výhodou se jeví **nabízené platební modely**, ve kterých uživatel platí pouze to, co opravdu využívá [1].

Kromě obecných cloudových služeb, které umožňují uživateli téměř libovolné využití existují také poskytovatelé, kteří své služby cíleně míří na určitou oblast zaměření. Lze tak například nalézt **služby se zaměřením** na telemetrii vodáren, plynáren a energetiky, nebo také na průmyslovou automatizaci, či podnikovou dokumentaci. Jako výhoda se tak jeví, že poskytovatel vkládá více časových i finančních prostředků do správy a vývoje jeho služeb.

Nevýhody

Velkou nevýhodou se jeví **fyzické umístění dat**, a to jak po stránce právní, tak i fyzické bezpečnosti [1]. Ve chvíli, kdy data opouští stěny společnosti směrem do cloudu jsou již v nebezpečí a je tak třeba zajistit jejich bezpečnost nejen po dobu průchodu sítí, ale také po dobu setrvání dat v cloudu. Více se této problematice budu věnovat v kapitole 2.1.5.

Pokud se společnost rozhodne svěřit svá data do rukou poskytovatele, měla by při jeho výběru zvážit spolehlivost v ochraně před ztrátou a odcizením dat. Poskytovatel většinou řeší ochranu před ztrátou **duplikací dat** do více nezávislých, geologicky různě situovaných datových center, ale nelze počítat se stoprocentní dostupností dat a jejich neztrátovostí, proto lze využít například kombinaci lokálního a cloudového úložiště, nebo vícero cloudových úložišť.

Další nevýhodou je **čas**, který musí uživatel/uživatelé strávit, aby se naučil/naučili novou platformu, službu či aplikaci ovládat. V případě firem s více zaměstnanci je tak na zvážení, jestli se přechod z řešení, které aktuálně využívají, vyplatí. Tomuto rozhodnutí by však měla předcházet důkladná SWOT (Strengths, Weaknesses, Opportunities, Threats) analýza, tj. definice silných a slabých stránek, příležitostí a hrozeb, a analýza nákladů spojených s implementací nového řešení v porovnání se stávajícím řešením.

2.1.5 Bezpečnost a rizika cloudových služeb

Kvalitní poskytovatel služeb by měl splňovat vysokou úroveň zabezpečení nejen pro data, ale také pro komunikaci se servery. Data, která nejsou šifrována mohou být při přenosu jednoduše odposlechnuta, a proto se běžně využívá **šifrování a dešifrování** na straně zákazníka [48]. Šifrovaná jsou data také na serveru

poskytovatele [1]. Tím je zabráněno, aby se k datům v případě odcizení serverů někdo bez klíče dostal.

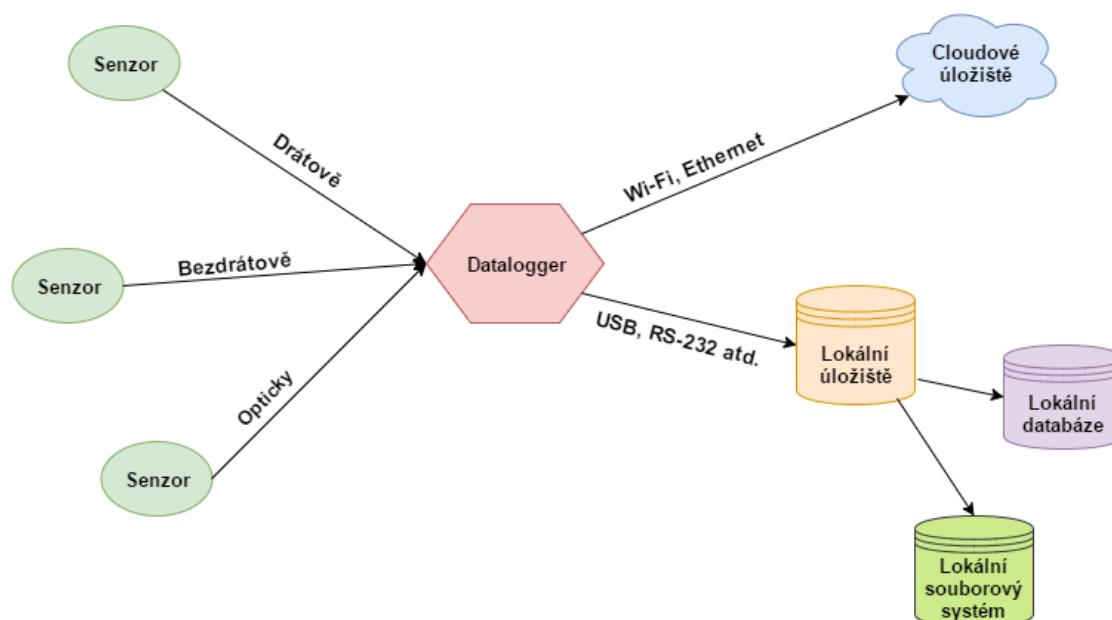
Ve chvíli, kdy jsou data fyzicky umístěna v infrastruktuře poskytovatele cloudových služeb, je poskytovatel povinen zajistit určitou bezpečnost pro data, a to jak po straně hardwaru, tak i softwaru. Mezi **fyzickou bezpečnost** patří např. zabezpečení zázemí pro hardware a zamezení neoprávněné manipulace s ním pomocí přístupových systémů s funkcí autentizace a autorizace [1]. Dále je nutné zajistit záložní zdroj energie v podobě UPS nebo generátorů pro případ výpadků elektřiny a také zajistit stabilní a rychlostně dostačující internetové připojení.

Na úrovni softwaru je pak důležité ze strany poskytovatele zajistit silný firewall, antivirovou a antispamovou ochranu, a především ochranu proti útokům hackerů [1]. Důležitou roli v bezpečnosti hraje také přístup společnosti k dané službě. **Důsledné dbání na přiřazené úrovně oprávnění** jednotlivým uživatelům tak nejednou pomůže předejít situacím při kterých se zaměstnanec dostane k datům, ke kterým nemá oprávnění, nebo se k nim naopak v případě potřeby nedostane [1].

Při výběru poskytovatele cloudových služeb by měla společnost nejprve **zvážit citlivost dat**, které bude do cloudu vkládat. Některá data (např. osobní údaje, autorská práva, výrobní tajemství) mohou dle firemní, státní nebo jiné politiky podléhat určitému požadavku na zabezpečení a fyzického umístění dat, se kterými je třeba počítat [1]. Minimum poskytovatelů umožňuje výběr města, ve kterém budou data uložena. Spíše se lze setkat s lokací na úrovni světadílů, někteří dokonce výběr umístění neumožňují. Např. pro orgány veřejné moci, které by měly mít nad daty (osobní údaje, přísně tajné dokumenty apod.) plnou kontrolu a jsou zodpovědní za obsah a ochranu před zneužitím, se jeví využití cloudové služby jako příliš riskantní [49]. Autoři knihy Smejkal a Rais uvádí, že: *“V případě informačních systémů veřejné správy je možné připustit použití externího cloudu pouze na území České republiky a i v tomto případě po důkladné analýze rizik vzhledem k agendám, které by měly být takto zpracovány.”* [49].

3 Senzorová síť

Senzorovou síť lze charakterizovat jako několik autonomních, prostorově rozmístěných a komunikace schopných senzorů, které měří určitou fyzikální (délka, hmotnost, čas atd.), nebo technickou (tvrdost, spotřeba atd.) veličinu. Tyto naměřené údaje jsou senzory schopné vhodně upravit na signál, který lze přenášet do zařízení určených ke sběru, případně i vyhodnocení naměřených dat, tzv. dataloggerů. V dataloggeru jsou data dočasně uložena a dále mohou být přenesena například do lokálního úložiště, nebo cloudové služby. Dnes nachází senzorové sítě uplatnění v mnoha oblastech od průmyslu, přes chytré domácnosti až po ochranu životního prostředí.



Obr. 3.1 Architektura senzorové sítě.

3.1 Senzory

Hlavním prvkem v architektuře senzorové sítě jsou již výše zmíněné senzory. Detailněji lze říct, že se jedná o zařízení pro přeměnu měřené veličiny na veličinu snáze měřitelnou (napětí). Stav měřené veličiny snímá část senzoru obvykle označovaná jako čidlo a dále se informace zpracovává ve vyhodnocovacím obvodu senzoru. Důležitou částí je také část výstupní, která slouží ke komunikaci s okolím, tedy k přenosu získané informace do sběrného zařízení (dataloggeru) [16].

Senzory lze dělit podle [16]:

- Typu měřené veličiny (teplota, tlak, průtok apod.)
- Fyzikálního principu činnosti (odporové, indukční, magnetické apod.)
- Aktivní (vyžaduje externí napájení) a pasivní (bez externího napájení)
- Styku senzorů s měřeným prostředím (dotykové, bezdotykové)
- Tvaru výstupní veličiny na spojitě (analogové) a nespojitě (diskrétní)

Dále lze senzory dělit podle typu připojení a komunikace v sensorové síti, které může být drátové, bezdrátové nebo optické, a také se mohou dělit podle oblasti využití, např. průmyslové. V této práci se zaměřím především na rozdělení senzorů podle typu připojení a uvedu příklady některých typických senzorů.

Aby byla komunikace možná, má každý senzor definované vhodné rozhraní, které zajišťuje spojení, správnou komunikaci a přenos dat mezi zařízeními s přesně definovanými charakteristikami propojení fyzického, signálového, funkčního i procedurálního [24]. Mezi nejznámější standardy patří například RS-232, IEEE 802.11 (Wi-Fi) a IEEE 802.3 (Ethernet).

Mezi běžně využívané komunikační technologie patří např. Wi-Fi, Ethernet, Bluetooth. Tyto technologie jsou zodpovědné za fyzický přenos dat mezi zařízeními, avšak nijak nespécifikují, co data znamenají a jak s nimi zacházet. Toto obstarávají protokoly, které spadají pod vyšší vrstvy ISO/OSI modelu [25]. Pro Wi-Fi jsou to protokoly jako HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), DNS (Domain Name System), SNMP (Simple Network Management Protocol), nebo v průmyslu užívané protokoly Modbus-TCP a ProfiNet [25]. Nejnovějším přírůstkem jsou stále vyvíjené protokoly pro IoT. Mezi nejznámější se řadí poslední dobou často skloňovaný MQTT (Message Queue Telemetry Transport) protokol, dále pak CoAP (Constrained Application Protocol), XMPP (Extensible Messaging and Presence Protocol) a WebSocket [25]. Každý ze zmíněných komunikačních protokolů se hodí k jiné aplikaci, především se však liší ve způsobu komunikace (klient/server, point-to-point) a množstvím přenesených dat [25].

Vrstva	Funkce	Příklady protokolů
7. Aplikační	síťový proces aplikací	HTTP, SFTP, SSH
6. Prezentací	prezentace dat a šifrování	XML, JSON
5. Relační	komunikace mezi hostitely	NetBIOS, PPTP
4. Transportní	End-to-End spojení a spolehlivost	TCP, UDP
3. Síťová	Určování cesty a IP (logické adresování)	IP adresa
2. Spojová	MAC a LLC (Fyzické adresování)	MAC adresa
1. Fyzická	Médium, signál, binární přenos	Ethernet, Bluetooth, Wi-Fi

Obr. 3.2 ISO/OSI model.

S velkým rozmachem IoT v posledních letech se trh zaplavil především malými levnými senzory, které jsou nabízeny doslova za pár korun a poskytují tak jednoduchá a laciná řešení. Tyto senzory je možné zakoupit jako jednoduché drátové senzory nebo jako hotová bezdrátová řešení připravená k bezdrátové komunikaci.

3.1.1 Drátové senzory

Za drátové senzory se označují senzory, které ke komunikaci jako fyzické spojení využívají propojení mezi senzorem a dataloggerem kabelem. Každý takto označovaný senzor v sobě zahrnuje formu hardwaru navrženou tak, aby bylo možné odesílání elektrických signálů z jednoho zařízení do druhého [22]. Obvykle se u senzorů očekává jednosměrná komunikace směrem od senzoru do dataloggeru, ale výjimkou není ani obousměrná komunikace. Senzory mohou mít libovolný počet vodičů podle potřeby, ale nejčastěji se lze setkat se dvěma, nebo čtyřmi vodiči [23]. Z hlediska energie jsou drátové senzory neustále napájeny ze zdroje energie, jejich životnost tak není omezena výdrží baterie.

Jako rozhraní pro přenos dat se u drátových senzorů se nejčastěji vyskytuje sériové rozhraní (sériový přenos dat) a to RS-232, nebo jeho modifikace RS-422 a RS-485. Dalším, hojně využívaným sériovým rozhraním je Ethernet, který oproti zmíněným může dosahovat mnohonásobně vyšších přenosových rychlostí [24].

Z hlediska oblasti využití lze také přibližně rozdělit využívané komunikační protokoly na aplikační vrstvě. Pro průmyslovou komunikaci je nejvyužívanější Modbus-RTU (přes RS-232 a RS-485), nebo Modbus-TCP (přes ethernet) [27]. Senzory v oblasti IoT bývají často navrhované přímo pro určitou platformu, na které

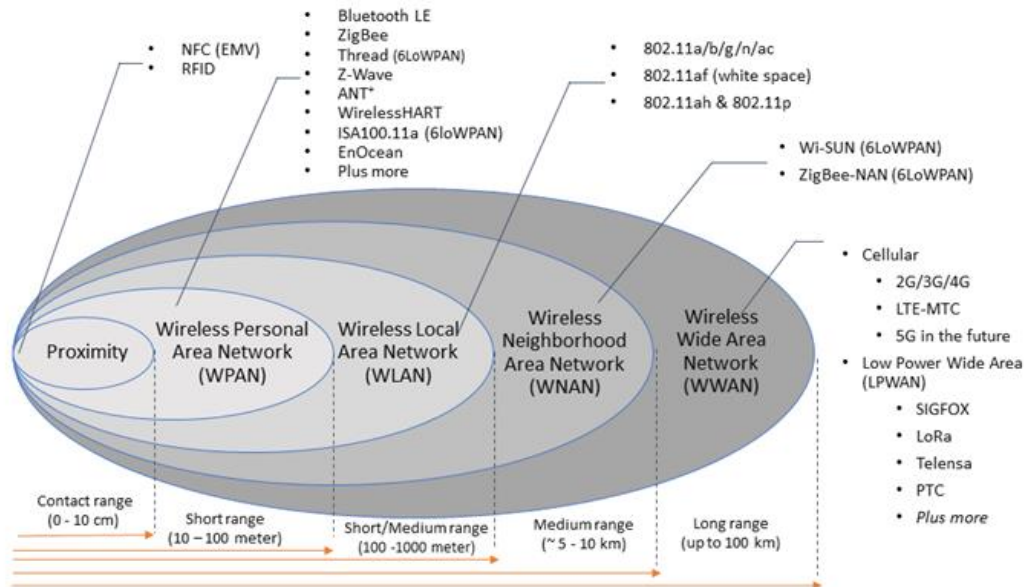
se definuje, co přijímaný signál označuje. Příkladem mohou být různé embedded platformy jako je Arduino, Raspberry Pi a další.

3.1.2 Bezdrátové senzory

Ve spojení se sensorovou sítí se nejčastěji skloňuje výraz „bezdrátová sensorová síť“. Tyto senzory lze rozdělit na dva typy podle principu činnosti. Prvním typem je senzor, který je schopen změřit veličinu a zároveň obsahuje komunikační jednotku s mikroprocesorem, pamětí a baterií, tedy jde o jednu součástku schopnou informaci získat a bezdrátově jí přenést dál do dataloggeru (nebo do úložiště v případě, že senzor vykonává funkce dataloggeru). Druhým typem je spojení dvou součástí, samotného senzoru a jednotky s mikroprocesorem, pamětí a baterií, která je schopna napájet sebe i senzor, přijímat od senzoru data (případně od více sensorů) a bezdrátově je přenést do dataloggeru. Jako v případě drátových sensorů i u bezdrátových lze komunikovat jedním, nebo oběma směry.

Hardware těchto sensorů je omezen především faktem, že je napájen pouze baterií s omezenou kapacitou. Při výrobě se tak klade důraz na hardwarové řešení s co nejmenší spotřebou energie. V dnešní době není neobvyklé, aby senzor na jedno nabití baterie vydržel 3 až 5 let v závislosti na jeho schopnosti aktivně využívat stand-by režim (úsporný režim, kdy senzor využívá minimum energie). Průměrnou spotřebu nelze jednoznačně určit, záleží na každém zařízení, ale obecně lze říct, že se jedná o desítky miliampér (v režimu vysílání) až desítky nanoampér (úsporný režim).

Komunikace v bezdrátových sensorových sítích probíhá na principu šíření radiových vln o určité frekvenci. Seznam dostupných komunikačních technologií je u bezdrátových sensorů poměrně rozsáhlý. Jednotlivé technologie lze rozdělit do skupin například podle radiového dosahu, nebo také podle energetické spotřeby. Mezi běžně užívané se řadí například Wi-Fi, Bluetooth nebo GSM, ale ty nejsou při snaze o nízkou energetickou náročnost vhodné, a proto vznikly technologie založené na nízké spotřebě. Patří mezi ně například LoRa (Long Range), Sigfox, Low Powered Wi-Fi, Zigbee, IQRF či BLE (Bluetooth Low Energy) [25].



Obr. 3.3 Volba komunikačního systému podle potřebného přenosového dosahu, převzato z [25].

Mnoho je také komunikačních protokolů na aplikační vrstvě, které se výrazně rozvíjejí společně s rozvojem sítí s nízkou spotřebou. Mezi již zmíněnými v kapitole 3.1 je třeba vyzdvihnout protokol MQTT. Jedná se o jednoduchý protokol, který je určený pro zařízení s malým výpočetním výkonem [46]. Jednou ze dvou důležitých vlastností je funkce: Publish a Subscribe/UnSubscribe. Pomocí této funkce je možné v síti zveřejňovat informace, které jsou centralizovaným bodem zpracované a přeposlané klientům, kteří tuto zprávu odebírají [46]. Druhou důležitou vlastností je, že MQTT zprávy jsou rozdělené do jednotlivých témat. Každá zpráva může patřit do některého z témat a hierarchie témat se odděluje lomítky. Výsledná podoba hierarchie může být například: `byt_01/pokoj_02/osvetleni_05` [46].

Dnes jsou bezdrátové senzorové sítě nepostradatelnou součástí každodenního života. Uplatnění nachází například ve sféře:

- Obchodní (sledování stavu zásob)
- Průmyslové (sledování provozu, výroby, stavu techniky)
- Životního prostředí (tlak, teplota, výška hladiny řek, sledování zvěře)
- Zdravotní (stav pacientů, sledování zařízení pracujících v těle)
- Armádní (sledování nepřátel, sledování vlastních zařízení)
- Chytrých domácností (ovládání topení, žaluzií, osvětlení)

3.1.3 Optické senzory

Jako optický senzor může být označován senzor, který využívá optické vlákno jako snímací prvek k měření veličiny, jako médium pro přenos signálu, nebo jako kombinaci obou zmíněných [29]. Oproti předešlým zmíněným způsobům přenosu signálu se optické vlákno liší především tím, že může dosahovat výrazně vyšších přenosových rychlostí oproti bezdrátovému přenosu, či přenosu po metalickém vedení a informace se v něm šíří buď pomocí úplného odrazu světla na rozhraní (dvě prostředí s rozdílným indexem lomu) optického vlákna nebo díky ohybu světla (gradientní vlákna) [50]. Optická vlákna často nahrazují kovové vodiče, jelikož jsou odolné vůči elektromagnetickému rušení a vykazují při přenosu na větší vzdálenosti výrazně menší ztráty [29].

Optické senzory lze kromě výše zmíněných skupin rozdělit také podle prostorového uspořádání na [40]:

- Bodové senzory
- Rozprostřené senzory
- Polo-rozprostřené senzory

Lze je také rozdělit podle měřené veličiny na [40]:

- Senzory fyzikálních veličin
 - Teplota
 - Tlak
 - Posuv
 - Vibrace
 - Proud
- Chemické a biochemické senzory
 - pH
 - Parciální tlak kyslíku

Optické senzory lze dnes najít v mnoha oblastech využití. Jsou to např. bodové senzory teploty, distribuované akustické senzory nebo také běžně užívané senzory pro měření vzdálenosti objektů. Lze s nimi měřit např. také vzdálenost objektů ve vakuu, kde funkčnost ultrazvukových senzorů selhává. Dnešní optické senzory zvládají detekovat i opticky transparentní (průhledné) objekty [51].

Rozdíl mezi senzory s optickým vláknem jako snímacím prvkem a jako médiiem pro přenos signálu je také v jejich spojení s dataloggerem. V prvním případě bývá běžné, že v sobě sensor kloubí jak měřicí, tak vyhodnocovací mechaniku. Optickým detektorem bývá nejčastěji fotodioda, která využívá fotoelektrický jev k přeměně energie světelného signálu na elektrickou energii [40]. Komunikace s dataloggerem tak probíhá pomocí elektrického signálu. Mezi běžně využívané komunikační standardy patří např. RS-232, RS485. Do této kategorie patří také senzory, které svou činností mění světelnou energii na elektrickou (opto-elektrické) [72]. Tyto senzory jsou sami o sobě převodníky a nepotřebují žádný další externí převodník. Díky tomu lze tyto senzory připojit přímo na piny dataloggeru. V dataloggeru lze definovat, jaká součástka je na jakém pinu a díky tomu může být popsána získaná informace, kterou přijaté hodnoty napětí představují. Patří mezi ně např. infračervený sensor, fotodioda, fotorezistor a další [72].

V druhém případě se nechává zpracování optického signálu na vyhodnocovací jednotce, která signály z více sensorů sdruží, vyhodnotí a v podobě elektrického signálu předá dataloggeru. Jako komunikační standardy se i zde využívají RS-232, RS485 přes protokol MODBUS, popř. DPN 3.0, či přes Ethernet protokolem TCP/IP [40]. I samotné vlákno může být sensor, např. pro měření vibrací, tlaku a dalších veličin. Lze k tomu využít např. metodu založenou na prchání světla nebo mikro ohybu [54].

Každá optická síť by měla splňovat tři charakteristické vlastnosti. První je **multiplexování (sdružování) a demultiplexování (rozdělování)**. Tyto vlastnosti umožňují jednotlivé signály ze sensorů kombinovat do jednoho signálu vhodného k přenosu po přenosovém médiu a opětovné rozdělení na jednotlivé signály [29]. Další vlastností je **schopnost neustálé činnosti** i v případě, kdy některý ze sensorů přestane fungovat. Činnost sítě i v případě nečinnosti některých bodů v síti je velmi důležitá nejen z hlediska komunikace (telefonní síť, internetová síť), ale také bezpečnosti osob (mosty, přehrady, elektrárny) a financí (únik ropy, vody, plynu) [29]. Poslední vlastností je schopnost komunikace se senzory na velikou vzdálenost [29].

Optická spojení se běžně využívají v místech, která jsou zatížena elektromagnetickým rušením. Mezi ně patří například automatické svařovací systémy, měniče frekvence, nebo motory [29]. Hlavní myšlenou optických sensorových sítí je ale především to, aby bylo možné sbírat hodnoty ze sensorů na vzdálenosti v řádech desítek až stovek kilometrů bez potřeby elektrického napájení mezi senzorem a dataloggerem. Sensorové sítě, respektive samotná optická vlákna také vykazují skvělou funkčnost v oblasti detekce poruch na různých vedeních jako jsou

telekomunikační sítě, vodní potrubí a jiné sítě, které mohou být dlouhé i tisíce kilometrů [29].

3.2 Dataloggery

Jako datalogger je označováno elektrické zařízení, které zpracovává data z interních (vlastních), nebo externích (v našem případě ze sensorové sítě) senzorů a dále je předává k uložení na vhodné médium [74]. Hlavním úkolem dataloggeru je tak vykonávat prostředníka mezi sensorovou sítí a úložištěm. Po hardwarové stránce se skládá z mikroprocesoru, který data přijímá a podle přesných instrukcí je zpracovává, dále pak interní paměti, která slouží jako přechodné, nebo stálé datové úložiště a také z napájecího a komunikačního konektoru. Do základní výbavy patří také velké množství digitálních a analogových konektorů, které slouží k připojení jednotlivých senzorů, ale tento fakt je silně závislý na výběru přenosového média a účelu využití dataloggeru.

Jednotlivé dataloggery můžeme rozdělit do skupin podle:

- Účelnosti (jednoúčelové, víceúčelové)
- Způsobu využití (jako prostředník, jako samostatné zařízení s vestavěným úložištěm)

3.2.1 Jednoúčelové

Tyto dataloggery, jak již název napovídá, jsou určené k vykonávání pouze jednoho účelu, například snímání určité veličiny nebo obecně pouze snímání. Hardware i software je zaměřen především k tomuto účelu a od toho se také odvíjí jejich nižší cena a menší rozměry v porovnání s víceúčelovými. Hardware bývá zpravidla doplněn pouze o konektory potřebné ke snímání veličiny, nebo se může jednat přímo o kombinaci senzoru a dataloggeru v jednom zařízení. Na trhu se nejvíce vyskytují v hardwarové verzi přizpůsobené k využívání jako prostředník, ale mohou se vyskytovat i jako samostatná zařízení s úložištěm.

Praktické využití nachází především v sítích, ve kterých dochází k měření jedné určité veličiny (napětí, proud, teplota, úhel apod.).

3.2.2 Víceúčelové

S rozvojem IoT se nejvíce ukázal potenciál víceúčelových dataloggerů, mezi které se řadí především samostatná zařízení s úložištěm. Od jednoúčelových se liší především ve schopnosti obstarávat více různých senzorů a vykonávat více různorodých procesů. Většina těchto dataloggerů je dodávána se softwarem, který umožňuje přizpůsobit jednotlivé procesy potřebám sítě, a některé dokonce umožňují instalaci jednoduchého operačního systému, především typu UNIX. Z hlediska hardwaru se datalogger rozšířil o komponenty schopné dosahovat potřebného výkonu a o více univerzálních vstupních a výstupních konektorů pro připojení více různých senzorů. To má za následek zvětšení rozměrů, a především navýšení ceny.

Nejčastěji se lze setkat s aplikací v IoT, kde se senzorové síť běžně skládají z různých senzorů a celé řešení se může omezit pouze na síť senzorů a datalogger, který může zastat funkci prostředníka a úložiště v jednom. Výjimkou není ani využití v oblasti průmyslu (zásobování, správa výrobní linky) a chytrých domácností (ovládání topení, žaluzií, světel).

Příkladem víceúčelových dataloggerů jsou průmyslové IP dataloggery, nebo dataloggery založené na embedded platformách jako je Arduino, Raspberry Pi, BeagleBone a další.

3.3 Úložiště dat

Po získání signálů ze senzorů a jejich převedení na dobře čitelná data v dataloggeru se musí získané informace uložit a především zužitkovat. Obecně se preferují tři možnosti uložení dat:

- Lokální úložiště dat
 - Lokální souborový systém (textový soubor, soubor aplikace Excel)
 - Lokální databáze (MySQL, MongoDB atd.)
- Cloudová služba (Microsoft Azure, Google Cloud Platform atd.)

Nelze jednoznačně určit, které řešení je lepší, protože každá firma může mít dle své firemní politiky různé preference na finanční nákladovost, umístění dat a jejich bezpečnost. O cloudové službě jako uložišti dat pojednává kapitola 2.1 Cloudové služby.

3.3.1 Lokální souborový systém

Prvním a na zavedení nejjednodušším úložištěm je lokální systém, respektive úložiště na lokální platformě (PC, notebook a jiné). Většina dataloggerů je dnes schopna zapisovat data alespoň do standardního textového souboru, který je čitelný pro většinu běžně užívaných operačních systémů jako je Windows, Mac OS, nebo Linux.

Vzhledem k tomu, že samotný textový soubor nedisponuje žádnou možností grafické, či jiné analýzy dat, je třeba zajistit navíc analyzátor, aby data nezůstávala jen v syrové podobě. Jako vhodné řešení se jeví balíček MS Office od společnosti Microsoft, především produkt „Microsoft Excel“, který dokáže zpracovávat syrová data z textového souboru a vytvořit z nich tabulky a grafy.

3.3.2 Lokální databáze

Ukládání v lokální databázi se od řešení v lokálním systému liší především možností vzdáleného přístupu k datům, které jsou stále ve vlastnictví společnosti. Databáze nemusí být nutně jako online řešení, ale jeví se jako vhodný způsob pro vzdálený přístup k datům.

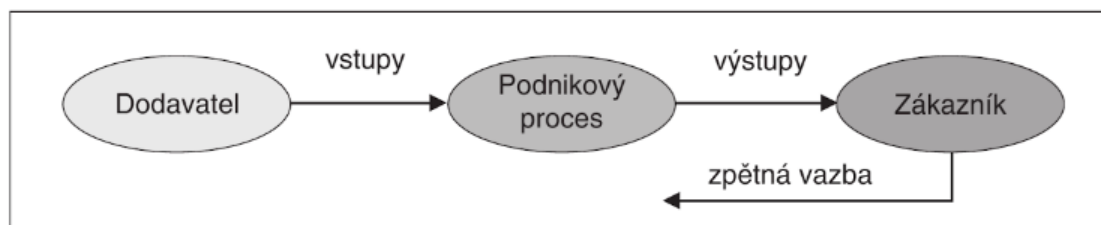
Jako příklad se hodí velmi oblíbený systém databází MySQL. Laicky řečeno se jedná o systém na bázi tabulek a buněk, ve kterých patří jedné buňce jedna změřená hodnota senzoru. Datalogger má přesně definováno, do jakých buněk má jaké hodnoty ukládat, a tím je zajištěna přehlednost a další zpracovatelnost dat. Takto data stále nejsou dobře čitelná, a proto se vytváří tzv. analytické prostředí, které je grafickým spravováním dat z tabulek a uživatel k němu přistupuje vzdáleně pomocí webového prohlížeče nebo jiné vhodné aplikace.

Z pohledu bezpečnosti hrozí riziko neoprávněného vstupu do systémů zvenčí (slabé heslo, chyba v aplikaci) a odposlechnutí dat při jejich přenosu (slabé, nebo nulové šifrování). Přesto je tento způsob ukládání a analyzování dat velmi využívaný, především pro možnost vzdáleného sledování stavu senzorové sítě a také pro velké objemy dat, které lze oproti ukládání v lokálním systému (textovém souboru, aplikaci Excel) výrazně rychleji analyzovat.

4. Procesy technologické firmy

Jelikož je téma „procesy technologické firmy“ poměrně rozsáhlé a jeho popsání by mohlo dát i na několik bakalářských či diplomových prací, pokusím se v této kapitole alespoň nastínit problematiku tohoto tématu. Především se zaměřím na plánování podnikových procesů, jelikož je to téma, které by mělo být v každé firmě co nejlépe zvládnuté, a také na správu podnikové dokumentace, která má často u technologických firem výrazně přísnější pravidla z důvodů jako jsou výrobní tajemství, postupy a jiné.

Jako příklad podnikového procesu může být objednávka na výrobu zboží, kterou firma přijme a zhotoví. V tomto případě se procesem rozumí postup vyřízení požadavku zákazníka, který začíná přijetím objednávky a končí předáním zboží zákazníkovi [30]. Jednotlivými kroky procesu jsou ty, které musí personál i zákazník vykonat, aby mohla být celá objednávka zhotovena a předána. Zjednodušeně tak lze říct, že: „*Podnikový proces je souhrnem činností, transformujících souhrn vstupů do souhrnu výstupů (zboží nebo služeb) pro jiné lidi nebo procesy, používající k tomu lidi a nástroje.*“ [30].



Obr. 4.1 Základní schéma podnikového procesu, převzato z [30].

Pro efektivitu podnikových procesů by se měly firmy řídit třemi základními oblastmi principu řízení. První oblastí je **znalost procesů**. Znalostí procesů se myslí, že si je firma vědoma svých procesů, jejich vstupů a výstupů. Také má přehled, jakým způsobem se vstupy mění na výstupy a jaké materiální i finanční prostředky se na to spotřebovaly [31]. Další oblastí je **ověřování činností pro přeměnu vstupů na výstupy**. Touto oblastí jsou charakterizovány principy, které vedou k výstupní charakteristice výkonosti přeměny vstupů na výstup. V podstatě to znamená, že všichni pracovníci jsou si vědomi své úlohy při přeměně vstupů na výstupy a také, že procesy jsou popsány a parametrizovány tak, aby bylo možné výstupní charakteristiku získat [31]. Poslední oblastí je **monitorování a zlepšování procesů**. Důležité je procesy neustále zlepšovat. K tomuto účelu je využívána výkonnost

charakteristika, na jejímž základě se měří účinnost procesů. Vzniká tak prostor pro nacházení a následné zlepšování slabých míst [31].

Procesní řízení se z hlediska procesů rozděluje na tři kategorie, které jsou vzájemně propojené a jejich správná činnost přispívá ke kvalitě služeb poskytovaných firmou. **Hlavní procesy** jsou takové procesy, které vytváří hodnotu (služba, výrobek) pro zákazníka [32]. Jsou účelem každé organizace a jejich náplň se liší především náplní práce jednotlivých firem. Například pro technologickou firmu zajišťující cloudovou službu je náplní hlavních procesů zajišťování činnosti této služby. Další kategorií jsou **podpůrné procesy**. Hlavní náplní práce podpůrných procesů je především sloužit jako podpora hlavních procesů [32]. Náplň podpůrných procesů se může u některých firem částečně lišit v závislosti na oboru činnosti, ale vesměs se jedná o stejné činnosti. Mezi tyto procesy se řadí například účetnictví, které je podle zákona povinná vést každá firma, dále pak řízení lidských zdrojů, nebo třeba nakupování a získávání zdrojů. Třetí kategorií jsou **řídící procesy**. Tyto procesy se věnují především fungování a rozvoji firmy. Nelze je vypsát jako výčet funkcí, jelikož jde o aktivity spojené s řízením, plánováním, organizováním celé firmy [32]. Příkladem řídicích procesů může být vytváření strategie, plánování a jiné. Zavedením procesního řízení tak získává firma přehled nad jejími činnostmi a je schopna efektivně své služby monitorovat a zlepšovat a zároveň snižovat potřeby zdrojů.

4.1 Plánování podnikových zdrojů

Plánováním podnikových zdrojů, dále jen ERP (Enterprise Resource Planning) bývá označována firemní aplikace, pomocí které firma řídí většinu procesů jako jsou zásoby, výroba, prodej, finance, personalistika a jiné [33]. Tyto aplikace mohou být do firmy nasazené ve třech variantách. První variantou je **lokální nasazení** („On-premises“), kdy se veškeré aplikace od poskytovatele ERP služeb instalují přímo do lokálního centra firmy. Další možností je **nasazení v cloudu**, kdy poskytovatel nabízí své aplikace typicky jako model nasazení SaaS. Poslední možností je **kombinací obou zmíněných**. Ta se využívá především pro procesy, které musí zůstat podle firemních pravidel v rámci „čtyř stěn“, či je kladen důraz na okamžitou odezvu požadavku a zároveň lze některé procesy přenechávat na zpracování cloudové službě.

4.1.1 Funkce ERP systémů

Předností ERP oproti původním integrovaným systémům je především schopnost sjednocení jednotlivých odvětví řízení společnosti do jednoho přehledného, dobře říditelného systému. Dnešní ERP systémy by měly pokrývat čtyři hlavní oblasti činnosti, jimiž jsou [33]:

- Výroba a logistika (plánování zdrojů, nákup, skladování a řízení zásob, plánování výroby)
- Finance (nákladové účetnictví, finanční účetnictví, závazky a pohledávky, dlouhodobý majetek)
- Personalistika (evidence zaměstnanců, mzdy, evidence odpracovaných hodin, hodnocení zaměstnanců)
- Obchod a marketing (plánování prodeje, řízení prodeje, zpracování zakázek)

Jednotlivé nabízené služby se liší podle poskytovatele. Tento seznam, a především výčet funkcí lze brát pouze z obecného hlediska, jaké pokrytí procesů je očekávané od firemních ERP systémů.

4.1.2 Charakteristiky firemního ERP systémů typu cloud

Termín ERP systém typu cloud není jednoznačně definovaný, proto je těžké určit, jestli je nabízená služba opravdu typu cloud ve smyslu kompletního nasazení v cloudové službě. Poskyvatelé ERP systémů tak označují vše od hostování služby, „On-premises“ řešení, přes privátní a veřejné sítě typu cloud až po poskytování ERP jako SaaS [1].

Tyto systémy bývají dodávány s funkcemi pro správu systému. Je tak kladen důraz na myšlenku samostatné správy cloudových služeb s minimální interakcí s poskytovatelem. Stejně tak je kladen důraz na myšlenku měsíčních plateb, namísto jednorázových poplatků za permanentní licenci [1]. V některých případech se lze setkat i s tím, že poskyvatelé požadují jednorázový poplatek za zřízení služby a k tomu měsíční poplatky. Výše poplatků je většinou stanovena podle počtu zaměstnanců přistupujících k systému a podle druhu zvoleného balíčku služeb, vesměs se ale jedná o částky v řádu tisíců korun za měsíční poplatky a v řádu desítek až stovek tisíc korun za jednorázový poplatek.

Při výběru vhodného firemního ERP systému typu cloud je třeba přihlížet k jednotlivým charakteristikám a zvolit si takovou jejich kombinaci, která bude dané

firmě nejlépe vyhovovat. Lze se řídit osmi hlavními charakteristikami, podle kterých by se měli firmy při výběru řídit [1]:

- Škálovatelnost a elasticita
- Měření využívání služeb
- Sdílení technologie
- Licencování
- Správa aplikace
- Umístění dat
- Snadnost přechodu k jinému řešení
- Kontrola nad změnami programového vybavení (software) včetně nových verzí (upgrade)

Škálovatelnost a elasticita je důležitá především pro firmy, u kterých dochází k jednorázovým, či náhodným nárůstům zátěží. Příkladem může být firma s obsáhlou senzorovou sítí (vodoměry, plynoměry). Tato firma bude uskutečňovat sběr dat a s tím spojený zápis do systému v jeden den v měsíci, a tím výrazně navýší spotřebovaný výkon oproti jiným dnům. V takovém případě je důležité zvolit takové řešení, které poskytuje možnost dynamické změny výkonu [1]. S potřebou elasticity služby je spojena především **měřitelnost využívaných služeb**. Klasický způsob licencování firem se nejčastěji objevuje ve formě platby za jednotlivé uživatele. Tento způsob se hodí především pro firmy, které mají stabilní předvídatelnou využívanost služeb, ale pro firmy s potřebou zvýšené elasticity se jeví jako výhodnější řešení platba za služby, které v daném období využívá [1].

Jako „**Sdílení technologie**“ může být označováno nejen sdílení jednoho hardwarového zařízení poskytovatele více firmami, ale také sdílení aplikační logiky systému (software je dodáván pro všechny firmy stejný). Porucha jednoho hardwaru poskytovatele může negativně ovlivnit nejednu firmu. Sdílení aplikační logiky systémů mnohdy usnadňuje rychlé aktualizace ze strany poskytovatele, ale nese s sebou také limity na individuální úpravu systému dle požadavků firmy [1]. **Licencování** může být nákladná záležitost, především pro začínající firmy. Každá firma by si měla před přechodem na řešení ERP typu cloud vypracovat statistiku, jestli se daný systém vyplatí licencovat v podobě jednorázového poplatků, nebo průběžných měsíčních/ročních poplatků [1].

Možnosti správy jsou silně závislé na zvoleném typu ERP řešení. V případě řešení typu SaaS je veškerá správa (zajištění infrastruktury, chod a aktualizace systému) ponechána poskytovateli služby. Naopak u řešení typu „On-premises“

veškerou správu zajišťuje firma. Při výběru vhodného systému je tak důležité si s poskytovatelem předem stanovit podmínky správy [1]. Jak již bylo řečeno dříve, některé firmy, především ty působící v silně regulovaném odvětví mohou mít specifické požadavky na **umístění dat**. Pro řešení typu SaaS je typické, že uživatel neví, kde jsou jeho data umístěna. Poskytovatel často s daty manipuluje a přemísťuje je podle potřeb vytížení jednotlivých bodů infrastruktury. Důležité je si s poskytovatelem předem ujasnit jaké má firma možnosti volby umístění dat [1].

U **přechodu k jinému řešení** je rozhodující důkladná SWOT a nákladová analýza pro stávající řešení, cloudové a „On-premises“ řešení. Tento proces bývá velmi komplikovaný a nejvíce komplikované se jeví řešení typu SaaS, a to především v případě komplikovaného stávajícího procesu. Pokud však v malém podniku je současné řešení založené na manuální činnosti, např. hlídání doby konkrétního procesu pomocí budíku/stopek, je přechod k jinému řešení méně náročný. Jelikož je správce služeb poskytovatel, vše v případě neošetření přechodu smlouvou záleží na jeho ochotě [1]. Poslední charakteristikou je **kontrola nad změnami (upgrade systému)**. V případě řešení typu „On-premises“ má plnou kontrolu nad novými aktualizacemi firma, která se může předem na update celého systému řádně připravit, aby se vyhnula co nejvíce chybám spojených s upgradem. Naopak u řešení typu SaaS má kontrolu nad správou aktualizací poskytovatel. V některých případech to může vést k problémům, které s sebou nesou přechody na nové verze systému a je třeba s nimi předem počítat [1].

Mezi dnešní největší poskytovatele ERP služeb patří například společnost Microsoft s více jak 83 000 zákazníky, za nimi je společnost Infor s více než 70 000 zákazníky a dále pak společnosti SAP a Oracle [35].

4.2 Správa dokumentů

Správa dokumentů a jejich uchovávání je mnohdy u firem pracujících s velkými objemy dat problémová. Při nesprávné činnosti dokumentového workflow (kam a jak má dokument putovat) tak může docházet k neúplnému zpracování dokumentů, či jejich ztrátě. Za účelem zlepšení těchto procesů vznikly tzv. DMS systémy (Document Management System – systém pro správu dokumentů).

Význam slova dokument zde neoznačuje pouze papír s informacemi, ale je tak označován i soubor v elektronické podobě bez ohledu na formát. Pod tímto označením se lze nejčastěji setkat s dokumenty spadající do kancelářského balíku MS Office jako je MS Word, Excel a podobné, ale dokument může být například i e-mail, technický postup, výkres, fax, či video [37].

Dokumenty lze rozdělit na strukturované a nestrukturované [37]. Mezi strukturované dokumenty se řadí ty, které lze jednoduše elektronicky zpracovat, např. tabulky a databáze. Opačným případem jsou dokumenty nestrukturované. Mezi ně patří typicky dokument, který dostane učení k oskenování a zpracování do systémů. Uvádí se, že až 90 % dokumentů ve firmě má nestrukturovanou podobu [37]. Především za účelem zefektivnění správy těchto 90 % dokumentů vznikly DMS systémy.

4.2.1 Funkce DMS systémů

Tyto systémy jsou určeny především k rychlému a efektivnímu zpracování velkého objemu dat a dokumentů. To přispívá k uspokojování potřeb zákazníků i firmy, a také k úsporám času a peněz [38]. Další oblastí uplatnění jsou legislativní požadavky, které na firmy kladou vyšší požadavky na uchování dat a dokumentů spojených s podnikáním. Základem pro činnost takového systému je centralizované úložiště. Nad úložištěm běží DMS systém, který spravuje přístupy jednotlivých zaměstnanců k dokumentům, dále pak zajišťuje funkcionalitu pro zpracování dokumentů a v neposlední řadě poskytuje přehledné a funkční dokumentové workflow [31].



Obr. 4.2 Workflow průchodu dokumentů firmou, převzato z [36].

Aby byla dokumentace řádně vedená a snadno dohledatelná, musí být dodržována určitá pravidla [38]:

- Jednoznačnost autora, data vzniku jednotlivých verzí a obsahu změny dokumentu

- Zachování jednotlivých verzí dokumentů, minimálně na úrovni schválených dokumentů
- Možnost připomínkování, a zejména schvalování dokumentů
- Řízení přístupových oprávnění k dokumentům v jednotlivých fázích procesu řízení dokumentace
- Potvrzení o přečtení dokumentu, notifikace o přiděleném úkolu atp.

Veškeré dokumenty tak lze zpracovat do elektronické podoby a díky těmto pravidlům je umožněno zálohování verzí dokumentů, jejich dohledatelnost, jednoznačnost a kategorizace podle daných oblastí.

4.2.2 Charakteristiky DMS systémů typu cloud

Tyto systémy mohou být stejně jako u ERP systému nasazené do firmy ve třech variantách. Jako lokální nasazení („On-premises“), hostované, nebo nasazení v cloudu. Souhrnně se však tyto varianty u poskytovatelů označují jako „cloudová řešení“. Obecně lze říct, že při výběru vhodného systému by firma měla hledět na stejné charakteristické vlastnosti jako jsou uvedené u ERP systémů (škálovatelnost, elasticita, správa aplikace, umístění dat, měření využívání služeb). Tyto systémy však mají ještě své specifické charakteristiky.

První charakteristickou vlastností je **implementace do hotových řešení**. Aby se u firem dosáhlo co největší komplexnosti užívaného systému, například typu ERP, poskytovatelé se zaměřují na možnost jednoduché implementace DMS systémů do běžně využívaných ERP systémů. **Verzování dokumentů** pomáhá udržovat přehled nad změnami v dokumentech od jejich vzniku až po konečně uzavření [38]. Dnes je tato funkce typická pro většinu dodávaných DMS systémů. **Řízení oběhu dokumentů (workflow)** je základním kamenem všech DMS systémů [38]. Workflow přesně definuje cesty, kterými musí dokument ve firmě projít. Příkladem tak může být smlouva, která má jít nejdříve přes účetní oddělení, dále k nadřízenému na podpis a znovu zpět do účetního oddělení.

Další důležitou charakteristickou je **přidělování uživatelských práv** [38]. Vhodným přidělením práv dochází k zamezení přístupu uživatelů k dokumentům, které pro ně nejsou určené a naopak. Dnešní technologie umožňují přístup k těmto systémům pomocí **webového prohlížeče** z většiny dnes běžně užívaných platform jako je stolní PC, notebook a mobilní telefon.

5. Zhodnocení cloudových služeb

Tato kapitola je zaměřená na malé podniky technologického zaměření. Podle úředního věstníku Evropské unie z roku 2014 lze **malý podnik** vymezit jako: „*Podnik, který zaměstnává méně než 50 osob a jehož roční obrat nebo bilanční suma roční rozvahy nepřesahuje 10 milionů EUR.*“ [39].

V této kapitole se zaměřím především na zhodnocení nákladovosti, spolehlivosti a bezpečnosti cloudových služeb pro malé podniky (dále jen firmy). Obecně lze charakterizovat několik vlastností cloudových služeb, díky kterým se jeví pořízení tohoto řešení v některých aspektech jako výhodné nebo nevýhodné oproti klasickému lokálnímu řešení (kompletní nákup a správa vlastního softwaru a hardwaru) tzv. řešení typu „On-premises“, kdy je služba zakoupena jen jako software a nainstalována na serveru firmy, která se pak stará o správu veškeré infrastruktury. Tyto vlastnosti jsou pouze výčtem vlastností uvedených v teoretické části.

Cloudové služby mají několik distribučních modelů viz 2.1.3. Proto budou dále v textu tyto modely (v případě, že se nepoukazuje pouze na jeden model) hromadně označovány jako „**cloudové služby**“ pro modely PaaS, IaaS a SaaS a cloudová služba na serveru zákazníka bude označována jako „**On-premises služba**“.

Pokud se firma rozhodne využít služeb cloudových poskytovatelů, měla by nejprve zvážit, který distribuční model bude pro její činnost nejvhodnější. Při rozhodování by mělo být přihlíženo k těmto aspektům:

- Finanční prostředky, které mohou být na zřízení a provoz služby uvolněny
- Stav IT oddělení (počet zaměstnanců a jejich schopnosti)
- Závislost na IT
- Stav stávající infrastruktury (rozšiřitelnost a spolehlivost vlastního hardwaru, prostory pro servery, kvalita internetového připojení)
- Integrace služby se stávajícím systémem
- Nároky na přizpůsobení služeb požadavkům firmy
- Bezpečnost dat (veřejná, tajná, přísně tajná)
- Rozsáhlost a nákladnost sensorové sítě
- Dostupnost aplikace

Každý distribuční model cloudového řešení přistupuje k těmto aspektům jinak, avšak nejvíce se liší v tom, jestli jsou nasazené v serveru poskytovatele, nebo

zákazníka. Proto budu dále porovnávat především cloudové služby a „On-premises“ služby.

5.1 Nákladovost

První z vlastností cloudových služeb je **odbourání počátečních nákladů**, které by v případě „On-premises“ služby připadly na pořízení vlastní infrastruktury (servery, chlazení, UPC, serverové skříně, software apod.). Firma tak dostává možnost investice financí do jiných oblastí své činnosti a taktéž není potřeba zaměstnávat více IT odborníků, kteří by se o lokální hardware museli starat.

Předvídatelnost nákladů je pro všechny firmy důležitým faktorem, ke kterému by měly při výběru poskytovatele přihlížet. V případě využití cloudových služeb přechází servis a správa serverů i aplikací (v závislosti na distribučním modelu viz Obr. 2.3) na poskytovatele. Z finančního hlediska tak odpadá platba za údržbu (výměna HDD a SSD, výměna chlazení, obnovování technologie, rozšiřování hardwaru) a správu (aktualizace aplikací, pravidelná kontrola správné činnosti). Díky tomu lze při tvorbě finančního plánu snížit předpokládané náklady na IT zaměstnance. Pro omezení neefektivnosti jednorázových, mnohdy extrémně drahých poplatků za celou službu začali poskytovatelé nabízet licence v podobě měsíčního poplatku. V případě sensorové sítě se převážně jedná o poplatek za připojenou jednotku a v případě systémů typu ERP, nebo DMS se převážně jedná o poplatek za uživatele služby. Z hlediska rozpočtu tak lze téměř přesně definovat jaké budou počáteční i průběžné náklady.

Oproti „On-premises“ službě mají cloudové služby jednoznačnou výhodu ve **škálovatelnosti služeb**. V případě, že je potřeba navýšit, nebo snížit výpočetní výkon služby, mají poskytovatelé definované ceny za tyto změny. Ty bývají účtovány hodinově v případě jednorázového navýšení, nebo měsíčně v případě dlouhodobé změny. Ceny za taková navýšení bývají mnohonásobně nižší než v případě přikoupení dodatečných serverů. Lze tak efektivně ušetřit náklady za provoz služby.

5.1.1 Ze sensorové sítě

Prioritou je snížení nákladů, především počátečních, ale také průběžných. Při rozhodování, který z těchto služeb je při žirování nákladnější lze vycházet z charakteristiky uvedené v kapitole 5.1.

Při porovnání dvou zmíněných služeb vychází na první pohled jako jasný vítěz cloudová služba, avšak nemusí být nutně nejvýhodnější za delší časové období.

Např. společnost Microsoft nabízí svou „On-premises“ službu nesoucí název „Microsoft Azure Stack“, dále jen „MAS“, která nabízí stejné možnosti jako cloudová služba Microsoft Azure. Za využití MAS si Microsoft neúčtuje žádné jednorázové licenční poplatky, a navíc finančně zohledňuje umístění služby v infrastruktuře firmy. Stejně jako u „Microsoft Azure“ se platí za to, co firma skutečně využije a z toho důvodu může být pořízení vlastní infrastruktury z dlouhodobého hlediska výhodnější.

V Tab. 5.1 lze nalézt cenové relace některých poskytovatelů, kteří poskytují své řešení jako „On-premises“ službu [63].

Tab. 5.1 Poplatky za zřízení „On-premises“ služby.

Název	Ceny
Microsoft Azure Stack	Žádný jednorázový licenční poplatek. Stejná cenová hladina měsíčních poplatků jako u služby „Microsoft Azure“ (platba za to, co se využívá)
Oracle Cloud Machine	Žádný jednorázový licenční poplatek. Průběžný měsíční poplatek: 21 600\$/měsíc

Ve spojení se senzorovou sítí se objevují tzv. **IoT cloudy**. Tyto cloudy jsou nejčastěji nabízeny jako distribuční modely **SaaS**, nebo **PaaS**. Ze senzorové sítě jsou data zasílána do cloudových uložišť (viz kapitola 3) a zde mohou být buď uschována, nebo zpracována. Z finančního hlediska se jedná o pravidelné náklady, které jsou vynakládány za získaná data.

Vesměs si poskytovatelé účtují za počet přenesených zpráv na fyzickou jednotku (např. senzor), či za fyzické místo pro data v cloudu. Před výběrem vhodné služby by tak měla firma kromě jednorázových nákladů zvážit také náklady pravidelné. Tyto náklady si lze odvodit z odhadu počtu používaných senzorů a četnosti jejich komunikace. V Tab. 5.2 lze nalézt příklad účtovaných financí jednotlivých poskytovatelů. Tyto částky jsou uvedené na webu poskytovatele pro využití služeb typu cloud, jejich platnost pro službu jako „On-premises“ nelze zaručit. Více informací o jednotlivých poskytovatelích cloudových služeb pro senzorové sítě lze najít v Tab. 7, 8, 9 a 10.

Tab. 5.2 Ceny za IoT cloudové služby.

Název	Ceny
Microsoft Azure	Free: zdarma/měsíc, max. 8000 zpráv/den/jednotka S1: 50\$/jednotka/měsíc, max. 400 000 zpráv/den/jednotka S2: 500\$/jednotka/měsíc, max. 6 000 000 zpráv/den/jednotka S3: 5000\$/jednotka/měsíc, max. 300 000 000 zpráv/den/jednotka
Oracle cloud	210Kč/hodina výpočetního výkonu cloudové služby
Amazon Web Services	Ceny za počet přenesených zpráv (Evropa): 5\$/1 000 000 zpráv

V Tab. 5.3 lze najít přehledné finanční zhodnocení jednotlivých modelů nasazení, a to jak z pohledu jednorázových nákladů (zřízení služby, přechod na službu), tak i z pohledu pravidelných nákladů.

Tab. 5.3 Finanční zhodnocení z pohledu jednorázových a pravidelných nákladů.

	Náklady za služby	IaaS, PaaS, SaaS	On-Premises
Jednorázové náklady	Licence na software poskytovatele	Ne	Ano
	Licence na OS	Ne	Ano
	Licence na databáze	Ne	Ano
	Hardware	Ne	Ano
	Navýšení výpočetního výkonu	Ne	Ano (výrazně dražší)
Pravidelné náklady	poplatky za službu	Ano	Ne
	Správa hardwaru a softwaru	Ne	Ano
	Kvalitní internetové připojení	Ano	Ne
	Mzdy pro IT oddělení	Ne	Ano
	Elektřina a prostor pro servery	Ne	Ano
	Poplatek za data ze senzoru, nebo za fyzické místo v cloudu	Ano	Záleží na poskytovateli
	Navýšení výpočetního výkonu	Ano	Ne

Jako **první příklad** lze porovnat služby Microsoft Azure jako kombinaci modelů SaaS a PaaS a služby Microsoft Azure Stack jako „On-premises“ službu. V úvaze je zahrnuto 20 senzorů, např. na výrobní lince, které kontrolují hmotnost produktu. Předpokládá se, že všechny senzory zasílají mezi 8 000 až 400 000 zprávami měsíčně. V úvaze nejsou zahrnuty mzdové poplatky pro IT zaměstnance, jedná se pouze o porovnání nákladů za zřízení a provoz služby. V obou případech je započítána cena za koupi nového PC, určeného pouze ke správě služby.

Varianta 1 – Microsoft Azure [65]

Jednorázové náklady:

- Zřízení služby + licence 0 Kč
- Nastavení služby 0 Kč
- Náklady na zřízení infrastruktury 32 672 Kč
 - 20x senzor 20 000 Kč
 - 3x datalogger 672 Kč
 - PC + licence na OS 12 000 Kč

Pravidelné měsíční náklady:

- Poplatek za senzory + správa zařízení + monitorování 27 000 Kč / měsíc
- Náklady na infrastrukturu (elektřina, prostor atd.) 297 Kč / měsíc
- Servisní náklady (poškozené součástky) 1000 Kč / měsíc

Náklady za první rok: 372 236 Kč

Varianta 2 – Microsoft Azure Stack [66]

Jednorázové náklady:

- Zřízení služby + licence 0 Kč
- Nastavení služby 0 Kč
- Náklady na zřízení infrastruktury 202 370 Kč
 - 20x senzor 20 000 Kč
 - 3x datalogger 672 Kč
 - PC + licence na OS 12 000 Kč
 - Server pro službu viz Obr. 5.1 169 700 Kč
 - 2x 6 jádrový procesor 40 230 Kč
 - 6x 16GB RAM 49 473 Kč
 - 5x HDD, 500GB 27 031 Kč
 - Další komponenty (case, zdroj apod) 47 363 Kč
 - Microsoft Windows Server [58] 5 600 Kč

Pravidelné měsíční náklady:

- Poplatek za senzory + správa zařízení + monitorování 0 Kč / měsíc
- Náklady na infrastrukturu (elektřina, prostor atd.) 1 161 Kč / měsíc
- Servisní náklady (poškozené součástky) 1000 Kč / měsíc

Náklady za první rok: 228 300 Kč

Jednorázový náklad na nastavení služby není v této úvaze započítán, jelikož je to ve správě IT oddělení a cena za mzdy není v úvaze zohledňována. Cena senzorů je 1000 Kč / kus a cena dataloggerů je 224 Kč / kus [58]. PC s OS, obrazovkou, klávesnicí a myší se pohybuje v cenové relaci okolo 12 000 Kč [58]. Při výběru serveru bylo přihlíženo k minimálním požadavkům služby Azure Stack a byla zvolena taková kombinace, aby minimum splňovala [58, 64]. Položka „Servisní náklady“ zahrnuje částku, kterou si firma odkládá měsíčně na opravu součástí, případně na jejich koupi.

Obr. 5.1 Náklady za server pro službu Microsoft Azure Stack

Popis	Množ.	Cena (Kč)	DPH (21%)	Cena s DPH (Kč)
PY RX2520 M1 12x 3.5"	1	24 801,34	5 208,28	30 009,62
Intel Xeon E5-2420v2 6C/12T 2.2GHz 15MB	2	33 248,45	6 982,17	40 230,62
Independent Mode Installation	1	117,07	24,59	141,66
16GB (1x16GB) 2Rx4 L DDR3-1600 R ECC	6	40 886,90	8 586,25	49 473,15
HD SATA 6G 500GB 7.2K HOT PL 3.5" BC	5	22 339,75	4 691,35	27 031,10
SFP+ Module Multi Mode Fiber 10GbE LC	1	11 590,13	2 433,93	14 024,06
Made in Germany sticker	1	29,27	6,15	35,41
Modular PSU 450W platinum hp	1	2 341,44	491,70	2 833,14
Cable powercord rack, 4m, black	1	263,41	55,32	318,73
		135 617,76	28 479,73	164 097,49
Cena celkem s DPH / Kč				164 097,49

Uvedené poplatky za senzory ve variantě 1 vychází z Tab. 7. Jedná se o platební model S1 [69]. Předpokládá se využití služby IoT Hub v Microsoft Azure, která se stará o přijímání/odesílání zpráv z/do zařízení. Platební model S1 je pro tuto službu platný. IoT Hub není zpoplatněn licenčními poplatky. U druhé varianty se počítá s využitím vlastního serveru, přesněji s instalací virtuálního PC s operačním systémem Linux ve službě Azure Stack. IoT Hub není u této služby zatím podporován, proto lze zvolit pro sběr, vyhodnocení a ukládání dat využít variantu jako je aplikace Node-RED, která byl vyvinuta společností IBM pro propojování hardwarových zařízení a také pro služby v oblasti IoT. Tento způsob je detailně popsán v kapitole 6. Při využití této aplikace nejsou zprávy od senzorů zpoplatněny a jejich počet je omezen pouze místem na HDD.

Ceny za elektřinu se v úvaze odvíjejí od doby, po kterou je PC, server, nebo datalogger činný. Při ceně 4 Kč / kWh lze zhruba odhadnout částky náklady podle průměrné spotřeby komponentů. U PC s průměrnou spotřebou 100 W je částka

přibližně 288 Kč / měsíc a u serveru s průměrnou spotřebou 300 W je to přibližně 864 Kč / měsíc. Částka za datalogery je přibližně 15 Kč / měsíc.

Při porovnání nákladů za první rok se jeví jako výhodnější varianta č. 2, ale tyto úvahy jsou silně závislé na počtu senzorů a na vhodně zvoleném poskytovateli. Uvažujeme-li, že se bude hardware, konkrétně PC, datalogery, senzory a server vyměňovat až pátým rokem, tak v průběhu druhého až pátého roku lze počítat s náklady na jednotlivé varianty podle průběžných nákladů za rok jako:

- Varianta 1 – 339 564 Kč
- Varianta 2 – 25 932 Kč

Více cenových relací jednotlivých poskytovatelů lze najít v Tab. 7, 8, 9 a 10.

Druhým příkladem z pohledu finanční nákladnosti může být demo, vytvořené pro tuto práci. Porovnáván je jako implementovaný do služby Microsoft Azure Virtual Machines (model IaaS) a běžící lokálně na dataloggeru Raspberry Pi. Podrobný popis je uveden v kapitole 6.

5.1.2 Z procesů technologické firmy

Nejprve by měla každá firma zvážit, jestli je pro ni přechod na nové řešení vhodný. Měly by být zváženy požadavky na funkce služby a také finanční možnosti firmy. Aby si mohla firma vybírat mezi vhodnými poskytovateli, měla by před výběrem zhodnotit své požadavky na službu viz kapitola 5.

Tab. 5.4 Nabízené distribuční modely ERP systémů.

Název	On-premises/cloud/hybridní režim
Microsoft Dynamics 365	Ano/Ano/Ano
Infor ERP	Ano/Ano/Ano
SAP Business One	Ano/Ano/Ano

Oproti cloudovým a „On-premises“ službám pro senzorové sítě se služby v oblasti ERP a DMS systémů vyznačují vysokými cenami za licence na software a za jejich implementaci a nastavení pro procesy dané firmy. Kromě těchto nákladů je třeba také počítat s náklady za školení zaměstnanců, vyšší servisní podporu a případnou úpravu systému pro požadavky firmy. Se servisní podporou je také spojené, že tyto systémy jsou dodávány pro standardizované užití a za jejich úpravy na pro konkrétní

potřeby firma je třeba si u poskytovatele připlatit, je-li to vůbec možné. Z hlediska počátečních nákladů se jeví, zvláště pro malé firmy, jako vhodnější využít cloudových služeb, jelikož u nich běžně nebývá příplatek za instalaci do serveru firmy, jako je tomu v případě „On-premises“ služby. Tyto příplatky se pohybují v řádech desítek až statisíců korun. Poskytovatelé si v nejvíce případech u takových systémů účtují cenu za uživatele, který software využívá. V Tab. 5.5 lze vidět příklady cen při nasazení softwaru jako cloudové služby.

Tab. 5.5 Ceny za ERP systémy nasazené v cloudu.

Název	Ceny za cloudovou službu
Microsoft Dynamics 365	Dynamics 365 Plan 1: 115\$/uživatel/měsíc Dynamics 365 Plan 2: 210\$/uživatel/měsíc
Infor ERP	Různé v závislosti na poskytovateli služby (v ČR např. společnost GEMMA Systems, spol. s r.o.)
SAP Business One	Různé v závislosti na poskytovateli služby (v ČR např. společnost Versino CZ, s.r.o.)

Jako finanční výhoda se také jeví možnost integrace DMS systémů do ERP systémů. Lze tak odbourat nejen problémy s kompatibilitou a s ní spojenou nákladovostí za servis v případě, že jsou využity služby dvou různých poskytovatelů, ale také lze snížit poplatky za licence, a to především u „On-premises“ služeb, pokud jsou tyto dvě služby dodávány jako celek. V Tab. 5.6 lze vidět příklady známých ERP systémů a s jakými DMS systémy jsou kompatibilní. Více v Tab. 12.

Tab. 5.6 Známé ERP systémy kompatibilní s MS Office.

Název	Možnost integrace DMS do ERP
Microsoft Dynamics 365	Ano (MS Office 365)
Infor ERP	Ano (MS Office)
SAP Business One	Ano (MS Office)

Na základě těchto informací může být vytvořena zhodnocovací tabulka ukazující, které náklady jsou u jakého modelu nasazení.

Tab. 5.7 Finanční zhodnocení z pohledu jednorázových a pravidelných nákladů.

	Náklady za služby	IaaS, PaaS, SaaS	On-Premises
Jednorázové náklady	Licence na software poskytovatele	Ne	Ano
	Licence na OS	Ne	Ano
	Licence na databáze	Ne	Ano
	Hardware	Ne	Ano
	Navýšení výpočetního výkonu	Ne	Ano (výrazně dražší)
Pravidelné náklady	poplatky za službu	Ano	Ne
	Správa hardwaru a softwaru	Ne	Ano
	Kvalitní internetové připojení	Ano	Ne
	Mzdy pro IT oddělení	Ano	Ano
	Elektřina a prostor pro servery	Ne	Ano
	Poplatky za uživatele	Ano	Ano
	Navýšení výpočetního výkonu	Ano	Ne

Jako **první příklad** může být porovnání cloudové služby „Microsoft Dynamics 365“ a „On-premises“ služby „Microsoft Dynamics 365 (On-premises)“. Dynamics 365 v sobě kloubí služby ERP systémů (procesy spojené s financemi, personalistikou prodejem, výrobou a logistikou), a CRM systémů (procesy spojené s marketingem a službami pro zákazníky). Uvažujme 10 uživatelů přistupujících ke službě. V úvaze nejsou zahrnuty mzdové poplatky pro IT zaměstnance, jedná se pouze o porovnání nákladů za zřízení a provoz služby. V obou případech je započítána cena za koupi nového PC, určeného pro každého zaměstnance.

Varianta 1 – Microsoft Dynamics 365 (cloud) [67]

Jednorázové náklady:

- Náklady na zřízení infrastruktury 56 000 Kč
 - 10x PC + 10x licence na OS 36 000 Kč
- Zřízení služby + licence 0 Kč
- Nastavení služby 0 Kč
- Školení personálu 20 000 Kč / 2 dny

Pravidelné měsíční náklady

- Poplatky za uživatele 5 460 Kč / měsíc
- Náklady na infrastrukturu (elektřina, prostor atd.) 960 Kč / měsíc
- Servisní náklady (opravy PC) 2000 Kč / měsíc

Náklady za první rok: 177 040 Kč

Varianta 2 – Microsoft Dynamics 365 (On-premises) – odhadované [68]

Jednorázové náklady:

- Náklady na zřízení infrastruktury 97 543 Kč
 - 10x PC + 10x licence na OS 36 000 Kč
 - Server pro službu 61 543 Kč
 - 1x 4 jádrový procesor 15 700 Kč
 - 1x 8 GB RAM 4 200 Kč
 - 5x HDD, 300GB 7 200 Kč
 - Microsoft Windows Server 5 600 Kč
 - Další komponenty (case, zdroj apod) 15 758 Kč
- Zřízení služby + licence 319 304 Kč
 - Licence za uživatele 141 180 Kč
 - Licence za server 178 124 Kč
- Nastavení služby 0 Kč
- Školení personálu 20 000 Kč / 2 dny

Pravidelné měsíční náklady:

- Poplatky za uživatele 0 Kč / měsíc
- Náklady na infrastrukturu (elektřina, prostor atd.) 1392 Kč / měsíc
- Servisní náklady (opravy PC, serveru) 2000 Kč / měsíc

Náklady za první rok: 477 550 Kč

Jednorázový náklad na nastavení služby není v této úvaze započítán, jelikož je to ve správě IT oddělení a cena za mzdy není v úvaze zohledňována. PC s OS, obrazovkou, klávesnicí a myší se pohybuje v cenové relaci okolo 12 000 Kč [58]. Při výběru serveru bylo přihlíženo k minimálním požadavkům služby Microsoft Dynamics 365 a byla zvolena taková kombinace, aby splňovala doporučenou konfiguraci [60]. Položka „Servisní náklady“ zahrnuje částku, kterou si firma odkládá měsíčně na opravu součástí, případně na jejich koupi. V ceně je zahrnuta také odhadovaná částka za školení externistou. Jelikož jsem nemohl dohledat školící společnost na tuto službu, odhadl jsem částku podle společnosti SoftGate s.r.o., která na svém webu uvádí nabízí kurzy za školení produktů společnosti Microsoft [61]. U druhé varianty nebylo možné určit přesně částky za licenci na server a za licence pro uživatele, jelikož ve verzi Microsoft Dynamics 365 poskytovatel podává informace o

cenách na vyžádání. Proto jsem vycházel z cen produktu, který byl předchůdcem verze 365, tedy produktu Microsoft Dynamics CRM [62]. Položka „Servisní náklady“ zahrnuje částku, kterou si firma odkládá měsíčně na opravu součástí, případně na jejich koupi.

Poplatky za uživatele v první variantě vychází z Tab. 12. Konkrétně jde o platební model Dynamics 365 Plan 2 [70]. Licence na službu není zpoplatněná, firma platí pouze za zaměstnance využívající službu. U druhé varianty platí firma nejvíce za jednorázové licence pro zaměstnance a server, avšak tyto licence jsou permanentní.

Ceny za elektřinu se v úvaze odvíjejí od doby, po kterou je PC a server činný. Při ceně 4 Kč / kWh lze zhruba odhadnout částky náklady podle průměrné spotřeby komponentů. U PC s průměrnou spotřebou 100 W je částka za 10 PC, které běží 8 hodin denně přibližně 960 Kč / měsíc a u serveru s průměrnou spotřebou 150 W běžícího 24 hodin denně je to přibližně 432 Kč / měsíc.

Při porovnání nákladů za první rok se jeví jako výhodnější varianta č. 1, ale tyto úvahy jsou silně závislé na počtu zaměstnanců a na vhodně zvoleném poskytovateli. Uvažujeme-li, že se bude hardware, konkrétně PC a server, vyměňovat až pátým rokem, tak v průběhu druhého až pátého roku lze počítat s náklady na jednotlivé varianty podle průběžných nákladů za rok jako:

- Varianta 1 – 101 040 Kč
- Varianta 2 – 40 704 Kč

Více cenových relací jednotlivých poskytovatelů lze najít v Tab. 12.

Druhým příkladem může být porovnání nákladů na DMS systém. Uvažujme 10 uživatelů stejně jako v minulém případě. Porovnávána bude cloudová služba Microsoft Office 365 Business Premium a „On-premises“ služba „M-Files DMS“. Služba Microsoft Office 365 není typickým představitelem DMS systémů. Jedná se o balíček služeb, mezi nimiž je aplikace Microsoft Sharepoint, která vykonává funkci DMS systému. Kromě správy dokumentů jsou v balíčku také aplikace jako Microsoft Word, Excel, PowerPoint, Outlook a další. M-Files DMS systém je určen pouze k automatizaci oběhu dokumentů, administraci dokumentů a schvalování dokumentů. V úvaze nejsou zahrnuty mzdové poplatky pro IT zaměstnance, jedná se pouze o porovnání nákladů za zřízení a provoz služby. V obou případech je započítána cena za koupi nového PC, určeného pro každého zaměstnance.

Varianta 1 – Office 365 Business Premium [71]

Jednorázové náklady:

- Náklady na zřízení infrastruktury 36 000 Kč
 - 10x PC + 10x licence na OS 36 000 Kč
- Zřízení služby + licence 0 Kč
- Nastavení služby 0 Kč
- Školení personálu 20 000 Kč / 2 dny

Pravidelné měsíční náklady:

- Poplatky za uživatele 3 429 Kč / měsíc
- Náklady na infrastrukturu (elektřina, prostor atd.) 960 Kč / měsíc
- Servisní náklady (opravy PC) 2000 Kč / měsíc

Náklady za první rok: 132 668 Kč

Varianta 2 – M-Files DMS [73]

Jednorázové náklady:

- Náklady na zřízení infrastruktury 97 543 Kč
 - 10x PC + 10x licence na OS 36 000 Kč
 - Server pro službu 61 543 Kč
 - 1x 4 jádrový procesor 15 700 Kč
 - 1x 8 GB RAM 4 200 Kč
 - 5x HDD, 300GB 7 200 Kč
 - Microsoft Windows Server 5 600 Kč
 - Další komponenty (case, zdroj apod) 15 758 Kč
- Zřízení služby + licence 319 304 Kč
 - Licence za uživatele 53 730 Kč
 - Licence za server nezjištěno
- Nastavení služby 0 Kč
- Školení personálu 20 000 Kč / 2 dny

Pravidelné měsíční náklady:

- Poplatky za uživatele 0 Kč / měsíc
- Náklady na infrastrukturu (elektřina, prostor atd.) 1392 Kč / měsíc

- Servisní náklady (opravy PC, serveru)

2000 Kč / měsíc

Náklady za první rok: 211 977 Kč

Jednorázový náklad na nastavení služby není v této úvaze započítán, jelikož je to ve správě IT oddělení a cena za mzdy není v úvaze zohledňována. Uvedené náklady jsou téměř shodné s náklady uvedenými v úvaze o cenách ERP systémů. Jelikož nebylo možné vyhledat požadavky na server, využil jsem stejné konfigurace jako u ERP. Také ceny za elektřinu jsou stejné, jelikož se v obou případech počítá s jedním serverem a deseti počítači. Školení si zajišťuje sám poskytovatel služby, ale neuvádí za něj ceny, proto byla uvažována částka jako v předchozích případech. U varianty č. 1 byl využit platební model Plán 2 [71], protože v balíčku služeb zahrnuje také aplikaci Sharepoint a u varianty č. 2 byl využit první platební model viz Tab. 14.

Při porovnání nákladů za první rok se jeví jako výhodnější varianta č. 1, ale tyto úvahy jsou silně závislé na počtu zaměstnanců a na vhodně zvoleném poskytovateli. Uvažujeme-li, že se bude hardware, konkrétně PC a server, vyměňovat až pátým rokem, tak v průběhu druhého až pátého roku lze počítat s náklady na jednotlivé varianty podle průběžných nákladů za rok jako:

- Varianta 1 – 76 668 Kč
- Varianta 2 – 40 704 Kč

Více cenových relací jednotlivých poskytovatelů lze najít v Tab. 14.

5.2 Spolehlivost

Při zřizování cloudové služby je důležité předem počítat s navýšením provozu v internetové síti firmy. Poskytovatelé služeb se snaží o co nejmenší datovou náročnost komunikace se servery, přesto je třeba pro takovou firmu zajistit **rychlé a stabilní internetové připojení**. S internetovým připojením je také spojená **rychlost odezvy služby**. Rychlost odezvy je závislá na trase, kterou musí urazit informace od uživatele ke službě a zpět. Především je tak závislá na hardwaru (switche, routery, huby), který je na trase situován. Dalšími prvky, které mohou ovlivňovat dobu odezvy jsou použité technologie přenosu mezi jednotlivými uzly v síti (Wi-Fi, Ethernet, DSL, 3G,4G, optické sítě atd.). V neposlední řadě může dobu odezvy ovlivnit také kvalita signálu, a to především u bezdrátových sítí. Doba odezvy je pouhým součtem dílčích zdržení na jednotlivých úsecích trasy. Při výběru vhodného poskytovatele by tak měla

firma přihlížet k přijatelné době odezvy od nabízeného datového centra. Podle webové aplikace cloudping [55] je odezva z mého PC do okolních datových center cloudové služby Amazon Web Services (Irsko, Anglie, Německo) pod 100ms, což je hodnota, při které časová prodleva nepůsobí na člověka jako zpoždění. V případě odezvy větší, než 100ms mohou nastat problémy spojené s přenosem dat, tj. neúplné doručení, ztráta dat apod.

Z pohledu škálovatelnosti se nejedná pouze o finanční, ale také technickou výhodu. V případě nutnosti **navýšení výpočetní kapacity** u cloudové služby stačí pouze několik minut na zřízení žádosti a ta bývá během několika minut až hodin zpracována. Oproti „On-premises“ službě tak odpadá čekací doba na fyzické dodání serverů a jejich integrace do stávající infrastruktury.

Jako výhoda cloudových služeb se jeví jejich **údržba**, a s tím spojená **pravidelná aktualizace služeb**. Poskytovatel se zaručuje udržovat takovou kvalitu služby, kterou má s firmou smluvně ujednanou. Díky tomu odpadá potřebný čas, který by této činnosti musel věnovat zaměstnanec údržby, nebo IT oddělení jako tomu je u služby typu „On-premises“. Aktualizace služeb na úrovni platformy, či aplikace bývá zpravidla bezplatná. Tyto aktualizace mohou být nehlášené a je tak třeba předem počítat se změnami ve funkcích aplikace, které by mohly ochromit činnost firmy.

Při výběru cloudové služby by měla firma přihlížet také k její **minimální garantované dostupnosti**. Většina poskytovatelů ke svým službám uvádí její procentuální dostupnost. Jinými slovy to znamená, že pokud je uvedena hodnota např. 99,95 %, tak je garantovaná doba fungování v jednom měsíci 99,95 % času. Do zbylých 0,05 % času je zahrnuta možnost výpadku z blíže nespecifikovaných důvodů. Jako standard je u cloudových služeb poskytována **24 hodinová technická podpora**. Oproti možnosti výpadku firemního serveru by se tato doba mohla zdát příliš dlouhá, ale v případě poruchy a potřeby výměny firemního serveru se lze bavit o časech na opravu v rámci minut až dnů.

5.2.1 Ze senzorové sítě

U technologických firem, které při své pracovní činnosti spoléhají na činnost senzorové sítě, je třeba důsledně dbát při výběru služby na její co možná největší dostupnost, dostačující výkon, spolehlivost a v případě potřeby i rozšiřitelnost.

V případě cloudové služby jsou data odesílána prostřednictvím internetu do vzdáleného cloudu, je tak třeba počítat s určitou časovou prodlevou. Tato prodleva by mohla způsobit dočasné výpadky výroby či jiných procesů a způsobit firmě ztráty. V některých případech lze mluvit i o kompletním zastavení provozu celé firmy, a to je

s její činností neslučitelné. Cloudová služba se tak jeví jako vhodná v případě, kdy firma pracuje s velkými objemy dat, které nevyžadují okamžitou odezvu. Oproti tomu se „On-premises“ služba jeví jako vhodná varianta při potřebě okamžité odezvy. Jelikož jsou data shromažďována pouze z lokální sítě (např. výrobní hala), doba odezvy je minimální a lze tak mluvit real-time sbírání a vyhodnocování dat.

Při výběru vhodného řešení je třeba kromě odezvy služby přihlížet také k její dostupnosti. Minimální garantovaná dostupnost cloudové služby bývá uváděna ve smlouvě o úrovni poskytovaných služeb, tzv. SLA (Service Level Agreement) smlouvě. Ta je součástí smluvní dohody mezi firmou a poskytovatelem o zřízení a využívání služby. SLA firmě garantuje dohodnutou kvalitu služeb a s ní spojenou uvedenou dostupnost. V případě, že poskytovatel nedodrží určitou kvalitu služby, kterou garantuje, může mít firma nárok na odškodnění v podobě snížení poplatků za danou službu. Reálným příkladem výpadku cloudové služby je výpadek služby Amazon Web Services společnosti Amazon z února 2017. Několikahodinový výpadek zapříčinil, že nefungovali některé webové stránky a aplikace, např. známá aplikace Snapchat nebo Slack [41]. „On-premises“ služba takové smluvní ujednání o dostupnosti služeb neobsahuje. Software je dodáván jen jako aplikace (případně jako vývojová platforma) do serverů firmy a veškerá starost o dostupnost tak připadá na IT oddělení firmy. Příklad garantovaných dostupností IoT cloudových služeb lze nalézt v tabulce IV, více pak v Tab. 7, 8, 9 a 10.

Tab. 5.8 Dostupnost služeb uvedená v SLA.

Název	Min. garantovaná dostupnost
Microsoft Azure	99,95 %
Oracle cloud	99,9 %
Amazon Web Services	99,95 %

Na první pohled by se mohlo zdát, že výhodnější je jednoznačně „On-premises“ služba, která by měla mít teoreticky 100 % dostupnost. Proti tomuto faktu svědčí obecně známá věc a to, že elektronika nemá nekonečnou životnost. Při přihlédnutí k poměru serverů, které vlastní poskytovatel cloudové služby a četnosti záloh, kterými disponuje, je zřejmé, že v případě poruchy na straně poskytovatele nemusí k výpadku cloudové služby vůbec dojít nebo dojde k takovému výpadku, který je poskytovatel schopen odstranit v rámci vteřin až minut.

Pro vhodnost cloudové služby také svědčí často garantovaná podpora 24/7. Při řešení ve vlastním datovém centru opět připadá správa na IT oddělení. Aby mohla firma pokrýt podporu 24/7, musela by zaměstnávat více IT odborníků nebo si

příplácet za neustálou pohotovost stávajícího IT personálu, a to by mohl být velký zásah do rozpočtu malé firmy. Výsledkem tak je, že v případě poruchy lokálního serveru by mohla být přerušena činnost firmy na dobu několika hodin, případně i dnů a týdnů při nutnosti kompletní výměny serveru.

Zdarma aktualizace aplikací bývají obecně zahrnuty ve smluvních podmínkách při zřizování jak cloudové služby, tak „On-premises“ služby. Myšlenkou každého poskytovatele je udržet svůj software, ale i hardware v aktuální verzi, aby se omezili chyby a případné mezery v zabezpečení poskytovaných systémů. Pokud firma využívá „On-premises“ službu, připadají na její IT oddělení také aktualizace aplikací. Mohlo by se to zdát jako nevýhodné oproti cloudové službě, u které se aktualizace provedou sami bez zásahu uživatele, ale výhoda by se mohla rychle změnit v problém. Ve chvíli, kdy má poskytovatel připravenou aktualizaci pro své služby, většinou neváhá a aktualizuje je. V případě, že se jedná o rozsáhlejší aktualizaci, která by mohla změnit činnost stávajícího systému, bývá zákazník, v tomto případě firma, upozorněna předem. I přesto, že firma ví o připravované aktualizaci předem, nebývá zvykem, aby mohlo IT oddělení do této aktualizace nahlédnout a předem se připravit. V takovém případě nelze zcela vyloučit, že tato aktualizace nepoškodí nebo neznemožní činnost firmy. V případě „On-premises“ služby se IT oddělení dostává k aktualizaci předem a dostává tak možnost ji vyzkoušet před nasazením do aplikace firmy.

5.2.2 Z procesů technologické firmy

Od ERP a DMS systémů si firmy slibují zefektivnění spolupráce mezi jednotlivými procesy. U ERP se jedná především o řízení výroby a řízení příjmových a výdejových procesů. Dalšími požadavky na systém je např. snižování doby realizace výrobních procesů a s tím spojená vyšší návratnost investic, dále také např. zlepšení komunikace mezi zaměstnanci.

Většina nabízených ERP a DMS systému je dnes nabízena pro obecné užití a z toho vyplývá, že nemají příliš mnoho možností úprav dle potřeb firmy. Nejčastěji se lze setkat s těmito systémy u cloudové služby v podobě modelu SaaS, tedy v podobě kompletního předpřipraveného softwaru. Jelikož software běží v serveru poskytovatele a je uzpůsoben tak, aby k němu mohlo přistupovat i několik firem využívající tentýž systém, poskytovatel ne příliš ochotně povoluje zásahy do funkcí systému, a tak je při využití cloudové služby firma odkázána na předpřipravené funkce a ochotu poskytovatele. Právě kvůli těmto omezením se především ERP systémy vyskytují na trhu v podobě „On-premises“ služby. Díky nasazení služby na

serveru firmy jsou otevírány možnosti úprav systému, kterým se poskytovatel nemusí nijak bránit.

Většina ERP a DMS v systému v sobě již zahrnuje tzv. workflow viz kapitola 4.2.2, které napomáhá definovat procesní cesty a udává pokyny k jednotlivým procesům. Workflow bývá zahrnuto v obou systémech jako jakýsi standard pro tyto služby, případně si ho lze u některých poskytovatelů zakoupit jako službu navíc. Jak v případě cloudové služby, tak „On-premises“ služby se o workflow stará IT oddělení.

Tab. 5.9 ERP a DMS systémy s integrovaným workflow.

Název	Workflow zahrnuto v systému
Microsoft Dynamics 365	Ano
Infor ERP	Ano
SAP Business One	Ano
Google G Suite	Ano
Office 365 Business Premium	Ano
M-Files DMS	Ano

Díky využití cloudové služby je umožněno řízení vzdáleně. To znamená, že v případě nějaké poruchy nebo náhle potřeby změny v některém z procesů se může zaměstnanec vzdáleně před webové rozhraní přihlásit do systému a změnu provést. Taková možnost u „On-premises“ služby není.

Na rozdíl u senzorových sítí se u ERP a DMS systémů neklade takový důraz na odezvu. Činnosti spojené s procesy jako je kontrola zásob, kontrola stavů objednávek či práce s dokumenty nemívají kritické následky při delší časové odezvě, a proto lze využití cloudové služby zvažovat při výběru vhodného systému. S tím je také spojená dostupnost služby nasazené v cloudu, která u většiny poskytovatelů přesahuje hodnotu 99,9 %. V případě výpadku internetu ve firmě, nebo výpadku cloudové služby by mohla firma vykazovat ztráty a je tak třeba nejprve zvážit, jestli se je takové riziko pro danou firmu přijatelné. U technologické firmy lze předpokládat, že by výpadek spojení mohl narušit její procesy, a je tak třeba tuto možnost eliminovat, např. více nezávislými internetovými připojeními proti výpadku internetu a zabezpečovacím systémem, který výpadek rozpozná a nedovolí zaměstnancům/strojům vykonat činnost, kterou by mohly procesy poškodit. Lze si představit například stroj, který vykonává v jedné ose řez a dostane povel, aby začal, ale už mu díky výpadku nedorazí povel na zastavení. Takový stroj by mohl bez ochranného procesu poničit sebe, nebo vyráběný předmět.

Jako v případě cloudů pro senzorové sítě i pro ERP a DMS systémy platí, že poskytovatel má velké množství serverů situované v různých oblastech. Díky tomu je při využití cloudové služby zajištěna vysoká bezpečnost pro data s pravidelným zálohováním mezi více serverů. I u malé firmy lze předpokládat, že pracuje s velkým množstvím dat a díky velkému, teoreticky neomezenému úložnému prostoru, který cloudy nabízejí lze tato velká množství dat uchovávat po dobu několika let i desetiletí v závislosti na financích, které firma do úložného prostoru dá. Oproti tomu při nasazení softwaru ve vlastním centru je firma omezená kapacitou úložného prostoru serveru a rozšiřitelnost takového prostoru je řádově o desetitisíce až statisíce zdraží, než by tomu bylo u cloudové služby.

Dokumenty a data firem mohou mít různou podobu. Mezi běžně využívané se řadí např. souborový formát PDF firmy Adobe nebo souborové formáty textových dokumentů DOC(X) a tabulek XLS(X) z kancelářského balíku Microsoft Office společnosti Microsoft a další. Při přechodu firmy na cloudovou nebo „On-premises“ by mělo být přihlíženo k tomu, jestli software umožňuje integraci těchto dokumentů do systému. Většina ERP, a především DMS systémů tuto funkci umožňuje a také většina těchto systémů umožňuje práci minimálně s formáty z balíku Microsoft Office. Některé DMS systémy navíc nabízí možnost skenování papírových dokumentů do systému a podle předem definovaných šablon si systém sám přečte informace a vhodně je přiřadí do složek.

5.3 Bezpečnost

Především **povaha firemních dat** může hned ze začátku rozhodnout o zamítnutí využití cloudové služby na serveru poskytovatele. Dnes se ještě mnoho firem brání přechodu na cloudovou službu z obav jako je ztráta dat, odcizení a zneužití citlivých dat, případně jim to nedovoluje firemní politika. Tyto obavy jsou reálné, avšak poskytovatelé si nemohou dovolit jakýkoliv únik dat zákazníka, jelikož by to mohlo znamenat okamžitou ztrátu dobrého jména a především zákazníků. V případě, že data z cloudu uniknou, můžou být na poskytovatele uvaleny sankce dle smluvního ujednání o nedodržení kvality služeb (SLA).

Fyzické umístění dat je často skloňovaným tématem především u firem pracujících s daty různých citlivostí (know-how, výrobní tajemství apod.). Data jsou nejcennějším majetkem firem, a proto je třeba je velmi dobře zabezpečit před odcizením a zneužitím. Na první pohled by se mohlo jevit využití „On-premises“ služby jako nejvhodnější, ale nemusí tomu tak být. V tomto případě se o zabezpečení dat stará IT oddělení firmy, které zajišťuje bezpečnost vlastními

prostředky. Data jsou neustále ohrožována malwary (počítačové viry, trojské koně, spywary, adwary) a útoky zvenčí (DDOS útoky). Tyto cílené útoky jsou neustále zlepšovány, aby mohly snáze proniknout do systémů firem, a proto je důležité dbát na aktuálnost a kvalitu stávajícího zabezpečení. Data jsou také ohrožovány vlastními zaměstnanci, kteří je mohou vynášet z lokálních serverů neúmyslně, ale i úmyslně. Uvádí se, že až tři čtvrtiny případů úniku dat je způsobeno nedbalostí, či případným úmyslným vynášením dat zaměstnanci firmy [43].

V případě, že firma nedisponuje dostatečnými finančními prostředky pro zajištění požadovaného zabezpečení svých dat (fyzické zabezpečení serverů, budovy, silný firewall, antivirový program apod.), jeví se využití cloudové služby jako vhodná varianta. Ve chvíli, kdy začne firma využívat cloudových úložišť mimo svojí vnitřní infrastrukturu, začne svoje data poskytovat poskytovateli. To se může jevit jako nevýhodné v mnoha ohledech, avšak kvalitní poskytovatel zajišťuje neustálou aktuálnost zabezpečení svých služeb. Aby bylo zabráněno odcizení dat při přenosu do/z cloudu, je třeba dbát na šifrování odesílaných dat a při výběru poskytovatele přihlížet k tomu, jestli cloudová služba disponuje požadovanými bezpečnostními certifikáty a jestli umožňuje příjem a zasílání šifrovaných dat, avšak to je dnes téměř standardem. Standardem je také **přirazování přístupových práv** pro jednotlivé zaměstnance i zákazníky firmy.

Z **legislativního hlediska** je třeba brát v potaz, jestli firma nepracuje s daty, které nemohou opustit určité hranice (firmy, státu, světadílu). I v takových případech existují poskytovatelé, kteří s takovými omezeními počítají a nabízejí různé balíčky služeb a smluvních ujednání podle potřeb firmy. Častou možností bývá v tomto případě **hybridní řešení**, kdy jsou citlivá data ponechávána v lokálním serveru a zbylé v cloudové službě. Pro malé firmy, které nevyžadují od serverů vysokou výkonost a veliký úložný prostor, lze uvažovat servery v cenové relaci od deseti tisíc do sto tisíc [58]. Využití hybridního řešení se tak jeví jako reálné jak u firem, které teprve plánují nákup infrastruktury, tak i u těch, které již infrastrukturu mají.

V případě **fyzické bezpečnosti serverů**, vychází lépe cloudová služba. Lze předpokládat, že malá firma nedisponuje velkým počtem serverů, takže má omezené možnosti záloh, ale pokud ano, většinou jsou tyto servery situované v jedné místnosti, či objektu. Tyto místnosti se servery by kromě ochrany v podobě dveří a stěn měly mít také bezpečnostní alarmy jako prevenci proti krádežím, hlásiče požárů, efektivní klimatizaci a měly by být situované v takové lokalitě, aby se dalo snížit riziko vlivu živlů, např. vytopení při povodni. Zmíněné bezpečnostní prvky jsou charakteristické také pro datová centra poskytovatelů, která disponují počtem serverů v řádu stovek až tisíců. Aby byla zajištěna maximální ochrana, data bývají

zálohována mezi více datovými centry situovanými v různých lokalitách. Proti neoprávněnému vniknutí osob bývají datová centra kontrolována ochrankou během celého dne i noci. Aby se nezapomínalo na životní prostředí, někteří poskytovatelé staví svá datová centra v oblastech, které jsou celoročně chladné a lze tak kromě aktivního chlazení využít také pasivní chlazení z okolí.

5.3.1 Ze sensorové sítě

Jak už bylo zmíněno, data jsou v neustálém ohrožení, a proto by mělo být prioritou firem si je chránit, počínaje jejich sběrem ze sensorové sítě až po jejich fyzické odstranění z uložště.

Senzory, které přenášejí informaci pomocí metalického nebo optického spoje jsou proti útokům díky jejich uzavřenosti více odolné, než je tomu u bezdrátového přenosu, avšak napadnout je také lze, např. fyzickým napojením se na spoj mezi senzorem a dataloggerem. Hůře jsou na tom bezdrátové systémy, které jsou neustále vystavovány potencionálním útokům. Proto se k ochraně bezdrátově přenášených dat využívá síťové šifrování. Např. IQRF technologie využívá k šifrování komunikace standardizovaný algoritmus AES-128 (Advanced Encryption Standard), který umožňuje šifrování a dešifrování jedním klíčem [52]. Dalším příkladem může být v IoT hojně využívaný MQTT protokol, který je čistě textový a bez použití šifrování je komunikace zcela nešifrovaná. Takto nešifrovaná komunikace je použitelná při komunikaci v lokálních sítích pod TCP kanálem 1883 a do tohoto řešení spadá i „On-premises“ služba. Pokud by ale měla sensorová síť komunikovat po internetu s externím brokem a dále s cloudem, jako je tomu při využití cloudových služeb, je třeba data šifrovat. K tomuto účelu lze využít šifrovaný SSL (Secure Sockets Layer), či TLS (Transport Layer Security) přenos pod TCP kanálem 8883 [46]. Pro zajištění bezpečnosti přenosu dat bývá běžné, aby probíhalo **šifrování a dešifrování** až na straně zákazníka.

V Tab. 5.10 lze vidět komunikační protokoly, díky kterým je možné s danou službou komunikovat. Nejčastěji se v IoT objevují protokoly jako MQTT, WebSockets, či HTTPS (Hypertext Transfer Protocol Secure). Více pak v tabulkách 7, 8, 9 a 10.

Tab. 5.10 Komunikační protokoly, programovací jazyky a platformy.

Název	Komunikační protokoly
Microsoft Azure	AMQP, HTTPS, MQTT
Oracle cloud	HTTP, MQTT
Amazon Web Services	HTTP, WebSockets, MQTT

U velkých poskytovatelů cloudových služeb je běžné, že mají svá datová centra v mnoha místech po celém světě. Mezi výhody takto situovaných center patří např. možnost uchovávání dat v rámci Evropské unie, či České republiky. V Tab. 5.11 lze najít příklady oblastí, které lze využít pro ukládání dat a také informaci, zda je umožněn výběr mezi těmito lokacemi. Více pak v tabulkách 7, 8, 9 a 10.

Tab. 5.11 Polohy datových center pro ukládání dat ze senzorové sítě.

Název	Umístění ve vlastním serveru (On-premises)	Oblasti umístění dat (na serveru poskytovatele)	Možnost volby umístění dat (na serveru poskytovatele)
Microsoft Azure	Ano	Jihovýchodní Asie, Jihovýchodní Austrálie, Severní Evropa, Středozápad USA, USA – východ, USA – západ, Východní Asie, Východní Austrálie, Východní Japonsko, Západní Evropa	Ano
Oracle cloud	Ano	Severní Amerika, Jižní Amerika, Evropa, Asie a Tichomoří	Ano
Amazon Web Services	Ano	Východní Amerika, Západní Amerika, Jižní Amerika, Evropa, Asie a Tichomoří	Ano

Detailněji bude problematika ukládání citlivých dat popsána v kapitole 5.3.2.

5.3.2 Z procesů technologické firmy

Témata bezpečnosti u technologických firem jsou především:

- Přiřazování přístupových práv k informacím
- Umístění citlivých dat

Oproti IoT cloudům, ke kterým přistupuje minimum pověřených osob jsou ERP a DMS systémy uzpůsobeny tak, aby k nim přistupovala většina zaměstnanců. Firma může mít mnoho oddělení jako je účetní oddělení, oddělení starající se o výrobu, oddělení správy zásob a jiné. Zaměstnanci jednotlivých oddělení však přistupují ke stejné aplikaci, a proto je třeba důsledně dbát na přiřazování práv. O to se v obou případech nasazení stará IT oddělení. Základem je, že každý zaměstnanec má svoje přístupové údaje a podle nich se mu zpřístupní právě ty funkce, které se své činnosti vyžaduje. V případě vyššího zabezpečení se využívají k přihlašovací údajům i identifikační karty, nebo otisky prstů. V případě, že data uniknou z lokálního serveru firmy, není mnoho možností, jak vymáhat odškodné po zaměstnanci, proto by u firem pracujících s citlivými daty měla být u každého zaměstnance podepsaná smlouva

o mlčenlivosti. V případě úniku dat z cloudové služby lze podle SLA požadovat od poskytovatele odškodné na základě smluvených podmínek.

Tab 5.12 ERP a DMS systémy s funkcí přiřazování práv.

Název	Funkce systému přiřazovat práva
Microsoft Dynamics 365	Ano
Infor ERP	Ano
SAP Business One	Ano
Google G Suite	Ano
Office 365 Business Premium	Ano
M-Files DMS	Ano

Fyzická bezpečnost dat byla popsána v kapitole 5.3. Dokumenty a data lze rozdělit na 3 stupně podle úrovně ochrany, kterou vyžadují na [53]:

- Úroveň 1 – běžná úroveň ochrany (veřejně přístupné obchodní a vnitropodnikové dokumenty určené pro větší skupinu lidí)
- Úroveň 2 – vysoká úroveň ochrany (neveřejné obchodní a vnitropodnikové dokumenty určené pro určitý okruh lidí)
- Úroveň 3 – velmi vysoká úroveň ochrany (důvěrné a tajné dokumenty, určené pro malý okruh lidí s oprávněným přístupem)

U první úrovně jsou data veřejná, proto je lze ukládat jak v cloudu, tak v lokálním serveru firmy. Mezi tyto dokumenty patří např. obchodní nabídky, ceníky, katalogy, brožury, vyhlášky, obchodní podmínky apod. [53].

U druhé úrovně je už třeba zvážit, jaké by byly následky úniku takových dokumentů a jakou kontrolu nad daty vyžaduje firemní politika. V případě, že data mohou být umístěna v cloudu, lze přistoupit k ochraně pomocí šifrování, která znemožňuje čtení dat kýmkoliv neoprávněným viz kapitola 5.3.1. Další ochranou může být smluvní dohoda s poskytovatelem o bezpečnosti citlivých dat. Tato možnost není standardně nabízena a je třeba kontaktovat poskytovatele a domluvit se s ním na požadované úrovni ochrany. Data mohou být šifrována také v lokálním serveru, většina dnešních ERP a DMS systémů umožňuje šifrování/dešifrování při práci s daty a jejich následném ukládání. Mezi tyto dokumenty patří např. obchodní nabídky, cenové nabídky, zdravotní dokumentace, obchodní výsledky apod. [53].

Do třetí úrovně spadají dokumenty s velmi vysokou úrovní ochrany. Umístění takových dokumentů je většinou řízeno firemní politikou a může být omezováno

zákony, či nařízením daného státu. V takovém případě nezáleží tolik na tom, jestli by firma chtěla cloud využít, ale jestli může. Aby mohly být tato data umístěna do cloudu, musí služby splňovat určité kvalitativní a bezpečnostní standardy. Mezi dokumenty spadající do třetí úrovně ochrany patří např. patenty, know-how, výrobní tajemství, finanční údaje, tajné spisy, tajné dokumenty s mimořádným opatřením, přísně tajné dokumenty (armáda, policie, tajné služby) apod. [53]. V případě, že některá data nemohou opustit prostory společnosti lze využít např. hybridního modelu nasazení.

Tab. 5.13 Polohy datových center pro ukládání dat z procesů technologické firmy.

Název	Oblasti umístění dat	Možnost volby umístění
Microsoft Dynamics 365	Severní a jižní Amerika, Kanada, Velká Británie, EMEA, Německo, Japonsko, Rakousko, Indie	Ano
Infor ERP	-	Ne
SAP Business One	Využívá Amazon Web Services (umístění viz Tab. X)	Ano

6. Demo

Demo vzniklo za účelem zhodnocení a porovnání cloudové služby běžící v cloudu a služby běžící na serveru firmy („On-premises“). Celé demo se skládá z několika komerčních součástí blíže popsanych v kapitole 6.1, cloudové služby a open source softwaru. Snahou je především poukázat na finanční rozdíly mezi těmito dvěma distribučními modely a také na spolehlivost a bezpečnost jednotlivých řešení. Open source software Node-RED, který jsem si pro demo vybral, není představitelem služby nabízené poskytovateli jako využitelné na vlastním serveru, avšak v tomto demu může představovat např. již dříve zmíněnou službu Microsoft Azure Stack, která stejně jako Node-RED není licenčně zpoplatněná.

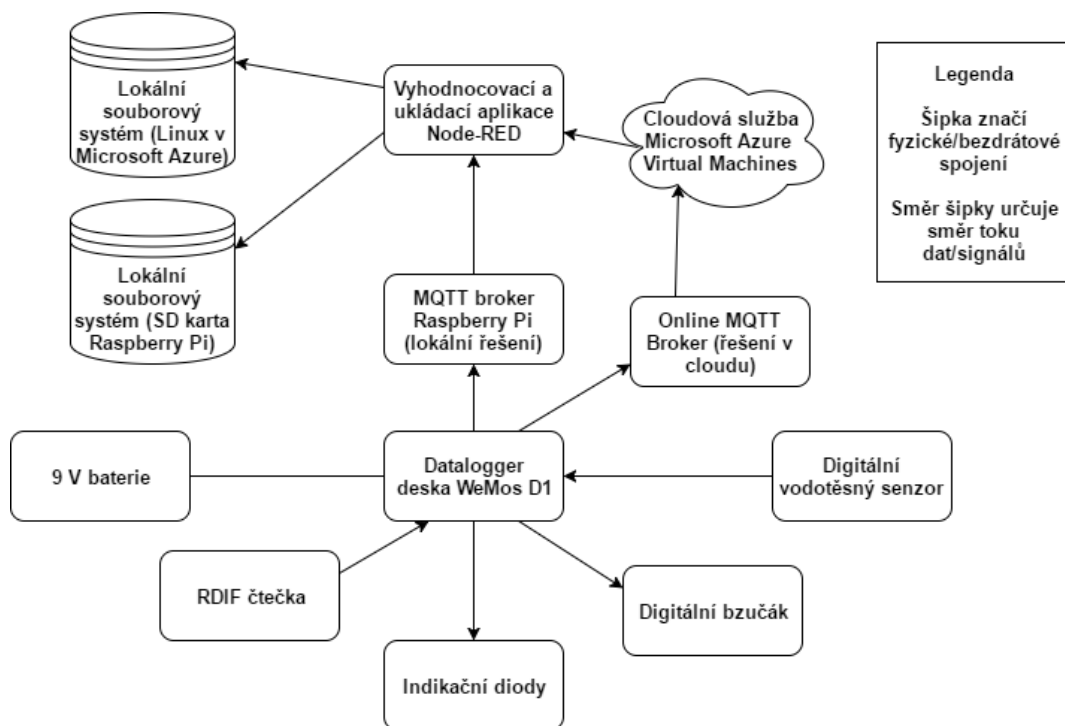
Zadání „Zrealizujte demo sestávající se z vybraných senzorů, mini PC a cloudové služby“ jsem pojal ve spojitosti s technologickou firmou jako měření veličin, v tomto případě teploty a času při výrobních procesech firmy. Za tímto účelem jsem vytvořil spojením několika součástí bezdrátový senzor, který měří teplotu pomocí voděodolného teploměru a také aplikaci v softwaru Node-Red, která data vyhodnocuje v grafickém prostředí a zároveň je ukládá pro zpětné zhlednutí, či budoucí využití. Detailněji je činnost dema popsána v kapitole 6.2.

6.1 Použité prostředky

Veškeré použité prostředky jsou na českém trhu volně dostupné [43 – 45].

6.1.1 Hardware

Na Obr. 6.1 lze vidět blokové schéma dema. Je v něm zahrnuto zároveň zapojení v režimu využití cloudové služby a zapojení při lokálním řešení. Pod blokovým schématem jsou uvedeny jednotlivé komponenty/služby, které byly v demu využity. Každý produkt je charakterizován přiřazenou tabulkou, která obsahuje informaci o ceně a funkci, kterou komponent/služba v demu vykonává. Jak fyzický bezdrátový senzor vypadá lze vidět na Obr. 6.6.



Obr. 6.1 Blokové schéma dema.

Vývojová deska WeMos D1



Obr. 6.2 WeMos D1, převzato z [43].

Tab. 6.1 Údaje o produktu WeMos D1.

Název produktu	ESP8266 ESP-12E OTA WeMos D1 CH340 WiFi Arduino IDE UNO R3
Funkce v demu	Wi-Fi modul, datalogger, napájení pro senzor
Cena za kus (bez DPH)	224 Kč

Vývojová deska Raspberry Pi 3



Obr. 6.3 Raspberry Pi, převzato z [43].

Tab. 6.2 Údaje o produktu Raspberry Pi.

Název produktu	Raspberry Pi 3 Model B Quad Core 1.2 GHz 64bit CPU, 1GB RAM, WiFi, Bluetooth 4.1
Funkce v demu	Wi-Fi modul, MQTT broker, mini PC s OS Linux, „On-premises“ služba
Cena za kus (bez DPH)	1 041 Kč

RDIF čtečka + RFID tagy



Obr. 6.4 RFID čtečka, převzato z [43].

Tab. 6.3 Údaje o produktu RFID čtečka.

Název produktu	Arduino RFID čtečka s vestavěnou anténou
Funkce v demu	Autorizace, spouštění a ukončování měření
Cena za kus (bez DPH)	180 Kč

Digitální vodotěsný teploměr



Obr. 6.5 Digitální teploměr, převzato z [43].

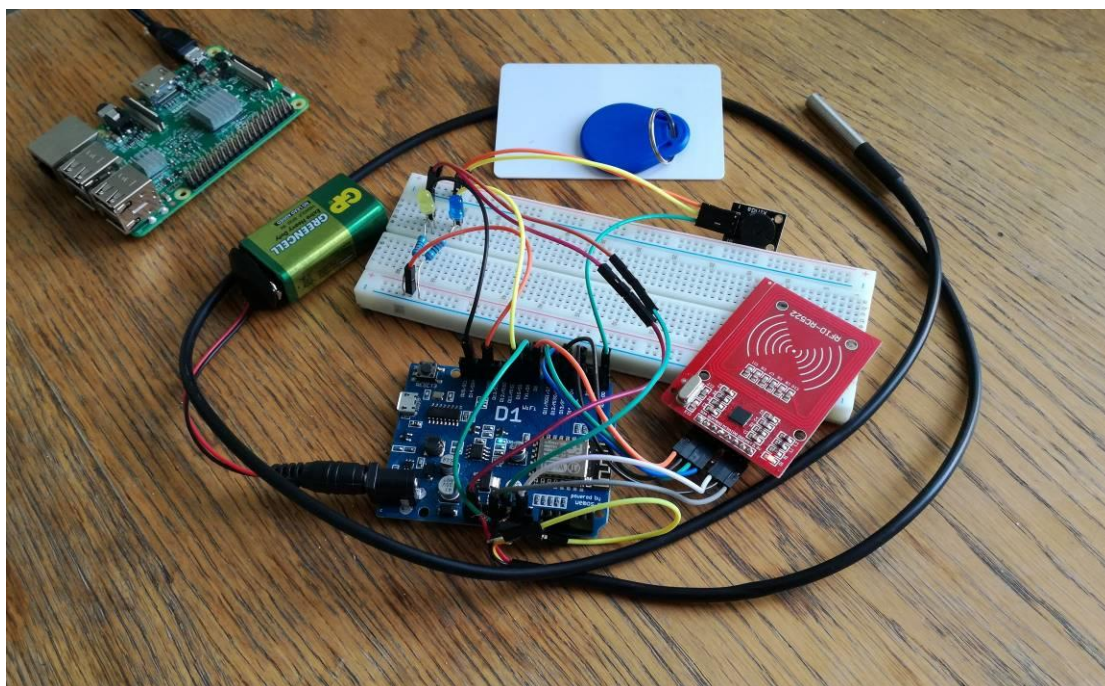
Tab. 6.4 Údaje o produktu digitální teploměr.

Název produktu	Teploměr vodotěsný digitální pro Arduino Rasberry IOT
Funkce v demu	Snímání teploty
Cena za kus (bez DPH)	74 Kč

Další produkty

Tab. 6.5 Údaje o dalších produktech.

Název	Barevné diody	Arduino akustický bzučák	10cm DuPont M-F Kabely Barevné 40 žil samec samice	Rezistory 200 Ohm 0.25 W 1%
Cena za kus (bez DPH)	2 Kč	88 Kč	50 Kč	1 Kč
Funkce	Signalizace stavů	Signalizace stavů	Propojky	Odpor pro diody



Obr. 6.6 Demo bezdrátového senzoru.

6.1.2 Software

Microsoft Azure Virtual Machine je typickým příkladem cloudové služby nabízené jako distribuční model IaaS. Služba také umožňuje okamžitou instalaci operačního systému s licencí (Linux, Microsoft Windows). Pro toto demo byl zvolen operační systém Linux. Úspěšné nasazení OS do virtuálního stroje služby je otázka několika minut. Pro komunikaci s virtuálním serverem je třeba komunikační program, který vytvoří virtuální tunel mezi mým a virtuálním strojem. K tomuto účelu jsem využil volně dostupný program „Putty“ [56]. Ke komunikaci je využíván zabezpečený komunikační protokol SSH (Secure Shell). Služba je přístupná pomocí přihlašovacího příkazu a vlastního hesla. Dále už se služba jeví jako typický Linuxový operační systém, který lze ovládat příkazovou řádkou.

Instalace aplikace Node-RED probíhá pomocí několika příkazů [57]. Po jejím spuštění lze k aplikaci přistupovat pomocí webového rozhraní na adrese: <http://<přidělená-IP>:1880/>. Díky tomu, že aplikace běží v cloudové službě a má přiřazenou veřejnou IP adresu, lze k aplikaci přistupovat přes prohlížeč z jakéhokoli PC. Takto je aplikace zcela nezabezpečená a je potřeba jí okamžitě přiřadit přihlašovací údaje pro správu aplikace a pro uživatele. Node-RED aplikace pracuje na principu spojování bloků, které mají definovanou funkci a mohou představovat např. hardware, grafickou nebo matematickou funkci, či online služby. Jak jsou v mém demu bloky propojené lze vidět na Obr. 6.9. Každý blok má definovanou

činnost, kterou vykonává a každé spojení bloků představuje trasu, po které data putují. Výsledky měření se ve aplikaci graficky znázorňují viz Obr. 6.10 a zároveň jsou ukládány do lokálního souborového systému. Na levé půlce obrázku lze vidět stav, při kterém neprobíhá měření. V pravé půlce obrázku je již měření aktivní, a kromě aktuální teploty ze senzoru jsou zobrazovány a ukládány také hodnoty jako stav měření, datum a čas, či identifikace produktu.

Microsoft Azure Virtual Machines



Obr. 6.7 MA Virtual Machine, převzato z [45].

Tab. 6.6 Údaje o službě MA Virtual Machines

Název produktu	Microsoft Azure Virtual Machines
Funkce v demu	Virtuální PC s operačním systémem Linux (služba v cloudu)
Cena	486 Kč / měsíc

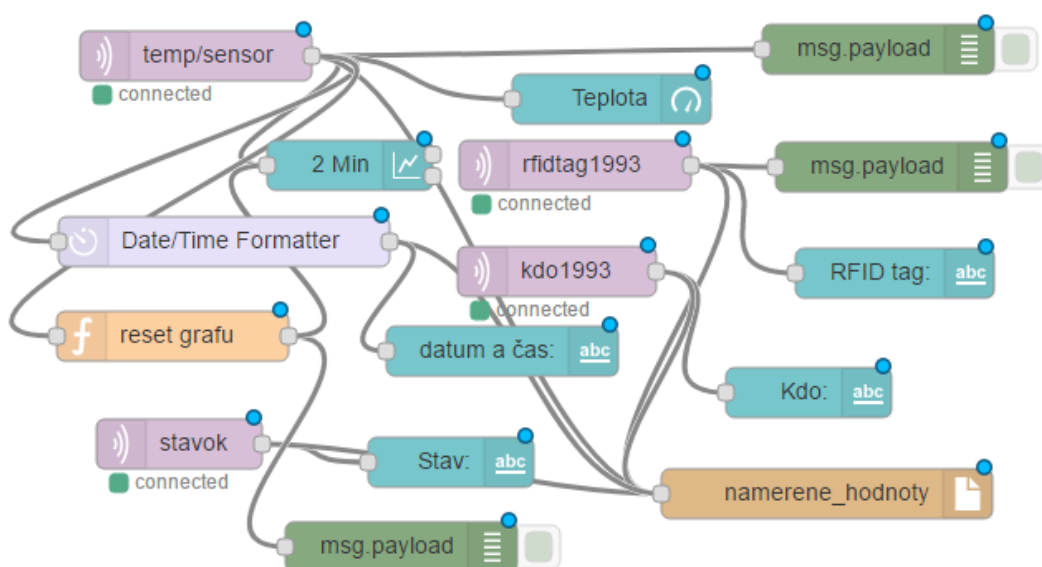
Node-RED



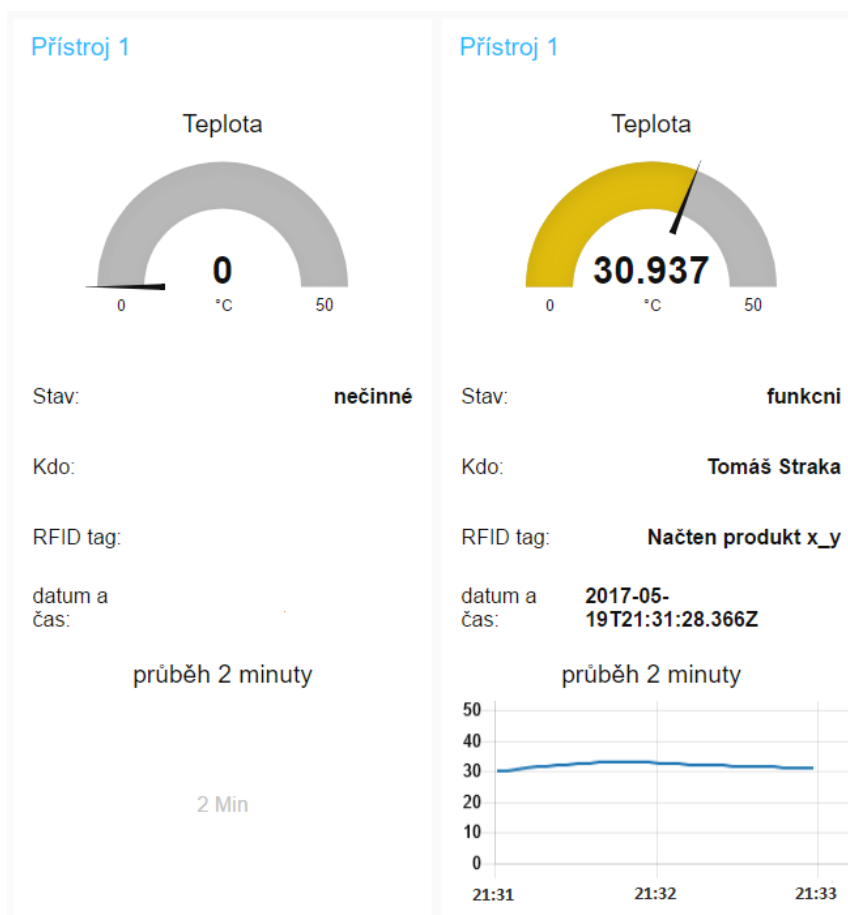
Obr. 6.8 Node-RED, převzato z [44].

Tab. 6.7 Údaje o aplikaci Node-RED

Název produktu	Node-RED
Funkce v demu	Grafické vyhodnocování a ukládání dat
Cena	0 Kč / měsíc



Obr. 6.9 Vizualní propojení jednotlivých bloků.



Obr. 6.10 Grafické znázornění průběhu měření.

6.2 Princip činnosti

Aby bylo teplotu možné měřit, je potřeba především teplotní senzor. Voděodolný senzor pro demo je napájen 5 V z desky WeMos D1, která zde zastává kromě napájecí funkce také funkci dataloggeru. Samotná deska je napájena 9 V baterií a jelikož působí jako zdroj energie pro všechny užití komponenty, tak umožňuje činnost dema bez externího napájení. Komunikace probíhá pomocí jediného vodiče, který je připojen na digitální vstup desky. Datalogger je nastaven tak, aby odečetl hodnotu teploty jednou za 2 vteřiny.

Dalším prvkem v demu je RFID čtečka, která plní funkci spouštění a ukončování měření v závislosti na přiloženém tagu. Čtečka je stejně jako senzor napájena z desky WeMos D1 (3,3 V) a ke komunikaci využívá sériové periferní rozhraní (SPI).

Ke zprovoznění celku (dále jen senzoru) musí být nejdřív splněno pravidlo, a to úspěšné připojení dataloggeru k síti Wi-Fi. Po úspěšném připojení je senzor připraven a vyčkává na vhodný tag. Lze si to představit jako zaměstnance, který přijde se senzorem ke kádince s vodou a potřebuje v ní změřit teplotu. U kádinky je tag s vnitřním označením, které je v systému spjaté s touto kádinkou. Po přiložení

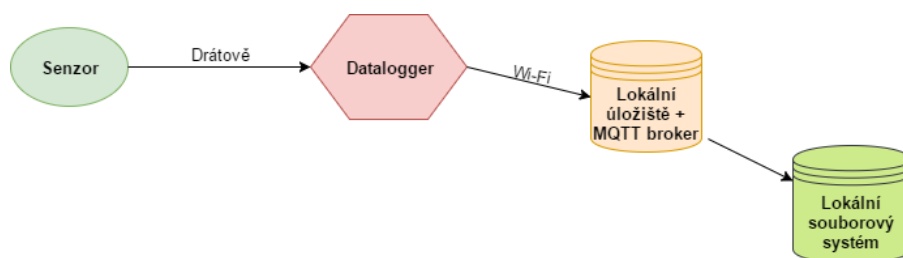
tagu k senzoru zablikají diody a ozve se zvukový signál označující úspěšný, či neúspěšný začátek měření. Po požadované době měření svým univerzálním tagem, který nosí při sobě měření zastaví a jde na další kádinku. Naměřená data tak dostanou potřebné informace typu: kdo, kde a kdy. Takto si lze představit např. 10 zaměstnanců, kteří tento úkon dělají ve stejný čas na více místech. V tu chvíli ve firmě probíhá plnohodnotné odečítání dat ze sensorové sítě.

Aby měl zaměstnanec přehled o měření, může využít aplikaci vytvořenou v softwaru Node-RED, která představuje grafické znázornění měřených dat. Tato aplikace je buď dostupná na IP adrese, která je dostupná komukoliv pomocí webového prohlížeče (řešení v cloudu), nebo na adrese, která je dostupná pouze v lokální síti firmy (řešení „On-premises“).

Rozdíl v těchto dvou řešeních je především v tom, jakým způsobem lze k datům přistupovat, jak se data z dataloggeru dostanou do aplikace a jak a kde jsou dále uloženy. Tyto rozdíly budou dále popsány v kapitolách 6.2.1 a 6.2.2. V obou případech je třeba počítat s využitím PC, přes který lze přistupovat k aplikaci a datům v uložení.

6.2.1 Demo jako lokální řešení

V tomto případě jsou data z dataloggeru posílána přes Wi-Fi do mini PC Raspberry Pi. Ten je dostatečně výkonný, aby na něm mohl běžet operační systém Linux. Na Linuxu je nainstalován software Node-RED, na kterém běží aplikace, která uvádí informace o měření a graficky znázorňuje průběh.



Obr. 6.11 Schéma činnosti demo nasazeného jako „On-premises“.

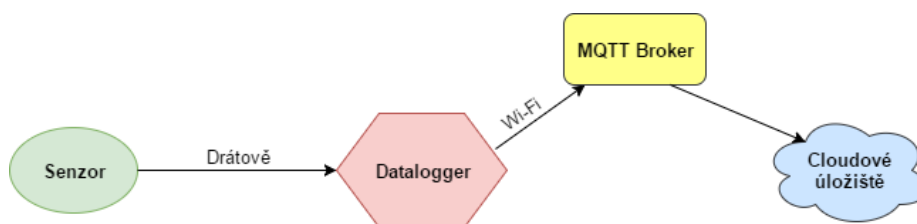
Ke komunikaci mezi dataloggerem a mini PC a také mezi mini PC a aplikací je využito komunikační protokol MQTT, který je blíže popsán v kapitole 3.1.2. Funkci publishera zastává datalogger, který data ze senzoru pod vhodným tématem (topicem) zasílá na brokera, kterým je v tomto případě mini PC. Broker data přijme a následně je přeposílá k přečtení čtenářům, tzv. subscriberům, kteří odebírají data

pod určitým tématem. Funkci subscriberů zde plní aplikace, resp. její dílčí části, které odebírají jednotlivá témata a vypisují získané hodnoty.

Celý tento proces probíhá ve vnitřní síti firmy, data tak nejsou dostupná odkudkoliv, kde se lze připojit k internetu. Toto tvrzení se však omezuje pouze na připojení pomocí známé IP adresy. V případě, že firma umožňuje zaměstnancům přístup pomocí tzv. vzdáleného přístupu (např. aplikace TeamViewer), tak jsou data stejně dostupná, jako by byl zaměstnanec na vnitřní síti. Data jsou aplikací ukládána v podobě textového souboru do lokálního úložiště na SD kartu v mini PC.

6.2.2 Demo jako řešení v cloudu

V druhém případě jsou data z dataloggeru WeMos D1 posílána přes MQTT brokera do cloudové služby. Stejně jako u řešení „On-premises“ plní funkci publishera datalogger. Změnou je však broker, kterého v tomto případě zastává online broker. Tím je webová služba CloudMQTT [59], která využívá ke své činnosti cloudové služby společnosti Amazon. Data jsou z dataloggeru zasílána na brokera a od něj jsou dále předávána subscriberům, resp. aplikaci Node-RED. Zde je oproti předešlému řešení také změna, jelikož aplikace již neběží na mini PC, ale běží na virtuálním PC s Linuxem ve službě Microsoft Azure, resp. v Microsoft Azure Virtual Machines. V tomto řešení lze Raspberry Pi zcela vynechat, jelikož neplní ani funkci brokera, ani funkci infrastruktury pro aplikaci.



Obr. 6.12 Schéma činnosti demo nasazeného v cloudu.

Data jsou také aplikací ukládána do textového souboru, avšak ten je fyzicky umístěn v serveru poskytovatele. Pro opětovné grafické zobrazení naměřených dat z textového souboru lze využít např. open source aplikaci „OpenOffice“, která je v obou případech součástí OS Linux.

6.3 Zhodnocení řešení

Nákladovost, spolehlivost a bezpečnost služby jsou hlavními faktory, kterými se firmy řídí při výběru vhodného řešení.

6.3.1 Nákladovost

Jednotlivé ceny za komponenty užití v demu lze najít v tabulkách v kapitole 6.1. V obou případech porovnávání je zahrnuta také částka za IT odborníka, který se musí starat jak o hardwarovou, tak softwarovou stránku řešení. Uvažujme opět 20 takovýchto bezdrátových senzorů a jeden PC s operačním systémem, např. Microsoft Windows 10. Jelikož je senzorů 20, u online MQTT brokera byl zvolen platební model „Keen Koala“, který je omezen na 100 připojených zařízení. PC s licenci na OS nemusí být výkonný, lze tedy uvažovat kancelářský PC s OS, obrazovkou, klávesnicí a myší v cenové relaci okolo 12 000 Kč, viz [58]. V případě firmy, která již disponuje PC s OS, lze ho z úvahy odebrat.

Varianta 1 – „On premises“

Jednorázové náklady:

- Zřízení služby + licence 0 Kč
- Nastavení služby 0 Kč
- Náklady na zřízení infrastruktury 25 481 Kč
 - 20x senzor 12 440Kč
 - Mini PC Raspberry Pi 1 041 Kč
 - PC + licence na OS 12 000 Kč

Pravidelné měsíční náklady:

- Mzda za IT odborníka 25 000 Kč / měsíc
- Poplatek za senzory + správa zařízení + monitorování 0 Kč / měsíc
- Poplatek za virtuální stroj 0 Kč / měsíc
- Náklady na infrastrukturu (elektřina, prostor atd.) 288 Kč / měsíc
- Servisní náklady (výměna baterií, poškozené součástky) 2 400 Kč / měsíc

Náklady za první rok: 357 737 Kč

Varianta 2 – Cloud

Jednorázové náklady:

- Zřízení služby + licence 0 Kč
- Nastavení služby 0 Kč
- Náklady na zřízení infrastruktury 24 440 Kč
 - 20x senzor 12 440 Kč
 - PC + licence na OS 12 000 Kč

Pravidelné měsíční náklady:

- Mzda za IT odborníka 25 000 Kč / měsíc
- Poplatek za senzory + správa zařízení + monitorování 494 Kč / měsíc
- Poplatek za virtuální stroj 486 Kč / měsíc
- Náklady na infrastrukturu (elektřina, prostor atd.) 297 Kč / měsíc
- Servisní náklady (výměna baterií, poškozené součástky) 2400 Kč / měsíc

Náklady za první rok: 368 564 Kč

Náklady na elektřinu lze spočítat z odhadovaných hodnot odběru jednotlivých komponent. Uvažujme, že PC společně s obrazovkou odebírá cca 100 W, což je přibližně 72 KW / měsíc. Při částce 4 Kč / KW vychází náklady 280 Kč / měsíc. V druhém příkladu je zahrnuto Raspberry Pi, které málo kdy přesáhne hranici 3 W. Měsíční náklad je tak přibližně 9 Kč. To vše za předpokladu, že tyto komponenty pracují 24/7. Bezdrátový senzor není navržen tak, aby byl co nejúspornější, a proto je třeba uvažovat výměnu baterií jednou za 14 dní. Při průměrné ceně 60 Kč za 9 V baterii dělají náklady na 20 senzorů měsíčně přibližně 2400 Kč [58]. Zbylé poplatky vychází z cen uvedených v tabulkách u jednotlivých produktů.

Částky obou variant jsou podobné. V průběhu několika dalších let by měly částky růst přibližně stejně, jelikož v řešení není žádná součástka výrazně dražší, a proto se neuvažují ani vyšší servisní náklady a náklady na infrastrukturu. V případě rozšiřování senzorové sítě u cloudového řešení by se mohly zvýšit poplatky za MQTT brokeru.

6.3.2 Spolehlivost

Cloudové řešení je závislé na internetu. To znamená, že je závislé na rychlosti přenosu a rychlosti odezvy internetového připojení. Microsoft Azure garantuje ve SLA min. dostupnost 99,95 %, což je u tak velkého poskytovatele poměrně standardní dostupnost. Oproti tomu lokální řešení nevyžaduje propojení s okolním světem a může fungovat jen na lokální síti. Odezva u lokální sítě se pohybuje v řádu jednotek milisekund, kdežto u cloudového řešení jsou to desítky, ve vzdálených oblastech až stovky milisekund.

Po stránce výkonu nebyla ani u jednoho řešení zjištěna nedostatečnost. Node-RED je založen na frameworku Node.js, který je single-threaded (jednovláknový), proto není třeba využívat hardware s více jádry. Ani u jednoho řešení nebyl zaznamenán pád aplikace.

V lokálním řešení je výkon omezen především hardwarem v Raspberry Pi. Tento výkon lze navýšit pouze přidáním dalšího mini PC. Microsoft Azure nabízí desítky různých modelů virtuálních strojů, které se liší např. velikostí paměti RAM, počty jader a kapacitou disků, ale také výraznými rozdíly v cenách, které se pohybuje od 840 Kč / měsíc do zhruba 13 000 Kč / měsíc.

Z hlediska životnosti byly použity součástky, které nevykonávají sami žádnou mechanickou činnost, a kromě Raspberry Pi, které potřebuje pasivní, nebo aktivní chladič, nemají problémy s přehříváním. Odhadem by celý senzor i mini PC mohli vydržet 2–5 let podle četnosti užívání. Při porovnání mini PC a cloudové služby na kterých běží aplikace lze však říct, že s počtem serverů, kterými disponuje poskytovatel, je jistota dlouhodobé činnosti především u cloudu.

6.3.3 Bezpečnost

Jedno z témat bezpečnosti je bezpečnost přenosu dat. Data mohou být během své cesty do lokálního úložiště, případně do cloudu ztracena či odcizena. Od senzoru do dataloggeru je signál přenášen pomocí vodiče. Tím je sníženo nebezpečí odposlechnutí a ztrát, jako by tomu mohlo být např. v případě přenosu bezdrátovou technologií. Dále už se bezpečnost obou řešení liší. Protokol MQTT, který je užíván, je čistě textový, proto je komunikace bez použití SSL, nebo TLS zcela nešifrovaná [46]. Knihovna „PubSubClient.h“, která byla použita pro komunikaci mezi dataloggerem a MQTT brokerem možnost šifrování zatím neposkytuje. V případě lokálního řešení se to jeví jako přijatelné, jelikož jsou zaslány čistě číselné hodnoty, případně jméno a datum zaměstnance, a tyto hodnoty běžně nespádají do tajných

informací firmy. V případě cloudové služby se to však jeví jako problémové ve chvíli, kdy jsou data na MQTT brokera zasílána s přihlašovacími údaji k účtu. Jedním z řešení je využít jinou knihovnu podporující TTL/STL, nebo data posílat nejprve stejně jako v lokálním řešení na MQTT brokera v Raspberry Pi a až z aplikace Node-RED, která šifrování podporuje, je posílat na online brokera a z něho do aplikace běžící v cloudu. Tím by měla být zajištěna nečitelnost dat v případě odposlechnutí.

V případě fyzického odcizení dat, v bezpečnosti jasně vyhrává cloudové řešení. U mini PC se data ukládají na SD kartu, která je vyjímatelná, a tak v případě, že se k tomuto zařízení dostane neoprávněná osoba, mohou být nejen data, ale i celá aplikace odcizeny. V takovém případě by bylo vhodné, aby IT oddělení firmy dělalo pravidelné zálohy i na jiná média. Jak už bylo řečeno dříve, cloudoví poskytovatelé si zakládají na kvalitním zabezpečení pro data zákazníků. Z toho vyplývá, že pokud jsou data bezpečně dopravena do cloudové služby, tak je o jejich bezpečnost zajištěna v podstatně větší kvalitě, než by tomu bylo lokálně u firmy.

Samotná aplikace v Node-RED je rozdělena na vývojové prostředí a uživatelské prostředí, ve kterém se graficky znázorňuje proces měření. Obě tyto prostředí jsou zabezpečené autorizačními údaji. Aplikace nabízí 2 modely oprávnění, které lze aplikovat jak na vývojové, tak uživatelské prostředí. Jednotlivé modely umožňují buď zápis a čtení dat (např. IT odborník, zaměstnanec vyplňující hodnoty) nebo jen čtení (např. zaměstnanec kontrolující průběh měření). Stejně tak přístupy do cloudové služby a Linux systému běžícího na mini PC jsou chráněny autorizačními údaji. V dataloggeru neběží žádný operační systém a programovatelný je pouze pomocí USB, proto není třeba uvažovat jinou ochranu kromě odcizení.

Kromě možného odcizení dat je tu také hrozba napadení systému malwarem, či DDOS útoky na aplikaci. Microsoft Azure ve své dokumentaci tvrdí, že mají zajištěnou vysokou úroveň bezpečnosti svých služeb proti DDOS útokům [47]. Pokud lokální řešení využívá pouze lokální síť bez přístupu do internetu, tak je od DDOS útoku ušetřeno. V případě, že služba nabízená jako IaaS (tento případ cloudového řešení), kdy se IT oddělení stará o správu operačního systému, měla by být zajištěna ochrana systému proti malwarem a to i přesto, že Microsoft Azure poskytuje ochranu v podobě antimalwaru. Lokální řešení může být náchylné na malware nejen z internetu, ale také od zaměstnanců, kteří si nějaký vir mohou přinést s sebou na přenosovém mediu bez jejich vědomí.

7. Závěr

Tvorba této bakalářské práce mi přinesla mnoho nových poznatků v oblasti internetu věcí a cloudových služeb. Během psaní teoretické části jsem se nesetkal s problémy s pojenými s nedostatkem literatury, jelikož se jedná o témata, kterými se zabývalo již mnoho knižních autorů a publicistů technických článků. V druhé kapitole práce jsem se zaměřil na definování významu spojení „cloudová služba“ a s ní spojené termíny jako jsou modely nasazení, či distribuční modely. Zaměřil jsem se také na charakteristické vlastnosti služeb, díky kterým se jeví jejich využití vhodné pro firmy a koncem kapitoly jsem se zaměřil na bezpečnost služeb, jelikož je to jedna z hlavních věcí, ke které firmy přihlížejí při volbě poskytovatele.

Ve třetí kapitole jsem se věnoval definování pojmu „senzorová síť“. Postupně jsem popisoval jednotlivé prvky, které musí každá sensorová síť mít, aby byla zajištěna její funkčnost. Důraz jsem kladl na způsob propojení senzorů s dataloggery, jelikož sensorová síť není jen bezdrátová, jak se často v dnešní literatuře objevuje.

Čtvrtou kapitolu jsem věnoval popisu ERP a DMS systémů, které dnes tvoří neodmyslitelnou část mnoha firem. Zaměřil jsem se především na charakteristické vlastnosti těchto systémů typu cloud, jelikož se jedná o vlastnosti, které lákají firmy na přechod od tužky a papíru ke komplexnímu řešení.

V praktické části jsem se nejprve zaměřil na průzkum trhu s cloudovými službami. Ve spojitosti se sensorovými sítěmi jsem vypracoval tabulky s přehledem komerčních a open-source IoT cloudů a vypsali jsem vlastnosti služeb, které by podle mě mohly pomoci zákazníkovi s výběrem vhodného poskytovatele. Také jsem vytvořil tabulkový přehled pro ERP a DMS systémy. Tyto tabulky jsou umístěny na konci dokumentu a při zhodnocování v kapitole 5 jsem z nich čerpal.

Pátá kapitola je zaměřena na porovnání několik vybraných služeb z těchto tabulek. Jak jsem již avizoval v úvodu, snažil jsem se zaměřit především na porovnání služeb běžících na serveru poskytovatele a služeb s možností běhu na lokálním serveru firmy. Zaměřil jsem se především na jejich porovnání z hlediska nákladovosti, spolehlivosti a bezpečnosti.

V šesté kapitole je popisováno demo, které jsem pro tuto práci vytvořil. Moje snaha byla taková, aby mělo demo dvě varianty, jednu s využitím cloudové služby a jednu s využitím lokálního mini PC. Obě tyto varianty se mi podařilo zrealizovat a poté jsem obě varianty zhodnotil na základě nákladovosti, spolehlivosti a také bezpečnosti.

Z mého pohledu jsou cloudové služby téma, které jen tak neutichne, jelikož je v nich potenciál, který se dle mého názoru zatím zcela nerozvinul. Věřím, že tato práce pomůže lidem, kteří se o tuto problematiku zajímají a případně postrčí firmy, které o cloudových službách přemýšlí, ale nemají dostatečné informace, co využití těchto služeb přináší.

Literatura a zdroje

[1] BURIAN, Pavel. Internet inteligentních aktivit. Praha: Grada, 2014. Průvodce (Grada). ISBN 978-80-247-5137-5.

[2] MICHALEC, Libor. Velký přehled cloudů pro IoT. In: vyvoj.hw.cz [online]. HW server s.r.o., 2017. [cit. 28.04.2017]. Dostupné z: <http://vyvoj.hw.cz/velky-prehled-cloudu-pro-iot.html>

[3] DAVIDSON, Michelle. Cloud usage: Microsoft Azure the most popular IaaS provider. In: SiliconANGLE [online]. SiliconANGLE Media, Inc., 2016. [cit. 28.04.2017]. Dostupné z: <https://siliconangle.com/blog/2016/03/11/cloud-usage-microsoft-azure-the-most-popular-iaas-provider/>

[4] BEZPALEC, Pavel. Nové trendy v elektronických komunikacích Cloud Computing. In: Publi.cz [online]. Code Creator, s.r.o., 2014. [cit. 28.04.2017]. Dostupné z: <https://publi.cz/books/230/Impresum.html>

[5] VAŠÍČKOVÁ, Petra. Integrace cloudových a on-premise řešení do jedné platformy iPaaS. In: SystemOnline [online]. CCB spol. s r.o., 2014. [cit. 28.04.2017]. Dostupné z: <https://www.systemonline.cz/virtualizace/integrace-cloudovych-a-on-premise-reseni.htm>

[6] Co je cloud computing? Průvodce pro začátečníky [online]. Microsoft, © 2017. [cit. 29.04.2017]. Dostupné z: <https://azure.microsoft.com/cs-cz/overview/what-is-cloud-computing/>

[7] Co je veřejný cloud? [online]. Aira GROUP, s.r.o., © 2016 . [cit. 29.04.2017]. Dostupné z: <http://www.sprava-site.eu/verejny-cloud/>

[8] Co je privátní cloud? [online]. Aira GROUP, s.r.o., © 2016 . [cit. 29.04.2017]. Dostupné z: <http://www.sprava-site.eu/privatni-cloud/>

[9] Co je komunitní cloud? [online]. Aira GROUP, s.r.o., © 2016 . [cit. 29.04.2017]. Dostupné z: <http://www.sprava-site.eu/komunitni-cloud/>

[10] Co je hybridní cloud? [online]. Aira GROUP, s.r.o., © 2016 . [cit. 30.04.2017]. Dostupné z: <http://www.sprava-site.eu/hybridni-cloud/>

- [11] MELL, Peter a Timothy GRACE. The NIST Definition of Cloud Computing. In: NIST Page [online]. National Institute of Standards and Technology, 2011. [cit. 30.04.2017]. Dostupné z: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>
- [12] What is Broad Network Access? [online]. Techopedia Inc., © 2017. [cit. 30.04.2017]. Dostupné z: <https://www.techopedia.com/definition/28785/broad-network-access>
- [13] Datové centrum – Slovník pojmů [online]. NWT a.s., © 1992. [cit. 01.05.2017]. Dostupné z: <https://www.nwt.cz/it-telekomunikace/sprava-it-outsourcing/datove-centrum-slovník-pojmu/>
- [14] Internet věcí - Pavel Pohanka [online]. Pavel Pohanka, © PP 2015. [cit. 01.05.2017]. Dostupné z: <http://i2ot.eu/internet-of-things/>
- [15] EVANS, Dave. The Internet of Things, How the Next Evolution of the Internet Is Changing Everything. In: Cisco - Global Home Page [online]. Cisco Internet Business Solutions Group, 2011. [cit. 01.05.2017]. Dostupné z: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
- [16] VRŇATA, Martin a Filip VYSLOUŽIL. Senzory a senzorové systémy [online přednáška]. Praha: VŠCHT, UFMT. [cit. 25.05.2017]. Dostupné z: https://vscht.cz/ufmt/cs/pomucky/vrnatam/docs2/sss_1pred.ppt
- [17] Gartner IT Glossary [online]. Gartner, Inc. and/or its Affiliates, © 2017. [cit. 02.05.2017]. Dostupné z: <http://www.gartner.com/it-glossary/?s=internet+of=things>
- [18] CORSARO, Angelo. Architecting IoT Systems. In: Prismtech [online]. Primstech, 2014. [cit. 02.05.2017]. Dostupné z: https://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiSkN_tmdHTAhUDESvKHWbWD9IQFgglMAA&url=http%3A%2F%2Fwww.prismtech.com%2Fsf-lead-passthru%2F1730%2Fpdf%3Furl%3Dsites%2Fdefault%2Ffiles%2Fdocuments%2FArchitecting-IoT-Systems-Vortex.pdf&usq=AFQjCNGtGfredNE_4piO-MkPPqffEIKu2w

[19] KŘIŽANOVSKÝ, Pavel. Fog Computing aneb Rozhodování blíže zdroji. In: SystemOnLine [online]. CCB spol. s r.o., 2015. [cit. 02.05.2017]. Dostupné z: <https://www.systemonline.cz/clanky/fog-computing-aneb-rozhodovani-blize-zdroji.htm>

[20] Immer noch wolkig - aktuelle Trends bei Cloud Services [online]. DocPlayer.org. [cit. 02.05.2017]. Dostupné z: <http://docplayer.org/696365-Immer-noch-wolkig-aktuelle-trends-bei-cloud-services.html>

[21] JLAJ. Foggy about "Fog Computing"?. In: IoT Labs [online]. IoT Labs, © 2017. [cit. 02.05.2017]. Dostupné z: <http://iot-labs.com.my/2016/03/foggy-about-fog-computing/>

[22] BELL, Charles. Beginning sensor networks with Arduino and Raspberry Pi [online]. New York: Springer Science+Business Media New York, 2013. [cit. 04.05.2017]. ISBN 978-1-4302-5825-4. Dostupné z: http://www.hondosackett.com/yabb/Books/Beginning_Sensor_Networks_with_Arduino_and_Raspberry_Pi.pdf

[23] BELL, Charles. Beginning sensor networks with Arduino and Raspberry Pi. [online]. New York: Springer Science+Business Media New York, 2013. [cit. 04.05.2017]. ISBN 978-1-4302-5825-4. Dostupné z: http://www.hondosackett.com/yabb/Books/Beginning_Sensor_Networks_with_Arduino_and_Raspberry_Pi.pdf

[24] MAIXNER, Ladislav. Mechatronika: učebnice. Brno: Computer Press, 2006. ISBN 8025112993.

[25] VOJÁČEK, Antonín. Základní úvod do oblasti internetu věcí (IoT). In: Automatizace.hw.cz. [online]. HW server s.r.o., 2016. [cit. 04.05.2017]. Dostupné z: <http://automatizace.hw.cz/zakladni-uvod-do-oblasti-internetu-veci-iot.html>

[26] Networking for WordPress Administrators [online]. Feedjit Inc., © 2017. [cit. 04.05.2017]. Dostupné z: <https://www.wordfence.com/learn/networking-for-wordpress-administrators/>

[27] VOJÁČEK, Antonín. Jak na Modbus-TCP/RTU komunikaci v PLC IDEC SmartAxis Lite/Pro? In: Automatizace.hw.cz. [online]. HW server s.r.o., 2016. [cit. 04.05.2017]. Dostupné z: <http://automatizace.hw.cz/komponenty-plc-a-prumyslova-pc/jak-na-modbus-tcprtu-komunikaci-v-plc-idec-smartaxis-litepro.html>

- [28] VOJÁČEK, Antonín. Základní úvod do oblasti internetu věcí (IoT). In: Automatizace.hw.cz. [online]. HW server s.r.o., 2016. [cit. 04.05.2017]. Dostupné z: <http://automatizace.hw.cz/zakladni-uvod-do-oblasti-internetu-veci-iot.html>
- [29] FERNANDEZ-VALLEJO, Montserrat a Manuel LOPEZ-AMO. Optical Fiber Networks for Remote Fiber Optic Sensors. In: National Center for Biotechnology Information [online]. National Center for Biotechnology Information, U.S. National Library of Medicine, 2012. [cit. 04.05.2017]. Dostupné z: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3355392/>
- [30] ŘEPA, Václav. Podnikové procesy: procesní řízení a modelování. 2. aktualiz. a rozš. vyd. Praha: Grada, 2007. ISBN 9788024722528.
- [31] GRASSEOVÁ, Monika, Radek DUBEC a Roman HORÁK. Procesní řízení ve veřejném sektoru: teoretická východiska a praktické příklady. Brno: Computer Press, 2008. ISBN 9788025119877.
- [32] Podnikový proces (Business process). In: ManagementMania.com [online]. Wilmington (DE) 2011-2017, 12.12.2016 [cit. 08.05.2017]. Dostupné z: <https://managementmania.com/cs/business-process-podnikovy-proces>
- [33] BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy: podnik v informační společnosti. 2. výrazně přeprac. a rozš. vyd. Praha: Grada, 2008. ISBN 9788024722795.
- [34] Historie ERP systémů. In: ERP SYSTÉMY [online]. ERP SYSTÉMY – Instalace, pořízení a provozování ERP systémů, © 2017 [cit. 08.05.2017]. Dostupné z: <http://erp-systemy.cz/historie-erp-systemu/>
- [35] Top 5 ERP Software Systems [online]. ERP Software. [cit. 08.05.2017]. Dostupné z: <http://www.erpsoftware360.com/erp-software.htm>
- [36] IQDoc diagram. In: Icontio [online]. Icontio CR s.r.o., © 2016. [cit. 09.05.2017]. Dostupné z: <http://www.icontio.com/media/1371/iqdoc-diagram.png>
- [37] FLIESSIG, Stanislav. DMS: systémy pro správu a oběh dokumentů. In: SystemOnLine [online]. CCB spol. s r.o., 2014. [cit. 09.05.2017]. Dostupné z: <https://www.systemonline.cz/clanky/dms-systemy-pro-spravu-a-obeh-dokumentu.htm>

- [38] MARTÍNEK, Štěpán. Document Management System představuje moderní trend v práci s dokumenty. In: SystemOnLine [online]. CCB spol. s r.o., 2012. [cit. 10.05.2017]. Dostupné z: <https://www.systemonline.cz/sprava-dokumentu/dms-moderni-trend-v-praci-s-dokumenty.htm>
- [39] EU. Definice středních a malých podniků. In: Úřední věstník Evropské unie [online]. 2014, L 187 /70-72. [cit. 15.05.2017]. Dostupné z: http://www.uohs.cz/download/Sekce_VP/VP_update/definice-malych-a-strednich-podniku-2014.pdf
- [40] DUŠEK, Martin a Michal MAZANEC. Fyzikální principy optických a optovláknových snímačů. In: Centrum pro rozvoj výzkumu pokročilých řídicích a senzorických technologií [online]. Vzdělávání pro konkurenceschopnost, 2012. [cit. 15.05.2017]. Dostupné z: http://www.crr.vutbr.cz/system/files/brozura_06_1206.pdf
- [41] JAVŮREK, Karel. Cloud od Amazonu měl několik hodin problémy, způsobilo to výpadky velkých webů a aplikací. In: Connect.cz [online]. Connect.cz, 2017. [cit. 17.5.2017]. Dostupné z: <https://connect.zive.cz/bleskovky/cloud-od-amazonu-mel-nekolik-hodin-problemy-zpusobilo-to-vypadky-velkych-webu-a-aplikaci/sc-321-a-186420/>
- [42] KOVÁŘ, Pavel. Odvrácena strana cloudu: data v rukou třetích stran. In: Connect.cz [online]. Connect.cz, 2012. [cit. 17.5.2017]. Dostupné z: <https://connect.zive.cz/clanky/odvracena-strana-cloudu-data-v-rukou-tretich-stran/sc-320-a-162599/default.aspx>
- [43] VELKOOBCHOD, MALOOBCHOD S ARDUINEM - Arduino-shop.cz. [online]. ECLIPSE s.r.o., © 2017. [cit. 18.05.2017]. Dostupné z: <http://arduino-shop.cz/>
- [44] node-red [online]. GitHub, Inc., © 2017 [cit. 18.05.2017]. Dostupné z: <https://github.com/node-red>
- [45] vFlex - Microsoft Azure [online]. S3 Consulting Ltd., © 2015 [cit. 18.05.2017]. Dostupné z: <http://www.thinks3.co.uk/vflex-cloud-solution/microsoft-azure/>
- [46] VOJÁČEK, Antonín. IoT MQTT prakticky v automatizaci - 1.díl – úvod. In: Automatizace.hw.cz. [online]. HW server s.r.o., 2017. [cit. 19.05.2017]. Dostupné z: <http://automatizace.hw.cz/iot-mqtt-prakticky-v-automatizaci-1-dil-uvod.html>

[47] Microsoft Azure Network Security. In: Microsoft.com [online]. Microsoft, 2014. [cit. 19.05.2017]. Dostupné z: http://download.microsoft.com/download/c/a/3/ca3fc5c0-ece0-4f87-bf4b-d74064a00846/azurenetworksecurity_v2_oct2014.pdf

[48] KUBEŠ, Radek. Cloudové služby na všech frontách. In: CIO Business World.cz [online]. IDG Czech Republic, a. s., 2014. [cit. 20.05.2017]. Dostupné z: <http://businessworld.cz/analyzy/cloudove-sluzby-na-vsech-frontach-12036>

[49] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4. aktualiz. a rozš. vyd. Praha: Grada, 2013. ISBN 9788024746449.

[50] MARŠÁLEK, Leoš. Optická vlákna. In: Goronet [online]. VŠB - Technická univerzita Ostrava, 2006. [cit. 20.05.2017]. Dostupné z: <http://goro.czweb.org/download/interest/vlakna.pdf>

[51] VOJÁČEK, Antonín. Optické senzory přiblížení - obecný popis. In: Automatizace.hw.cz. [online]. HW server s.r.o., 2005. [cit. 20.05.2017]. Dostupné z: <http://automatizace.hw.cz/clanek/2005121901>

[52] IoT Starter Kit: podpora vývoje bezdrátových aplikací pro IoT. In: Živě.cz [online]. Microsoft TechNet, 2017. [cit. 21.05.2017]. Dostupné z: <http://www.zive.cz/clanky/iot-starter-kit-podpora-vyvoje-bezdratovych-aplikaci-pro-iot/sc-3-a-186529/default.aspx>

[53] Nová DIN 66399... nové stupně utajení [online]. UNIVOX s.r.o., 2014. [cit. 22.05.2017]. Dostupné z: <http://www.univox.cz/nova-din-66399-nove-stupne-utajeni/t-189/>

[54] DVOŘÁK, Milan. Optické senzory. In: Kompozity.info [online]. Kompozity.info. [cit. 22.05.2017]. Dostupné z: http://www.kompozity.info/clanky/optik_ten/opticke_senzory.pdf

[55] CloudPing.info [online]. Michael Leonhard, © 2010 - 2017. [cit. 23.05.2017]. Dostupné z: <http://www.cloudping.info/>

[56] Download PuTTY - a free SSH and telnet client for Windows. [online]. Simon Tatham. [cit. 23.05.2017]. Dostupné z: <http://www.putty.org/>

- [57] Node-RED: Running on Microsoft Azure [online]. JS Foundation. [cit. 23.05.2017]. Dostupné z: <https://nodered.org/docs/platforms/azure>
- [58] Alza.cz - největší obchod s počítači a elektronikou [online]. Alza.cz a.s., © 1994 – 2017. [cit. 23.05.2017]. Dostupné z: <https://www.alza.cz/>
- [59] CloudMQTT [online]. Amazon Web Services, Inc. or its affiliates. [cit. 23.05.2017]. Dostupné z: <https://www.cloudmqtt.com/>
- [60] Microsoft Dynamics 365 Server hardware requirements. In: Microsoft TechNet [online]. Microsoft, 2016. [cit. 23.05.2017]. Dostupné z: <https://technet.microsoft.com/cs-cz/library/hh699840.aspx>
- [61] SoftGate, s.r.o. | Počítačové kurzy a firemní školení, ECDL testování [online]. SoftGate, s.r.o., © 2016. [cit. 23.05.2017]. Dostupné z: <http://softgate.cz/>
- [62] CRM On-Premises Licensing and Pricing Information [online]. FMT Consultants, LLC., © 2017. [cit. 23.05.2017]. Dostupné z: <https://www.fmtconsultants.com/solutions/customer-engagement-crm/crm-licensing-deployment/crm-on-premises/>
- [63] Cloud Machine – Pricing [online]. Oracle and/or its affiliates, © 1995, 2017. [cit. 24.05.2017]. Dostupné z: <https://cloud.oracle.com/opc/cloud-machine/pricing>
- [64] SNOVER, Jeffrey. Microsoft Azure Stack: Hardware requirements. In: Hybrid Cloud Blog [online]. Microsoft, © 2017. [cit. 24.05.2017]. Dostupné z: <https://blogs.technet.microsoft.com/hybridcloud/2015/12/21/microsoft-azure-stack-hardware-requirements/>
- [65] Microsoft Azure: Cloudová výpočetní platforma a služby [online]. Microsoft, © 2017. [cit. 24.05.2017]. Dostupné z: <https://azure.microsoft.com/cs-cz/>
- [66] Azure Stack – Azure v místním prostředí [online]. Microsoft, © 2017. [cit. 24.05.2017]. Dostupné z: <https://azure.microsoft.com/cs-cz/overview/azure-stack/>
- [67] Microsoft Dynamics 365—ERP and CRM Business Software [online]. Microsoft, © 2017. [cit. 24.05.2017]. Dostupné z: <https://www.microsoft.com/en-us/dynamics365/home>

- [68] Microsoft Dynamics 365 (On-Premises), Enterprise edition [online]. Microsoft, © 2016. [cit. 24.05.2017]. Dostupné z: https://download.microsoft.com/documents/en-us/dynamics365/pricing/Dynamics_365_On-Premises_Enterprise_edition_Licensing_Guide_December_2016.pdf
- [69] Informace o cenách – IoT Hub [online]. Microsoft, © 2017. [cit. 24.05.2017]. Dostupné z: <https://azure.microsoft.com/cs-cz/pricing/details/iot-hub/>
- [70] Dynamics 365 pricing [online]. Microsoft, © 2017. [cit. 24.05.2017]. Dostupné z: <https://www.microsoft.com/en-us/dynamics365/pricing>
- [71] Porovnání všech produktů Microsoft Office [online]. Microsoft, © 2017. [cit. 24.05.2017]. Dostupné z: <https://products.office.com/cs-cz/compare-all-microsoft-office-products?tab=2>
- [72] ZOZEI - Optoelektronické součástky [online]. SŠSE Brno, © 2012 - 2017. [cit. 25.05.2017]. Dostupné z: <http://zozei.sssebrno.cz/optoelektronicke-soucastky/>
- [73] M-Files – Document Management System [online]. Digital Resources a.s.. [cit. 25.05.2017]. Dostupné z: <http://www.e-dms.cz/>
- [74] [74] Data Logger [online]. OMEGA Engineering, © 2003-2017. [cit. 25.05.2017]. Dostupné z: <http://www.omega.com/prodinfo/dataloggers.html>

Tab. 7 Komerční cloudové služby 1/2.

Název	Microsoft Azure	Google Cloud Platform	Oracle cloud	IMB Bluemix	GE Predix
Webová stránka [URL]	https://azure.microsoft.com/	https://cloud.google.com/	https://cloud.oracle.com/	https://www.ibm.com/cloud-computing/bluemix/	https://www.predix.io/
Free-trial	Ano	Ano	Ano	Ano	Ano
Ceny	Free: zdarma, max. 8000 zpráv/den/jednotka/měsíc S1: 50\$/jednotka, max. 400 000 zpráv/den/jednotka/měsíc S2: 500\$/jednotka, max. 6 000 000 zpráv/den/jednotka/měsíc S3: 5000\$/jednotka, max. 300 000 000 zpráv/den/jednotka/měsíc	Cena za místo v cloudu: cca 0,2\$/GB	210Kč/hodina výpočetního výkonu cloudové služby	Lite: zdarma, max. 20 jednotek, max. 100MB/zařízení/měsíc Standard: Lite + 0,001\$/MB navíc, neomezeno jednotek Advance security: Standard + 0,0013\$/MB navíc, více služeb	Ceny dle množství využívaných služeb
Platformy	Linux, Windows, Android	Linux, Mac OS X, Windows	Android, Windows, iOS	Android, iOS	-
Jazyky	C#, C, Java, Python, Node.js, .NET	Go, Java, .NET, Objective-C, Python, Ruby, PHP	Java, Javascript	Java, Node.js, Embedded C, Python, Go	Java, Node.js, Python, Ruby
Protokoly	AMQP, HTTPS, MQTT	HTTP	HTTP, MQTT	HTTP, MQTT	Modbus, MQTT, HTTP, WebSockets, OPC-UA
Min. garantovaná dostupnost	99,95 %	99,95 %	99,9 %	99,95 %	-
Základní kit	Ano	Ano	Ne	Ne	Ano
Možnost připojit vlastní HW	Ano	Ano	Ano	Ano	Ano
Umístění ve vlastním serveru (On-premises)	Ano	-	Ano	Ano	-
Oblasti umístění dat	Jihovýchodní Asie, Jihovýchodní Austrálie, Severní Evropa, Středozápad USA, USA – východ, USA – západ, Východní Asie, Východní Austrálie, Východní Japonsko, Západní Evropa	Západní Evropa, Střední Amerika, Východní Amerika, Severovýchodní Asie-Tichomoří	Severní Amerika, Jižní Amerika, Evropa, Asie a Tichomoří	Sydney, Německo, Spojené království, Jižní Amerika	-
Možnost volby umístění dat	Ano	Ano	Ano	Ano	-

[-] Příslušné informace nebylo možno zjistit z dostupné dokumentace

Tab. 8 Komerční cloudové služby 2/2.

Název	Amazon Web Services	ThingWorx	Samsung ARTIK cloud	SAP HANA	Salesforce IoT cloud
Webová stránka [URL]	https://aws.amazon.com/	https://www.thingworx.com/	https://artik.cloud/	https://hana.sap.com/	http://www.salesforce.com/iot-cloud
Free-trial	Ano	Ano	Ano	Ano	Ano
Ceny	Ceny za počet přenesených zpráv (Evropa): 5\$/1 000 000 zpráv	-	Hobbyist: zdarma, max. zpráv 150/den/jednotka Startup: 0,75\$/jednotka/měsíc, max. zpráv 1500/den/jednotka Business: 2\$/jednotka/měsíc, max. zpráv 10 000/den/jednotka Growth: 6\$/jednotka/měsíc, max. zpráv 100 000/den/jednotka	Pro vývojáře: Zdarma Pro středně velké podniky: 23€/uživatel/měsíc pro velké společnosti: 1500€/měsíc	Starter: 25\$/uživatel/měsíc, až pro 5 uživatelů Professional: 75\$/uživatel/měsíc, neomezeno uživatelů Enterprise: 150\$/uživatel/měsíc, pro potřeby podnikání Unlimited: 300\$/uživatel/měsíc, neomezené služby
Platformy	Android, iOS, Arduino Yún, Windows	Android, iOS	iOS, Mac OS X, Android	Linux, Mac OS X, Windows	-
Jazyky	Java, Ruby, Python, PHP, Node.js, .NET	C, Java, .NET	Java, Objective-C, Python, Ruby, PHP, Javascript, Swift, C#	-	Apex, Ruby, Java, Python, PHP, Node.js
Protokoly	HTTP, WebSockets, MQTT	WebSockets (MQTT, CoAP jako extension)	HTTP, WebSockets, MQTT, CoAP	HTTP, WebSockets, SMTP, RFC	HTTP
Min. garantovaná dostupnost	99,95 %	-	-	99,5 %	-
Základní kit	Ano	Ne	Ne	Ne	Ne
Možnost připojit vlastní HW	Ano	Ano	Ano	Ano	Ano
Umístění ve vlastním serveru (On-premises)	-	Ano	Ne	Ano	Ne
Oblasti umístění dat	Východní Amerika, Západní Amerika, Jižní Amerika, Evropa, Asie a Tichomoří	-	Amerika	Severní Amerika, Evropa, Tichomoří nebo využívají cloudy AWS a Microsoft Azure	Severní Amerika, Evropa, Asie a Tichomoří
Možnost volby umístění dat	Ano	-	Ne	-	Ano
[-] Příslušné informace nebylo možno zjistit z dostupné dokumentace					

Tab. 9 České komerční cloudové služby.

Název	Qline a.s.	Enectiva	FlowBox	mySCADA
Webová stránka [URL]	http://www.qline.cz/cs/internet-veci/	https://www.enectiva.cz/cs/iot/	http://flowbox.cz/	https://www.myscada.org/
Free-trial	Ne	Ne	Ne	Ano
Ceny	-	-	-	-
Platformy	Windows	-	-	Windows, Android, Mac OS X, iOS, Linux
Jazyky	-	Java, Javascript, Python, C#, PHP	-	-
Protokoly	Modbus, ARNEP, M-BUS	HTTP	-	HTTP(S), MQTT, Modbus, OPC UA
Min. garantovaná dostupnost	-	-	-	-
Základní kit	Ne	Ne	Ne	Ne
Možnost připojit vlastní HW	Ne	Ano	Ne	Ano
Umístění ve vlastním serveru (On-premises)	Ano	Ne	-	ano
Zaměření	Telemetrie vodáren, plynáren a energetiky	Telemetrie budov administrativních a průmyslových provozů	Kontrola energetické spotřeby budov	průmyslová automatizace
Oblasti umístění dat	-	Česká Republika, Holandsko	-	-
Možnost volby umístění dat	-	Ne	-	Ano
<i>[-] Příslušné informace nebylo možno zjistit z dostupné dokumentace</i>				

Tab. 10 Open source cloudové služby.

Název	Kaa	macchina.io	SiteWhere	Thingsboard	Lelylan
Webová stránka [URL]	https://www.kaaproject.org/	https://macchina.io/	http://www.sitewhere.org/	https://thingsboard.io/	http://www.lelylan.com/
Licence	Apache License 2.0	Apache License 2.0	CPAL 1.0	Apache License 2.0	Apache License 2.0
Zdarma	Ano	Ano	Ano	Ano	Ano
Platformy	Android, iOS, Linux, Snappy Ubuntu, Windows	Linux, Mac OS X	Linux, Windows	Windows, Linux, Mac OS X	Windows, Android, iOS, Linux
Jazyky	Objective-C, C, C++, Java	Javascript, C++	Java, JavaScript, Python, C	C, C++, Python, Javascript, Go	Noje.js, Angular.js, Ruby
Protokoly	HTTP(S)	HTTP(S), MQTT, CoAP, Modbus	MQTT, AMQP, STOMP	MQTT, CoAP, HTTP	HTTP, MQTT
Min. garantovaná dostupnost	-	-	-	-	-
Základní kit	Ne	Ne	Ne	Ne	Ne
Možnost připojit vlastní HW	Ano	Ano	Ano	Ano	Ano
Umístění ve vlastním serveru (On-premises)	Ano	Ne	Ano	Ano	Ano
Příklad HW	Raspberry Pi, ESP8266, Intel Edison	Raspberry Pi, Tinkerforge RED Brick	Raspberry Pi, Arduino, Android	Raspberry Pi, ESP8266, Arduino	Arduino, Raspberry Pi, ESP8266
Oblasti umístění dat	Vlastní server Veřejný cloud: AWS	Veškeré zpracování dat v rámci užití platformy (Raspberry Pi apod.)	Vlastní server Veřejný cloud: Microsoft Azure, AWS EC2	Vlastní server Veřejný cloud: AWS, Google cloud platform, Microsoft Azure	Vlastní server Veřejný cloud: AWS, Google cloud platform, Microsoft Azure
Možnost volby umístění dat	Ano	-	Ano	Ano	Ano
<i>[-] Příslušné informace nebylo možno zjistit z dostupné dokumentace</i>					

Tab. 11 Legenda k tab. 7, 8, 9, 10.

Free-trial	Udává, zda poskytovatel umožňuje vyzkoušet cloudovou službu před jejím zakoupením. Většinou se jedná o účet, který běžně na 30 až 60 dnů umožní přístup k většině nabízených služeb	
Ceny	Ceny se liší v poskytovaných službách, za které si společnosti účtují poplatky. V některých případech si společnosti účtují cenu za připojenou jednotku, jindy za množství přenesených dat, nebo třeba za místo v úložišti, které shromážděná data zabírají	
Platformy/Jazyky	Sady SDK pro zařízení, která lze propojit s danou cloudovou službou jsou dostupné pro různé programovací jazyky a platformy. Mezi nejčastěji podporované platformy se řadí např. Windows, Linux, nebo také Mac OS X, či iOS a mezi nejčastější jazyky se řadí Java, C, Python, Objective-C a další	
Protokoly	Protokoly příslušící nejvyšší aplikační vrstvě OSI modelu, které specifikují, co přenášená data reprezentují a jak s nimi nakládat. Například v případě Ethernetu se jedná o HTTP, HTML, SNMP, XML nebo v průmyslu například Modbus-TCP, či Modbus-RTU. Mezi nejvíce využívané protokoly v oblasti IoT patří MQTT, CoAP, XMPP a další	
Základní kit	Poskytuje-li společnost pro cloudovou službu základní kit. Jedná se o stavebnici, která se skládá z vývojářské desky a několika senzorů. Tato stavebnice umožňuje propojení vývojové desky a senzorů s cloudovou službou	
Možnost připojit vlastní HW	Udává, zda poskytovatel umožňuje propojení cloudové služby s komerčně dostupným produktem jako je například Arduino či Raspberry Pi, nebo povoluje pouze vlastní certifikovaná zařízení	
Min. garantovaná dostupnost	Poskytovatel garantuje určitou dostupnost své služby, ve které jsou započítána potřebná vypnutí z důvodů aktualizací a oprav, možné lokální, či globální výpadky internetové sítě a jiné důvody	
Umístění ve vlastním serveru	Jedna z možností umístění cloudové služby je v lokálním serveru zákazníka. Obecně se tento distribuční model označuje jako „On-premises“. Využití tohoto modelu nasazení bývá často využíváno u firem, které požadují rychlou odezvu služby a soukromí pro svá data	
Oblast umístění dat/volba umístění	V případě využití cloudové služby mimo lokální server uvádí poskytovatel oblasti na úrovni světadílů, států nebo měst, které využívají pro ukládání dat zákazníka. V některých případech si může uživatel zvolit umístění jeho dat, což je žádané především u firem s přísnými požadavky na zacházení s daty	
Vlastní produkty	Udává, zda společnost poskytující cloudové služby dodává ke svým řešením i vlastní produkty jako jsou senzory, datalogery, či jejich kombinace	
Příklad HW	Některé poskytovatele cloudových služeb přímo počítají s využitím komerčních produktů jako Arduino, Raspberry Pi a jim podobným platformám, proto na svých stránkách uvádí, pro které platformy mají připravené SDK, návody a ukázky	
Zaměření	Kromě obecných cloudových služeb, které nemají přesně specifikované využití existují také služby, které se přímo zaměřují na určité odvětví činnosti. Patří mezi ně např. Telemetrie vodáren, plynáren nebo také průmyslová automatizace a kontrola energetické spotřeby budov	
Další užitečné odkazy		Zdroje
Popis	Webová stránka [URL]	Pouze oficiální webové stránky, dokumentace k dané službě a emailová konverzace s poskytovatelem
Krátké zhodnocení nejznámějších komerčních a open source cloudů pro IoT. Dále lze na stránce nalézt rozsáhlou tabulku se seznamem dostupných cloudů a jejich základní údaje	http://www.postscapes.com/internet-of-things-platforms/	
V tomto článku se autor zaměřil na důležité vlastnosti, na které se dle výzkumu nejvíce hledí při výběru cloudu pro IoT. Výsledkem je přehledně zpracovaná tabulka	https://dzone.com/articles/iot-software-platform-comparison	
Velké přehled průmyslových IoT platform vyjádřený přehlednou tabulkou	http://www.mandsconsulting.com/industrial-iot-platform-comparison	
Český článek o přehledu cloudů v IoT. V textu autor popisuje základní informace o principu činnosti cloudů a dále pak jednotlivé cloudy zhodnotí krátkým popisem	http://vyvoj.hw.cz/velky-prehled-cloudu-pro-iot.html	

Tab. 12 ERP systémy typu cloud.

Název	Microsoft Dynamics 365	Infor ERP	SAP Business One	ABRA Gen	HELIOS Easy
Webová stránka [URL]	https://www.microsoft.com/en-us/dynamics365/	http://www.infor.com/solutions/erp/	https://www.sap.com/products/business-one.html	https://www.abra.eu/	https://www.idoklad.cz/
Free-trial	Ano	-	Ano	Ano	Ano
Ceny	Dynamics 365 Plan 1: 115\$/uživatel/měsíc Dynamics 365 Plan 2: 210\$/uživatel/měsíc	Různé v závislosti na poskytovateli služby (v ČR např. společnost GEMMA Systems, spol. s r.o.)	Různé v závislosti na poskytovateli služby (v ČR např. společnost Versino CZ, s.r.o.)	Individuální cena podle množství modulů Základní cena za uživatele: 1690Kč/uživatel/měsíc	HELIOS Easy Komplet: 5 uživatelů = 55 900Kč každý další uživatel: 23 900Kč
On-premises/cloud/Hybridní režim	Ano/Ano/Ano	Ano/Ano/Ano	Ano/Ano/Ano	Ano/Ano/-	Ano/Ano/-
Min. garantovaná dostupnost	99,9 %	99,5 %	99,5 %	99,90 %	99,99 %
Možnost integrace DMS do ERP	Ano (MS Office 365)	Ano (MS Office)	Ano (MS Office)	Ano (MS Office)	Ano (MS Office)
Řízení přístupových práv	Ano	Ano	Ano	Ano	Ano
Správa pomocí workflow	Ano	Ano	Ano	-	Ne (Ano ve verzi pro středně velké firmy "HELIOS Orange")
Webové rozhraní	Ano	Ano	Ano	Ano	-
Oblast umístění dat	Severní a jižní Amerika, Kanada, Velká Británie, EMEA, Německo, Japonsko, Rakousko, Indie	-	Využívá Amazon Web Services (umístění viz. tabulka "Komerční cloudové služby")	-	ČR
Možnost volby umístění	Ano	-	Ano	-	-
[-] Příslušné informace nebylo možno zjistit z dostupné dokumentace					

Tab. 13 Legenda k tabulce 12.

Free-trial	Udává, zda poskytovatel umožňuje vyzkoušet cloudovou službu před jejím zakoupením. Většinou se jedná o účet, který běžně na týden až měsíc umožní přístup k většině nabízených služeb	
Ceny	Ceny se liší v poskytovaných službách, za které si společnosti účtují poplatky. V některých případech si společnosti účtují cenu za uživatele za měsíc, jindy za uživatele na neomezenou dobu, nebo si účtují jednorázový poplatek za službu nezávisle na množství uživatelů	
On-premises /cloud/Hybridní režim	Kromě typického nasazení služby v cloudu nabízí poskytovatelé také řešení v podobě lokálního nasazení („On-premises“), nebo jejich kombinace (hybridní)	
Min. garantovaná dostupnost	Poskytovatel garantuje určitou dostupnost své služby, ve které jsou započítána potřebná vypnutí z důvodů aktualizací a oprav, možné lokální, či globální výpadky internetové sítě a jiné důvody	
Možná integrace DMS do ERP	V případě, že DMS služby nejsou v ERP systémů integrované, uvádí poskytovatel, zda je možná implementace těchto služeb.	
Řízení přístupových práv	Pro efektivní činnost jednotlivých zaměstnanců je důležité, aby měl každý individuální přístup ke službám systémů podle jeho pracovní náplně	
Správa pomoci workflow	Udává, zda je v rámci systému zahrnuta služba umožňující automatizaci procesů spojených s dokumenty	
Webové rozhraní	Přístup ke službě pomocí webového rozhraní představuje efektivní způsob vzdáleného přístupu, který je nezávislý na užití platformě	
Oblast umístění dat/volba umístění	V případě využití cloudové služby mimo lokální server uvádí poskytovatelé oblasti na úrovni světadílů, států nebo měst, které využívají pro ukládání dat zákazníka. V některých případech si může uživatel zvolit umístění jeho dat, což je žádané především u firem s přísnými požadavky na zacházení s daty	
Další užitečné odkazy		Zdroje
Popis	Webová stránka [URL]	Pouze oficiální webové stránky, dokumentace k dané službě a emailová konverzace s poskytovatelem
Přehledný seznam, především českých ERP systémů s výčtem jednotlivých funkcí	https://www.systemonline.cz/prehled-informacnich-systemu/erp-systemy/	
Výčet nejvyužívanějších světových ERP systémů s přehledným výčtem funkcí	http://www.pcmag.com/roundup/346016/the-best-erp-software	

Tab. 14 DMS systémy typu cloud.

Název	Google G Suite	Office 365 Business Premium	M-Files DMS	INOVIO elektronický oběh dokumentů	C SYSTÉM Správa dokumentů
Webová stránka [URL]	https://gsuite.google.com/	https://products.office.com/cs-cz/business/	http://www.e-dms.cz/	http://inovio.cz/	http://cloud.csystem.cz/
Free-trial	Ano	Ano	Ano	Ne	Ano
Ceny	<p>Basic: 4€/uživatel/měsíc, balík kancelářských služeb + uložení 30GB/uživatel</p> <p>Business: 8€/uživatel/měsíc, balík kancelářských služeb + neomezené uložení/uživatel</p>	<p>Plán 1: 10,50€/uživatel/měsíc při ročním závazku</p> <p>Plán 2: 12,70€/uživatel/měsíc při měsíčním závazku</p>	<p>Počet licencí: 5–49 = 199€/ks 50–190 = 179€/ks 200+ = 155€/ks</p>	<p>Na vlastním serveru: 55 000Kč</p> <p>Privátní cloud: 2 990Kč/měsíc</p>	<p>Plán 1: 4,20€/uživatel/měsíc při roční platbě</p> <p>Plán 2: 6,70€/uživatel/měsíc při roční platbě</p>
On-premises/cloud/Hybridní režim	Ne/Ano/Ne	Ano/Ano/-	Ano/Ano/Ano	Ano/Ano/-	-/Ano/-
Min. garantovaná dostupnost	99,90 %	99,90 %	-	99,80 %	99,90 %
Řízení přístupových práv	Ano	Ano	Ano	Ano	Ano
Správa pomocí workflow	Ano (Software Kissflow integrovaný do Google Apps)	Ano (součást aplikace SharePoint)	Ano	Ano	Ano
Webové rozhraní	Ano	Ano	Ano	Ano	-
Podpora typu souborů	MS Office	MS Office, PDF	MS Office, PDF, e-mail, CAD a další	MS Office, PDF, video, obraz a další	-
<i>[-] Příslušné informace nebylo možno zjistit z dostupné dokumentace</i>					

Tab. 15 Legenda k tabulce 14.

Free-trial	Udává, zda poskytovatel umožňuje vyzkoušet cloudovou službu před jejím zakoupením. Většinou se jedná o účet, který běžně na týden až měsíc umožní přístup k většině nabízených služeb	
Ceny	Ceny se liší v poskytovaných službách, za které si společnosti účtují poplatky. V některých případech si společnosti účtují cenu za uživatele za měsíc, jindy za uživatele na neomezenou dobu, nebo si účtují jednorázový poplatek za službu nezávisle na množství uživatelů	
On-premises /cloud/Hybridní režim	Kromě typického nasazení služby v cloudu nabízí poskytovatelé také řešení v podobě lokálního nasazení („On-premises“), nebo jejich kombinace (hybridní)	
Min. garantovaná dostupnost	Poskytovatel garantuje určitou dostupnost své služby, ve které jsou započítána potřebná vypnutí z důvodů aktualizací a oprav, možné lokální, či globální výpadky internetové sítě a jiné důvody	
Řízení přístupových práv	Pro efektivní činnost jednotlivých zaměstnanců je důležité, aby měl každý individuální přístup ke službám systémů podle jeho pracovní náplně	
Správa pomoci workflow	Udává, zda je v rámci systému zahrnuta služba umožňující automatizaci podnikových procesů	
Webové rozhraní	Přístup ke službě pomocí webového rozhraní představuje efektivní způsob vzdáleného přístupu, který je nezávislý na užití platformě	
Oblast umístění dat/volba umístění	V případě využití cloudové služby mimo lokální server uvádí poskytovatelé oblasti na úrovni světadílů, států nebo měst, které využívají pro ukládání dat zákazníka. V některých případech si může uživatel zvolit umístění jeho dat, což je žádané především u firem s přísnými požadavky na zacházení s daty	
Podpora typu souborů	Existují různé druhy souborových formátů. Při výběru DMS systému by měla firma přihlídnout k formátům, se kterými má v plánu pracovat.	
Další užitečné odkazy		Zdroje
Popis	Webová stránka [URL]	Pouze oficiální webové stránky, dokumentace k dané službě a emailová konverzace s poskytovatelem
Velký seznam nejznámějších DMS systémů	https://www.cmscritic.com/dir/dms	