Analýza „cloud computing“ systémů pro ŠKODA AUTO

Cloud Computing System Analysis for ŠKODA AUTO

Závěrečná zpráva projektu

Marek Rychlý a Dušan Kolář

Zadavatel projektu

Plánování značky, Výroba a logistika ŠKODA AUTO a.s.

Fakulta informačních technologií, Vysoké učení technické v Brně

Obsah

1 Úvod do technologie cloud computing

Technologii *cloud computing* je možné definovat jako nový směr v počítačovém zpracování, ve kterém jsou dynamicky rozšiřovatelné a často virtualizované zdroje poskytované jako služby prostřednictvím sítě Internet. Technologie *cloud computing* se postupně stala významným technologických trendem a mnoho odborníků očekává, že tato technologie změní infrastrukturu a způsob zpracování IT procesů a trhu. V prostředí technologie *cloud computing* mají uživatelé k dispozici celou řadu různých nástrojů, jako PC, přenosná PC, chytré telefony, prostřednictvím kterých a zejména sítě Internet přistupují k počítačovým programům, datovým úložištím, vývojářským platformám. Toto je právě umožněno díky službám nabízeným poskytovateli technologie *cloud computing*. Výhodami této technologie jsou úspory nákladů, vysoká dostupnost a jednoduchá rozšiřitelnost. [42]

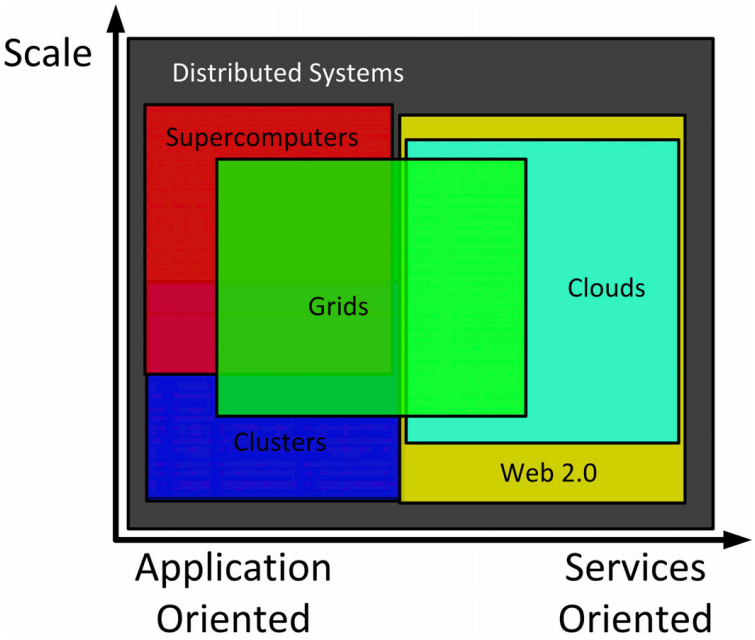
V průběhu několika posledních let stále roste potřeba po všudypřítomném výpočetním výkonu. Historicky, bráno z technologického úhlu podhledu, technologie *cloud computing* se začala vyvíjet ze střediskových počítačů (angl. *mainframe*), kde centralizované střediskové počítače poskytovaly výpočetní služby a datové úložiště centrálně. Postupně se architektura stala distribuovanou a přešla na model klient-server, kde služby jsou již poskytovány prostřednictvím sítě Internet. Uživatelem těchto služeb jsou potom lidé u osobních počítačů či malých přenosných zařízení. V minulosti měly všechny tyto architektury a způsoby zpracování své pevné místo a použití, avšak trpěly celou řadou problémů, které omezovaly jejich dostupnost a rozsah použití. Mezi takové problémy patří:

- vysoké náklady na údržbu a infrastrukturu – Je velice náročné udržovat technické (HW) a programové (SW) vybavení střediskových počítačů a serverů a jejich aplikace tak, aby svojí kvalitou dostávaly svým (nejen smluvním) závazkům. Např. vysoká dostupnost u kritických služeb vyžadovala velmi nákladná řešení, jako zálohované systémy, zálohování za běhu, přednastavené náhradní díly, minimální, nebo žádné výpadky (a to i po dobu údržby), apod.

- nízká rozšiřitelnost/rychlost změny – Uživatelské požadavky a využití programového i technického vybavení se v čase často mění s tím, jak se objevují nové obchodní příležitosti. Schopnost rozšířit systém podle rostoucí potřeby na jeho využití a tak udržet kvalitu poskytovaných služeb (rychlost odezvy systému na příchozí požadavek) nebo naopak zúžení systému tak, aby bylo možné uspořit užívané zdroje a tak snížit náklady, to jsou požadavky, které jsou jen těžko uspokojitelné a ekonomicky a fyzicky prakticky nesplnitelné v krátkém čase, či snad dokonce opakovatelně.

- problematický outsorcing (přesunutí služby k externímu dodavateli) – Přesouvaní IT služeb k externím dodavatelům je běžná věc nejen u malých a středně velkých podniků. Nicméně, pro daný hardware a software, který se nachází na konkrétním místě, vyvinutý je na konkrétní platformu, která je poskytovaná jediným dodavatelem, je velmi těžké izolovat konkrétní aplikace a ty přesunout k externímu dodavateli. Dokonce, pokud už došlo k přesunutí nějakých IT služeb k nějakému externímu poskytovateli, tak přesunout je zase jinam, bývá docela nákladné.

- nejasné účtování – IT oddělení bývají často považována za střediska s pevným ročním rozpočtem na správu infrastruktury a poskytování požadovaných služeb ostatním



Obrázek 1.1: Přehled „grid“ a „cloud“ zpracování (převzato z [41]).

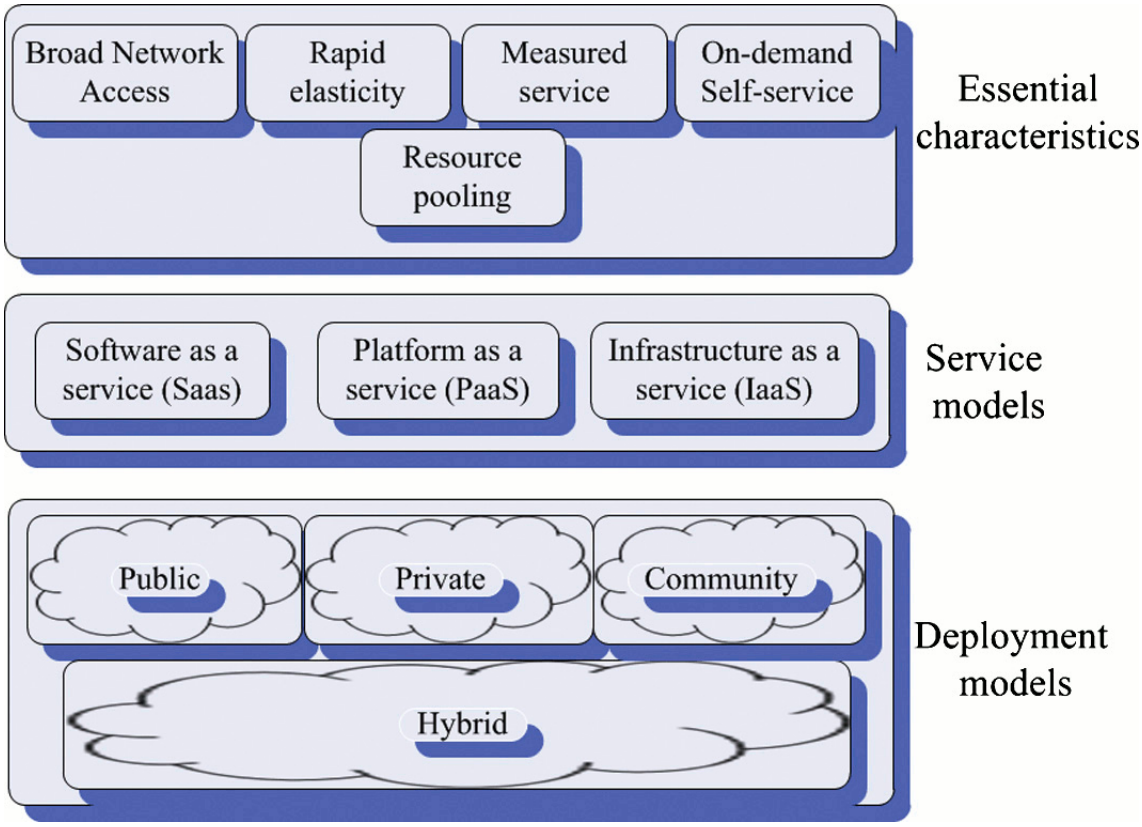
střediskům/oddělením. Přitom ostatní oddělení potřebují služby IT oddělení proto, aby mohla provádět svoji činnost a generovat zisk. Potom je ale velmi nesnadné propojit využití zdrojů IT oddělení skrze služby, které nabízejí, se ziskem organizace a dokázat tak, že IT oddělení, respektive služby jím poskytované, za cenu, kterou je nutné do něj vkládat, dodává dostatečnou hodnotu.

Tyto a další problémy byly známy a pokoušela se je odstranit různá řešení už před érou technologie *cloud computing*. Bylo vynaloženo hodně snah na distribuci výpočtů (vznikl tak např. standard Open MPI[1]), virtualizaci (řada dobře etablovaných otevřených i proprietárních řešení), virtuální privátní síť (anglicky „virtual private network“) (VPN) (propojují lokální pobočky organizací a umožňují globální využití služeb jednoho IT oddělení), atd. Např., tzv. *grid computing*, jeden z historických přístupů k řešení dané problematiky, který ukázal, že technologie *cloud computing* není úplně nový koncept, se snažil redukovat náklady na výpočetní výkon a zvýšenou spolehlivost a flexibilitu pomocí transformace počítačů z něčeho, co si koupíme a udržujeme sami, na něco, co nám zprostředkovává třetí strana [41]. Avšak technologie jako *grid computing*, *cloud computing* a jiné, se liší velikostí a zaměřením, jak ukazuje obrázek 1.1. Krom toho, všechna tato řešení vyžadují rychlé globální síťově připojení, takže, jelikož Internet začal nabízet rychlé propojení s dostatečnou kapacitou až od devadesátých let, technologie *cloud computing* nebyla hlavním trendem a široce přijímanou technologií až do doby zhruba před 10 lety.

1.1 Terminologie spojená s technologií cloud computing

V roce 2011 National Institute of Standards and Technology (NIST) (součást United State Department of Commerce /ministerstvo průmyslu a obchodu/) zveřejnil definici pro technologii *cloud computing* [75], aby vymezil její důležité aspekty a posloužila tak na širší porovnání služeb a strategií nasazení v prostředí této technologie. Dalším záměrem bylo

[1] `https://www.open-mpi.org/`



Obrázek 1.2: Definice technologie *cloud computing* dle NIST (převzato z [4]).

i nastolení základny pro diskuzi o tom, co tato technologie je a jak ji nejlépe využít. Podle NIST [75] je technologie *cloud computing* modelem pro nabízení všudypřítomného přístupu k síti na vyžádání tak, aby bylo možné přistupovat ke sdílenému zdroji konfigurovatelných výpočetních zdrojů (např. sítí, serverů, datových úložišť, aplikacím, jiným službám). Přitom jde o to, že tyto zdroje jsou poskytovány rychle a rychle uvolňovány v případě nepotřeby, a to s minimálním úsilím či interakcí poskytovatele.

Jak je vidět na obrázku 1.2, model výpočtu pro „cloud“ se skládá z pěti základních charakteristik (*essential characteristics*; vlastní obsluha na vyžádání, širokopásmové síťové připojení, sdílení prostředků, vysoká pružnost, měřitelné služby), třech modelů služeb (*service models*; infrastruktura-jako-služba (anglicky „Infrastructure as a Service“), platforma-jako-služba (anglicky „Platform as a Service“), software-jako-služba (anglicky „Software as a Service“)) a čtyř modelů nasazení (*deployment models*; privátní, komunitní, veřejné, hybridní). Níže budou podrobně definovány a popsány tyto základní charakteristiky, modely služeb a modely nasazení v technologii *cloud computing* pro potřeby tohoto dokumentu.

1.1.1 Základní charakteristiky

Definice technologie *cloud computing* podle NIST [75] uvádí těchto pět základních charakteristik:

- *Vlastní obsluha na vyžádání* (*on-demand self-service*) – Uživatel si může jednostranně opatřit výpočetní výkon, jako výpočetní čas na serveru, síťové datové úložiště, dle potřeby, zcela automaticky bez potřeby zásahu lidských zdrojů u každého poskytovatele služeb.

- *Širokopásmové síťově připojení* (*broad network access*) – Všechny schopnosti technologie jsou přístupné přes síťové připojení a standardními postupy, které umožňují jejich využití přes různé, heterogenní, tenké či tlusté klienty (např. mobilní telefony, tablety, přenosná PC, pracovní stanice).

- *Sdílení prostředů* (*resource pooling*) – Výpočetní zdroje poskytovatele jsou sdíleny tak, aby sloužily více uživatelům využitím modelu pro souběh uživatelů (víceuživatelský model, *multi-tenant model*). Přitom může docházet k tomu, že různé fyzické i virtuální zdroje jsou dynamicky přiřazovány podle potřeb uživatelů. Existuje zde jistá nezávislost zdrojů ve smyslu jejich umístění, takže uživatelé obecně netuší, ani nemají kontrolu nad tím, kde přesně se zdroje, které používají, nacházejí. Nicméně, na vyšší úrovni abstrakce toto umístění mohou vynutit (např. země, stát, datové centrum). Příkladem takto sdílených prostředků jsou datová centra, výpočetní výkon, paměť, šířka pásma síťového připojení.

- *Vysoká pružnost* (*rapid elasticity*) – Výpočetní zdroje poskytovatele je možné pružně přidělit i odebrat/uvolnit, v některých případech dokonce automaticky, aby bylo zajištěno jejich využití úměrně požadavkům. Uživateli se tak dostupné zdroje jeví často jako neomezené a je možné je čerpat kdykoliv a v libovolném množství.

- *Měřitelné služby* (*measured service*) – Systémy technologie „cloud“ automaticky řídí a optimalizují užití zdrojů pomocí měření[2] služeb na určité úrovni abstrakce vhodné pro daný typ služby (např. datové úložiště, šířka pásma, aktivní uživatelé na jeden účet). Užívání zdrojů je možné monitorovat, řídit, zaznamenávat tak, aby bylo jak pro uživatele, tak pro poskytovatele transparentní, jak bylo se službami/zdroji nakládáno.

Z technologického hlediska existuje ještě jedna vlastnost technologie *cloud computing* – souběh uživatelů, neboli víceuživatelský přístup (*multi-tenancy*). Z pohledu definice technologie, jak ji definuje NIST, to není základní charakteristika, nicméně je to důležitá vlastnost umožňující zaručit požadovanou kvalitu služeb a jejich bezpečnost a zabezpečení. Organizace „Cloud Security Alliance“ definuje souběh uživatelů takto [26]:

- *Souběh uživatelů* (*multi-tenancy*) – V nejjednodušší formě, souběh uživatelů/víceuživatelský přístup vynucuje použití stejných zdrojů či aplikací více uživateli, kteří mohou, ale nemusejí náležet do stejné organizace. Důsledkem souběhu uživatelů/víceuživatelského přístupu je viditelnost dat či pozůstatků operací jiným uživatelem. Souběh uživatelů/víceuživatelský přístup v prostředí technologie „cloud“ tedy vynucuje užití různých politik pro zajištění prosazení, oddělení, izolace, správy a úrovně služeb a také platebních modelů na základě volby uživatele.

1.1.2 Modely služeb

Definice technologie *cloud computing* podle NIST [75] uvádí kategorizaci podle následujících poskytovaných služeb:

- *software-jako-služba (anglicky „Software as a Service“) (SaaS)* – Prostředek poskytovaný uživateli je poskytovatelova aplikace běžící na infrastruktuře technologie „cloud“[3]. Aplikace jsou dostupné z různých klientských zařízení prostřednictvím tenkých klientů (např. e-mail jako webová aplikace), nebo rozhraní programu. Uživatel

[2] Typicky se to děje na principu zaplať za využití, nebo předplať si využití.

[3] Infrastruktura technologie „cloud“ je specifické programové a technické vybavení, které umožňuje realizovat 5 základních charakteristik technologie *cloud computing*. Na infrastrukturu technologie „cloud“ je možné pohlížet tak, že obsahuje jak fyzickou, tak abstraktní vrstvu. Fyzická vrstva sestává z technického

neřídí ani nespravuje podpůrnou infrastrukturu technologie „cloud“, jako je síť, servery, operační systém, datové úložiště, nebo dokonce možnosti jednotlivých aplikací (zde je však možná výjimka v oblasti uživatelsky specifických nastavení aplikace, která jsou často ale omezena).

- *platforma-jako-služba (anglicky „Platform as a Service“) (PaaS)* – Prostředek poskytovaný uživateli mu dává možnost spouštět na infrastruktuře technologie „cloud“ uživatelem vytvořené, nebo získané aplikace, které byly vyvinuty s pomocí programovacích jazyků, knihoven, služeb a nástrojů poskytovaných poskytovatelem[4]. Uživatel neřídí ani nespravuje podpůrnou infrastrukturu technologie „cloud“ jako je síť, servery, operační systém, datové úložiště, ale může řídit spouštěné aplikace a jejich nastavení v hostitelském prostředí.

- *infrastruktura-jako-služba (anglicky „Infrastructure as a Service“) (IaaS)* – Prostředek poskytovaný uživateli je možnost počítačového zpracování, uložení, síťového připojení, případně využití dalších výpočetních zdrojů, kde uživatel může spouštět a nechat běžet libovolné programové vybavení/software. To zahrnuje i operační systémy a aplikace. Uživatel neřídí ani nespravuje podpůrnou infrastrukturu, ale může řídit operační systémy, datová úložiště a spouštěné aplikace; a pravděpodobně také omezeně může řídit vybrané síťové prvky (např. firewall).

Modely služeb technologie „cloud“ obsahují a zveřejňují různé služby (viz obrázek 1.3) v programově-technickém zásobníku (*hardware/software stack*). V případě modelu služeb IaaS se jedná o služby na nízké úrovni, jako např. přístup k hardware a infrastruktuře zdrojů (jak nativních, tak virtualizovaných) pro systémové a síťové správce; v případě služeb PaaS se jedná o operační systémy, softwarové komponenty a middleware pro vývojáře; konečně u služeb SaaS se jedná o aplikace vhodné k okamžitému použití či aplikační rozhraní pro koncové uživatele. V tomto vrstveném zásobníku, který obsahuje modely služeb, každý model dědí schopnosti od modelů služeb pod ním, hlouběji v zásobníku.

Kromě třech výše uvedených modelů služeb, které jsou dohromady známy jako model SPI (SPI), byly popsány další modely, jako např. síť-jako-služba (anglicky „Network as a Service“) (NaaS), úložiště-jako-služba (anglicky „Storage as a Service“) (StaaS), či identita-jako-služba (anglicky „Identity as a Service“) (IdaaS).

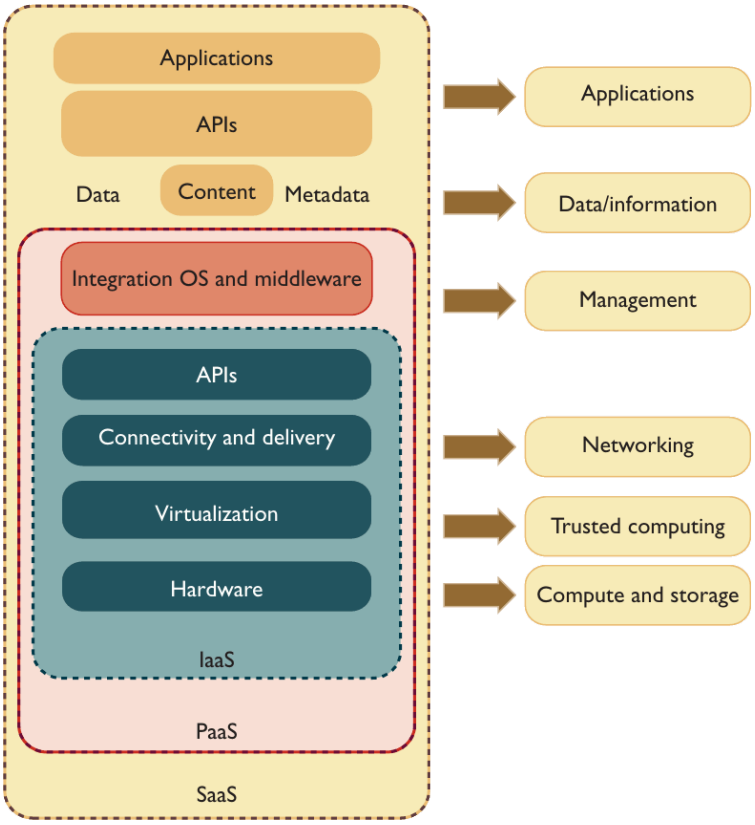
1.1.3 Modely nasazení

Definice technologie *cloud computing* podle NIST [75] uvádí čtyři možné modely nasazení podle umístění samotné technologie „cloud“:

- *Privátní/Soukromý* (*private cloud*) – Infrastruktura technologie „cloud“ je poskytována exkluzivně pro jedinou organizaci, která může sestávat z více jednotek (např. výrobní či obchodní oddělení). Může být vlastněn, spravován a provozován tou samou organizací, třetí stranou, nebo jejich kombinací. Může být umístěn v rámci prostor organizace i mimo (on/off premises).

vybavení/hardware nutného pro zajištění služeb v technologii „cloud“ a typicky to představuje server, datové úložiště, síťové prvky. Abstraktní vrstva sestává z programového vybavení/software spuštěného na fyzické vrstvě, což prokazuje základní charakteristiky technologie „cloud“. Konceptuálně potom abstraktní vrstva sedí na vrstvě fyzické.

[4]Toto ovšem nezakládá možnost využít kompatibilní programovací jazyky, knihovny, služby, či nástroje z jiných zdrojů,



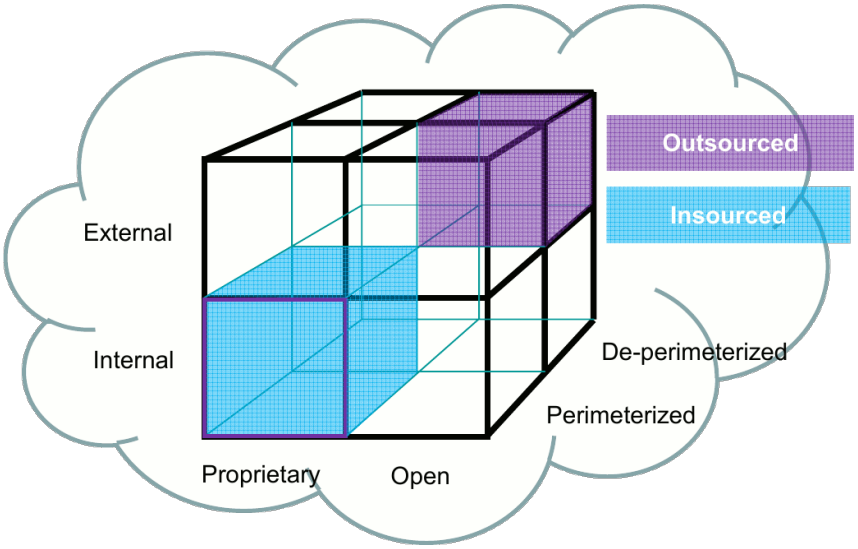
Obrázek 1.3: Tři modely služeb v technologii „cloud“ (převzato z [57]).

- *Komunitní* (*community cloud*) – Infrastruktura technologie „cloud“ je poskytována exkluzivně pro určitou komunitu uživatelů z organizací, které sdílejí určité zájmy (např. poslání, bezpečnostní požadavky, politiku, právní normy). Může být vlastněn, spravován a provozován jednou či více těmito organizacemi, třetí stranou, nebo jejich kombinací. Může být umístěn v rámci prostor organizace/í i mimo (on/off premises).
- *Veřejný* (*public cloud*) – Infrastruktura technologie „cloud“ je poskytována otevřeně pro použití běžnou veřejností. Může být vlastněn, spravován a provozován obchodními společnostmi, akademickou sférou, nebo vládními organizacemi, případně jejich nějakou kombinací. Je umístěn v prostorách poskytovatele.
- *Hybridní* (*hybrid cloud*) – Infrastruktura technologie „cloud“ je spojením dvou, nebo více infrastruktur (privátní, komunitní, nebo veřejné), které zůstávají unikátní v rámci struktury, ale které jsou dohromady propojeny standardní, či proprietární technologií, která umožňuje výměnu dat a přenositelnost aplikací (např. pro vyvážení zátěže mezi jednotlivými infrastrukturami při náhlé vysoké zátěži).

1.1.4 Kostičkový model — Cloud Cube Model

V roce 2009, tzv. Fórum Jericho [88] identifikovalo čtyři kritéria na rozlišení uskupení technologie „cloud“ a zejména odlišení způsobu jejich poskytování. Kostičkový model — Cloud Cube Model (CCM) — je na obrázku 1.4 a shrnuje tyto čtyři dimenze takovýmto způsobem [88]:

- *Dimenze interní (I) / externí (E)* (*Internal/External*) definuje fyzické umístění dat



Obrázek 1.4: Kostičkový model (CCM) jak ho prezentuje Fórum Jericho (převzato z [88]).

v technologii „cloud“, rozlišuje, jestli existuje uvnitř, nebo mimo fyzické hranice organizace. Jako příklad interní technologie „cloud“ můžeme uvést sdílené úložiště, které má virtualizované disky uvnitř datového centra dané organizace. Zatímco stejné úložiště v Amazon SC3 by byl příklad externí technologie „cloud“.

- *Dimenze proprietární (P) / otevřený (O)* (*Proprietary/Open*) definuje vlastnictví technologie „cloud“, služeb ní nabízených, rozhraní, atd. Proprietární znamená, že poskytovatel služeb vlastní prostředky poskytující tyto služby, přičemž otevřený znamená, že existuje více poskytovatelů nějaké technologie, která není proprietární. V případě otevřené technologie uživatel nebude omezován v možnosti sdílet data či aplikace, nebo spolupracovat s vybranými stranami prostřednictvím stejné otevřené technologie. Proto dimenze P/O indikuje stupeň interoperability stejně jako možnost jakési „přenositelnosti“ dat/aplikací mezi aktuálním systémem a jinými formami technologie „cloud“, jako i možnost odstranění dat z úložiště v technologii „cloud“, nebo jejich přesun k jinému poskytovateli bez nějakých omezení.

- *Dimenze v perimetru (Per) / mimo perimetr (D-p)* (*Perimeterised/De-perimeterised Architectures*) reprezentuje „architektonický styl“ daného řešení technologie „cloud“, kde jednotlivé přístupové body do technologie leží uvnitř, nebo vně IT perimetru infrastruktury dané organizace.

  Architektura v perimetru implikuje pokračování činností uvnitř tradičního IT perimetru. Toto je často naznačeno existencí síťového zabezpečení (např. firewall), které řídí přístup ke službám technologie „cloud“ stejným způsobem jako v případě služeb mimo technologii „cloud“, které běží uvnitř, i když třeba virtuálního, perimetru organizace. V tomto případě je perimetr organizace často jednoduše rozšířen do externí domény pro technologii *cloud computing* pomocí VPN, nebo virtuálního serveru pracujícího v IP doméně dané organizace, aby bylo možné využít jejích vnitřních služeb pro řízení přístupu.

  Architektura mimo perimetr předpokládá, že systémový perimetr je spravován poskytovatelem technologie „cloud“ a že služby s ní spojené musejí být explicitně ochráněny, což je mnohem náročnější (např. data musejí být zabalena do metadat a musejí

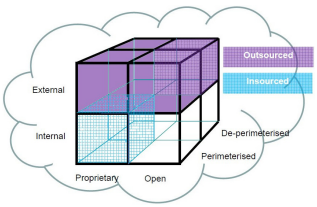
existovat mechanismy pro ochranu dat před nechtěným užitím). Například, vezměme do úvahy použití externí proprietární technologie „cloud“ Amazon SC3, kdy byla zavedena kombinace virtuálních serverů v perimetru společnosti Amazon a datové sady, které jsou veřejné a mimo perimetr společnosti, které slouží pro tvorbu privátních výsledků, které jsou dále vráceny zpět do interního prostředí, které leží mimo technologii „cloud“.

- *Dimenze vnitřních / vnějších zdrojů* (*Insourced/Outsourced*) popisuje, kdo spravuje poskytování služeb technologie „cloud“ zastřešovaných danou organizací. Služby mohou být poskytovány danou organizací za plného řízení jejích zaměstnanců, nebo smluvní třetí stranou. Toto je typicky otázkou politiky organizace (tedy obchodní rozhodnutí, ne technologické hledisko). Také musí být součástí smlouvy s poskytovatelem technologie „cloud“. V Kostičkovém modelu CCM je tato čtvrtá dimenze zobrazena dvěma barvami; libovolná z osmi forem (Per IP, IO, EP, EO; a D-p IP, IO, EP, EO) může mít jednu z těchto dvou barev.

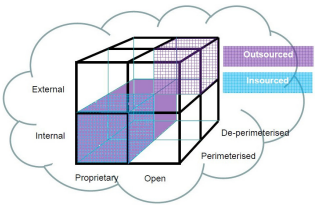
Kostičkový model CCM ilustruje permutaci hodnot v dimenzích uvedených výše. Tyto dimenze jsou dnes běžně k dispozici u různých poskytovatelů. Model ukazuje možné hodnoty u čtyř dimenzí s cílem odlišit *formace* technologie „cloud“ a způsob jejich poskytování. Dalším cílem je umožnit pochopení, jak technologie *cloud computing* ovlivňuje způsob zajištění bezpečnosti [26]. Bezpečnostní hledisko technologie „cloud“ bude dále rozebráno v sekci 2.3.

Kostičkový model CCM je také využit v [22] pro přehled aktuálních obchodních modelů v oblasti technologie *cloud computing*. Krom toho jsou zde uvedeny návrhy, jak by organizace mohly dosáhnout udržitelnosti díky zavedení jednoho z osmi obchodních modelů technologie *cloud computing* při znalosti svých silných i slabých stránek (viz obrázek 1.5):

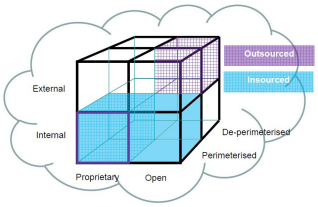
- *Poskytovatelé služeb, orientace na služby* – pro externí technologie „cloud“ s vnějšími zdroji poskytující cokoliv z modelů služeb IaaS, PaaS či SaaS,
- *Smluvní služby a podpora* – pro interní privátní technologie „cloud“ s vnějšími zdroji poskytující cokoliv ze služeb IaaS, PaaS či SaaS,
- *Privátní technologie „cloud“ provozována interně* – pro interní technologie „cloud“ s vnitřními zdroji pracující v perimetru implementující model SaaS,
- *Technologie „cloud“ se vším všudy pro velké podniky* – pro interní technologie „cloud“ s vnitřními zdroji pracující v perimetru v kombinaci s řešeními cele založenými na vnějších zdrojích sloužícími k pokrytí všech modelů architektur a služeb,
- *Zdroje a služby pod jednou střechou* – pro externí technologie „cloud“, kde je možné pracovat s vnitřními i vnějšími zdroji, obvykle se jedná o komunitní prostředí,
- *Vládní financování* – pro vládou financované organizace, které využívají privátní technologie „cloud“ s vnějšími zdroji v soukromém sektoru, nebo využívají otevřené technologie „cloud“ s vnitřními zdroji v případě akademických institucí,
- *Venture kapitál* – pro soukromé společnosti, často začínající (start-up), které využívají externí privátní technologie „cloud“, externí otevřené technologie „cloud“ s vnějšími zdroji, nebo otevřené technologie „cloud“ s vnitřními zdroji,
- *Zábava a sociální sítě* – pro externí privátní technologie „cloud“ s vnějšími zdroji pracující mimo perimetr implementující model služeb SaaS.



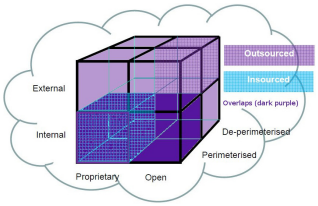
(a) Poskytovatelé služeb, orientace na služby



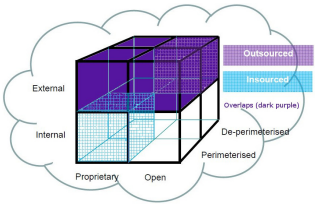
(b) Smluvní služby a podpora



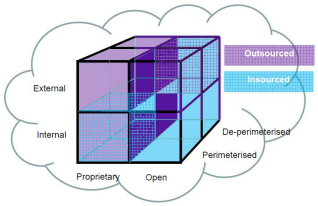
(c) Privátní technologie „cloud“ provozována interně



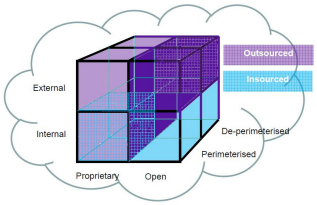
(d) Technologie „cloud“ se vším všudy pro velké podniky



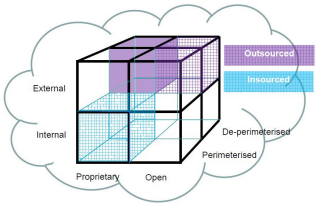
(e) Zdroje a služby pod jednou střechou



(f) Vládní financování



(g) Venture kapitál



(h) Zábava a sociální sítě

Obrázek 1.5: Obchodní modely technologie *cloud computing* (převzato z [22]).

Obchodní model pro technologii *cloud computing* uvedený výše bude použit při porovnání dostupných služeb technologie „cloud“ v kapitole 3.

1.2 Přehled současného stavu a budoucích trendů vývoje technologie cloud computing

Jak je popsáno v [42], technologie *cloud computing* je distribuované výpočetní paradigma, které propojuje aspekty technologie *grid computing* (cituji, „... infrastruktura hardware a software, která poskytuje spolehlivý, konsistentní, pervazivní a přitom nikoliv drahý přístup k špičkovým výpočetním prostředkům ...“ [40]), tzv. *Internet computing* (cituji, „... výpočetní platforma geograficky rozložená v celém prostředí sítě Internet ...“ [76]), *utility computing* (cituji, „... sada technologických a obchodních praktik, které umožňují nenásilně a spolehlivě realizovat výpočty na více počítačích současně ... k dispozici jsou dle potřeby a účtovány podle vytížení, podobně jako voda, nebo elektrická energie se dnes běžně účtuje ...“ [98]), *autonomic computing* (cituji, „... výpočetní systémy, které se samy řídí na základě požadavků vysoké úrovně daných administrátorem ...“ [67]) *edge computing* (cituji, „... poskytuje generické šablonovité vybavení použitelné pro libovolný druh aplikací tak, aby bylo možné rozprostřít výpočet do k tomu určené sítě, aby se vyvážila zátěž jednotlivých uzlů sítě ...“ [30]) a *green computing* (jelikož se předpokládá, že účty za energii spojenou s IT se vztahují i k znečištění životního prostředí [42]).

Díky těmto aspektům technologie *cloud computing* a díky úzkým vazbám mezi touto technologií a řadou dalších technologických a výzkumných odvětví je zřejmé, že objevující se oblasti zájmu a inovací v příbuzných oborech nutně ovlivňují i směrování výzkumu v samotné technologii *cloud computing*. V následujících sekcích budou prezentovány dva současné přístupy k technologii *cloud computing* v oblasti zpracovatelského průmyslu a také budou nastíněny budoucí trendy vývoje v této oblasti.

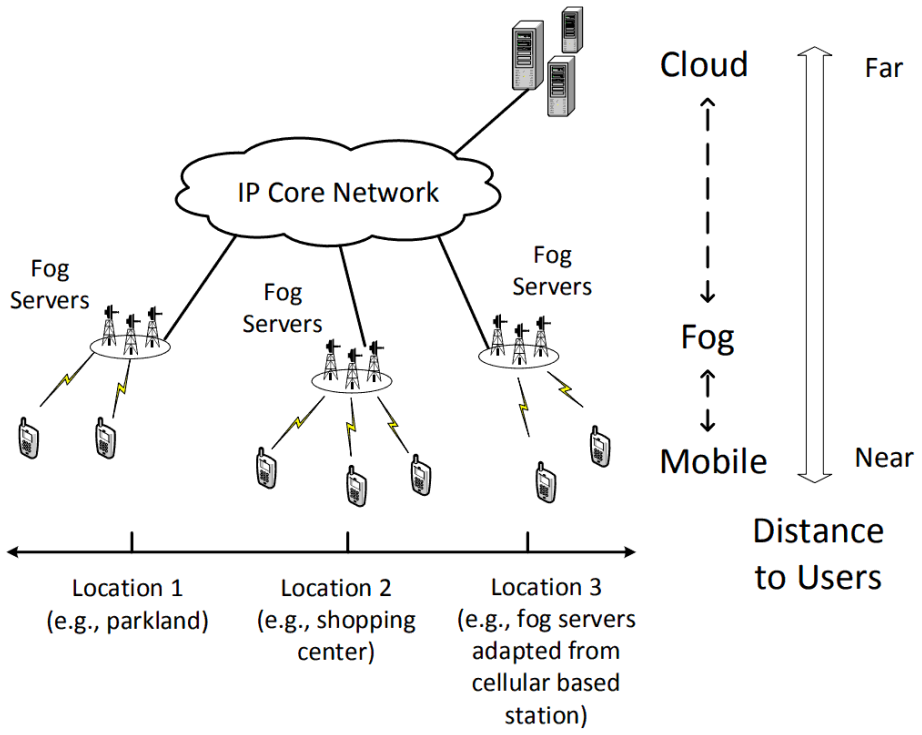
1.2.1 Technologie edge computing a fog computing

Náš síťový provoz je dnes ovlivněn dvěma zřejmými trendy [73]:

- *Internetem založeným na technologii „cloud“* (*Cloud-based Internet*) – Technologie *cloud computing* se již vyvinula jako klíčová výpočetní infrastruktura v oblasti Internetu s plnohodnotnou nabídkou služeb, která zahrnuje nejenom obsah, ale i způsob komunikace, aplikace a obchodní styk. Jak bylo zjištěno, tak okolo 90% uživatelů Internetu celosvětově nyní spoléhá na služby poskytované technologií „cloud“, jednak přímo, skrze uživatelské služby, nebo nepřímo, díky různým poskytovatelům služeb, kteří využívají různá komerční řešení technologie „cloud“.

- *Nárůst mobilních („edge“) výpočtů* (*Proliferation of mobile (edge) computing*) – Od roku 2011 převyšuje počet prodaných chytrých telefonů počet prodaných PC. K dnešnímu dni narostlo zastoupení chytrých telefonů v USA na 80%. Jak předpokládá společnost Cisco, tak průměrný počet připojených zařízení na osobu v roce 2020 bude 6,58. S tím, jak různé chytré přístroje do rukou uživatelů přinášejí silný výpočetní výkon a rychlou komunikaci kdekoliv na světě, tak roste počet mobilních aplikací z různých oborů, např. virtuální realita, snímání a navigace, které vyústily v klíčové změny návyků, jak lidé žijí.

Technologie *fog computing* se pokouší sloučit oba dva výše zmíněné trendy. Služby poskytované technologií „cloud“ se posunují blíže uživatelům díky síti a mobilním zařízením,



Obrázek 1.6: Architektura *fog computing* (převzato z [73]).

která se podílejí na vlastní technologii „cloud“ na hranici sítě jako poskytovatelé individuálních služeb (viz obrázek 1.6). Přitom jádro technologie *cloud computing* poskytuje sdílené služby na podporu různých zařízení v souladu s potřebami výpočetního modelu, který se koncentruje kolem technologie *edge computing* [44]. V infrastruktuře technologie *fog computing* [111] mohou být služby umístěny přímo na koncových zařízeních, jako např. přístupové body, nebo zařízení typu set-top-box. Infrastruktura tohoto nového distribuovaného výpočetního modelu umožňuje, aby aplikace byly spouštěny co nejblíže zdrojům detekovaných a často masivních toků dat, která vycházejí z lidí samotných, procesů a věcí. Tento koncept technologie *fog computing*, vlastně se jedná o technologii *cloud computing* přivedenou až k samotnému základu, vytváří automatizovanou reakci, která přináší hodnotu.

Technologie *fog computing* byla nedávno v [118] definována jako scénář, kde obrovský počet heterogenních (bezdrátových a někdy autonomních) všudypřítomných a decentralizovaných zařízení komunikuje mezi sebou a potenciálně spolupracují mezi sebou a prostřednictvím sítě i s dalšími zařízeními za účelem ukládání dat a jejich zpracování bez zásahu třetí strany. Tyto úlohy mohou podporovat základní funkce sítě, nebo nové služby a aplikace, které běží v odděleném prostředí (*sandboxed environment*). Uživatelé, kteří si část těchto zařízení pronajímají k tomu, aby získali tyto služby, jsou k tomu různě pobízeni.

Jelikož je technologie *fog computing* implementována na hraně („edge“) síťového prostředí, poskytuje nízkou dobu zpoždění, dobrou lokalitu služeb a zlepšuje kvalitu služeb (QoS) pro přenos médií a aplikace pracující v reálném čase. Krom toho, tato nová infrastruktura podporuje heterogenitu, protože zařízení v technologii „fog“ zahrnují koncová uživatelská zařízení, přístupové body, přepínače a směrovače pro práci na hraně („edge“) celé infrastruktury technologie. Paradigma technologie *fog computing* se dobře hodí pro zpracování velkého množství dat v reálném čase, podporuje velmi vzdálené sběrné body dat a poskytuje výhody pro zábavu, reklamu, osobní výpočty a další aplikace. [111]

Příklady technologie fog computing

Typické příklady aplikací technologie *fog computing* zahrnují automatizaci, dopravu a sítě senzorů a aktuátorů [111]. V těchto případech koexistuje technologie *fog computing* a *cloud computing* v symbiotickém vztahu. Zatímco místní uzly technologie *fog computing* v továrnách, autech nebo chytrých městech (*smart city*) poskytují lokalitu, takže umožňují nízké zpoždění a kontextovost zmíněnou výše, tak technologie *cloud computing* poskytuje nutnou globální centralizaci [18].

První příklad ukazuje průmyslovou automatizaci, kde technologie *fog computing* může být použita v továrnách praktikujících Průmysl 4.0, kde je možné technologii použít na oddělení výrobních dat na nejnižší úrovni, aby bylo možné dosáhnout dostatečné rychlosti výpočtu, ušetřit šířku pásma, zvýšit efektivitu a podpořit decentralizaci, takže pouze užitečná data budou poskytována pro řízení, analýzu a manažerské úrovně zpracování dat [72].

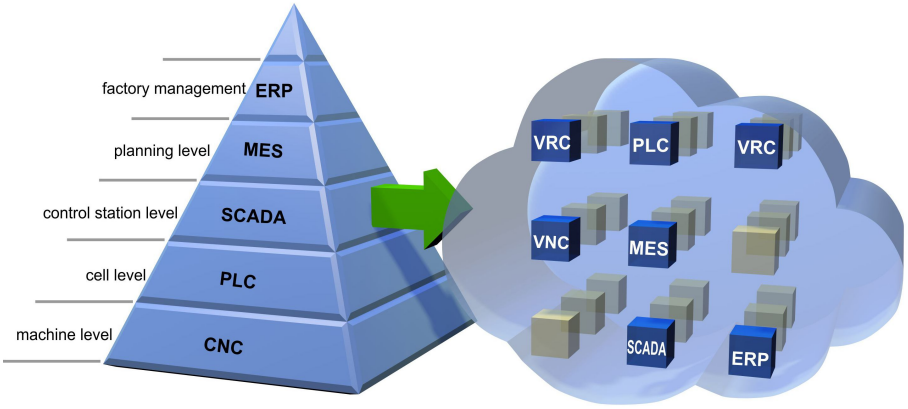
Druhý příklad demonstruje technologii *fog computing* v dopravě, kdy reprezentuje ideální platformu pro doručení široké nabídky služeb v oblasti zábavy a informací, bezpečnosti, podpory dopravy a různých druhů analýz. A to proto, že to spolu přináší další vhodné atributy: geografické rozložení (uvnitř měst a podél cest), mobilitu a lokalitu, nízké zpoždění, heterogenitu a podporu pro interakce v reálném čase, jako například chytré ovládání semaforů v chytrých městech (*smart city*[5]) [18].

Konečně ve třetím příkladu je využita technologie *fog computing* pro implementaci technologie *smart grid*, kde sběrače dat v technologii „fog“ umístěné na konci/hraně („edge“) sítě sbírají data generovaná senzory a zařízeními z technologie „grid“. Některá z těchto dat spadají do řídicích a bezpečnostních smyček, které vyžadují práci v reálném čase (od milisekund až po zlomky sekund). První vrstva technologie „fog“, která je navržená pro komunikaci mezi stroji, sbírá a zpracovává data, na jejichž základě vysílá řídicí příkazy aktuátorům. Tak filtruje data, která se mají zpracovat lokálně od dat, která se posílají vyšším vrstvám. Druhá a třetí vrstva se zabývají vizualizací a podáváním zpráv (interakce člověk-stroj), stejně tak ale se zabývají systémy a procesy (interakce stroj-stroj). Časová měřítka těchto interakcí, všechny se odehrávají uvnitř technologie „fog“, se pohybují od několika sekund do minut (analýza v reálném čase), ale také až v rozměru několika dní (transakční analýza). Aby bylo dosaženo těchto vlastností, technologie *fog computing* musí podporovat několik typů úložišť, od dočasných na nejnižších vrstvách, přes částečně permanentní na nejvyšší úrovni. Také platí, že čím vyšší vrstva, tím větší geografické pokrytí a tím větší časové měřítko. Celkové, globální pokrytí je potom zajištěno technologií „cloud“, která je použita jako úložiště pro data, která se ukládají na dobu měsíců, nebo let, a která jsou základem pro obchodní analýzy. Toto je typické prostředí zpráv a ukazatelů, které zobrazují klíčové výkonnostní charakteristiky. [18]

Související koncepty a technologie

Příklady technologie *fog computing*, demonstrované v předchozí sekci, zmiňují tři klíčové budoucí trendy v oblasti technologie *fog computing*: Průmysl 4.0, chytrá města (*smart city*), *smart grid*. Kromě toho jsou tu další dvě technologie, které výrazně přispívají k vzniku takových aplikací: internet věcí (anglicky „Internet of Things“) (IoT) a softwarově definovaná síť (anglicky „software-defined network“) (SDN).

[5] Chytré semafory interagují s řadou senzorů v místě, kde stojí. Tyto senzory detekují přítomnost chodců, cyklistů, měří vzdálenost a rychlost přijíždějících vozidel. Dochází také k interakci s blízkými semafory, aby došlo ke koordinaci zelené vlny. Na základě takto získaných informací posílají semafory varování přijíždějícím vozidlům a také modifikují svůj vlastní cyklus, aby předcházely nehodám [18].



Obrázek 1.7: Modularizace a virtualizace řídicích prvků v továrně (převzato z [121]).

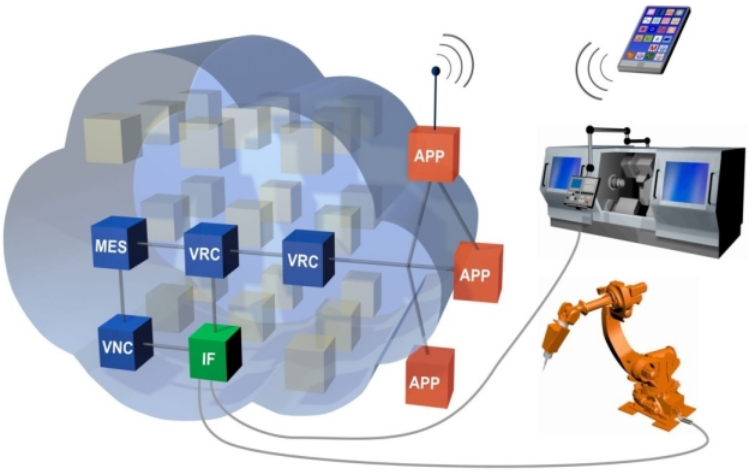
IoT je nové paradigma, které si rychle získává půdu v oblasti moderních bezdrátových komunikací. Základní myšlenkou tohoto konceptu je naprosté obklopení nás různými variantami věcí či objektů (příkladem jsou třeba RFID označení, senzory, aktuátory, mobilní telefony, apod.), které jsou díky jedinečnému adresovacímu schématu schopny interagovat jeden s druhým a spolupracovat se svými sousedy pro dosažení stejných cílů. [10]

SDN je nová síťová architektura, která je navržena pro použití standardního aplikačního programového rozhraní (API), aby umožnila programátorům síťových aplikací rychle definovat a rekonfigurovat způsob, jakým jsou data či zdroje v síti manipulována. Používání API umožňuje, aby síťové aplikace (e-mailové systémy, služby technologie *cloud computing*, telefonní aplikace) mohly jednoduše přistupovat k rozhraní a rekonfigurovat síť a její komponenty (jako přepínače, servery, virtuální stroje, apod.), nebo stahovat potřebná data podle toho, co zrovna potřebují. [68]

1.2.2 Technologie cloud computing pro továrny a RaaS

Budeme-li následovat trendy posledních let a také požadavky Průmyslu 4.0, tak továrna budoucnosti bude muset splňovat požadavky na plně zakázkovou výrobu, kde platí, že je série velikosti jedna (*lot size one*). Roboti a stroje tedy budou muset být rychle rekonfigurovatelní. Sběr a analýza všemožných dat z procesů se stane nutností. Všechny senzory, aktuátory a výpočetní algoritmy budou muset být vzájemně propojeny, aby dosáhly účinného sběru a užití dat. Aby bylo možné se vypořádat s modifikovanou strukturou výrobních systémů, řídicí architektura strojů a robotů se bude muset změnit z hierarchické na plochou a plně propojené sestavení. Tak zvaný kyberfyzikální výrobní systém (anglicky „cyber-physical production system“) (CPPS) [103] by potom měl být schopen poskytovat a využívat různé služby. [121]

Technologie „cloud“ pro továrny sestává z různých služeb řídicích systémů pocházejících z technologie „cloud“ samotné, jak je uvedeno na obrázku 1.7. Konkrétně to jsou položky z oblasti managementu továrny jako plánování podnikových zdrojů (anglicky „enterprise resource planning“) (ERP), přes výrobní informační systém (anglicky „manufacturing execution system“) (MES) na úrovni plánování, dispečerské řízení a sběr dat (anglicky „Supervisory Control and Data Acquisition“) (SCADA) na úrovni řízení stanic, až po výrobní programovatelný logický automat (anglicky „programmable logic controller“) (PLC) na úrovni jednotek a počítačové číslicové řízení (anglicky „computer numeric control“) (CNC) strojů na úrovni strojní. Všechny tyto řídicí systémy jsou modularizované a pro-



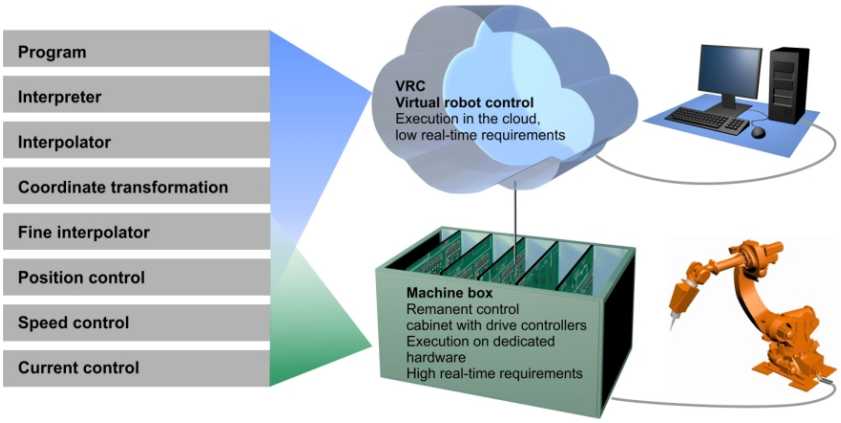
Obrázek 1.8: Tovární „cloud“ s rozhraními na roboty, stroje a služby (převzato z [121]).

pojené a jejich služby, veřejně dostupné v tovární technologii „cloud“, musejí být sehrány, aby vyhovovaly obchodním a továrním výrobním procesům. Integrace, kde se skládá soft-PLC a řídící jednotka robota (anglicky „robot controller“) (RC) do virtuálního stroje schopného pracovat v reálném čase, způsobí, že vzniká virtuální programovatelný logický automat (anglicky „virtual programmable logic controller“) (VPLC), respektive virtuální řídící jednotka robota (anglicky „virtual robot controller“) (VRC), jak je uvedeno v [121] a zobrazeno na obrázku 1.8.

Technologie „cloud“ pro továrny se běžně implementuje jako privátní technologie „cloud“, protože výrobní systémy vyžadují připojení s nízkým zpožděním pro přesné řízení připojených strojů. Avšak, v případě robotů a jejich virtuálních řídicích jednotek (VRC) je vhodné, aby byly jejich služby publikovány globálně a byly přístupné ve veřejné technologii „cloud“. Důvodem může být monitoring výroby různými metrikami a produkce a analýza správných výkonnostních ukazatelů (klíčový ukazatel výkonnosti (anglicky „key performance indicator“) (KPI)). Ve [23] je uveden koncept technologie robot-jako-služba (anglicky „Robot as a Service“) (RaaS) za účelem podchycení výše zmíněné problematiky.

Model služeb poskytovaných technologií RaaS vynucuje návrh a implementaci robota či zařízení tak, aby to byla jednotka „vše v jednom“ architektury orientované na služby (SOA). Tedy, jednotka zahrnuje služby pro vykonání potřebné funkcionality, zprostředkovatele na zjišťování dostupných a nabízení vlastních služeb, no a klientské aplikace pro přímý přístup. Na rozdíl od dřívějšího přístupu, kdy robot v architektuře SOA je aplikace, která využívá služeb počítače v pozadí, technologie RaaS dává robotovi mnohem více schopností a kapacity, takže může být kvalifikován jako plně soběstačná jednotka technologie „cloud“ v prostředí technologie *cloud computing*. [23]

Autoři zdroje [121] rozdělují jednotky VRC na dvě služby technologie „cloud“. Takto oddělují funkce s nízkými nároky na práci v reálném čase od funkcí s vysokými nároky na práci v reálném čase, které jsou nutné z hlediska umístění, rychlosti a přímého řízení robotů. V takovémto přístupu nová jednotka VRC implementuje služby technologie „cloud“ pro sadu funkcí s nízkými nároky na práci v reálném čase, zatímco funkce mající vysoké nároky na práci v reálném čase jsou implementovány jako hraniční („edge“) služby technologie „cloud“, vzhledem k tomu, jak je definován model služeb technologie RaaS. Takto mohou být nové služby jednotek VRC technologie „cloud“ přesunuty do veřejné technologie „cloud“ a původní privátní technologie „cloud“ může být dynamicky rozšířena pomocí veřejných zdrojů, jak je ukázáno na obrázku 1.9.



Obrázek 1.9: Přenos funkcí z řídicího centra do VRC v závislosti na požadavcích práce v reálném čase (převzato z [121]).

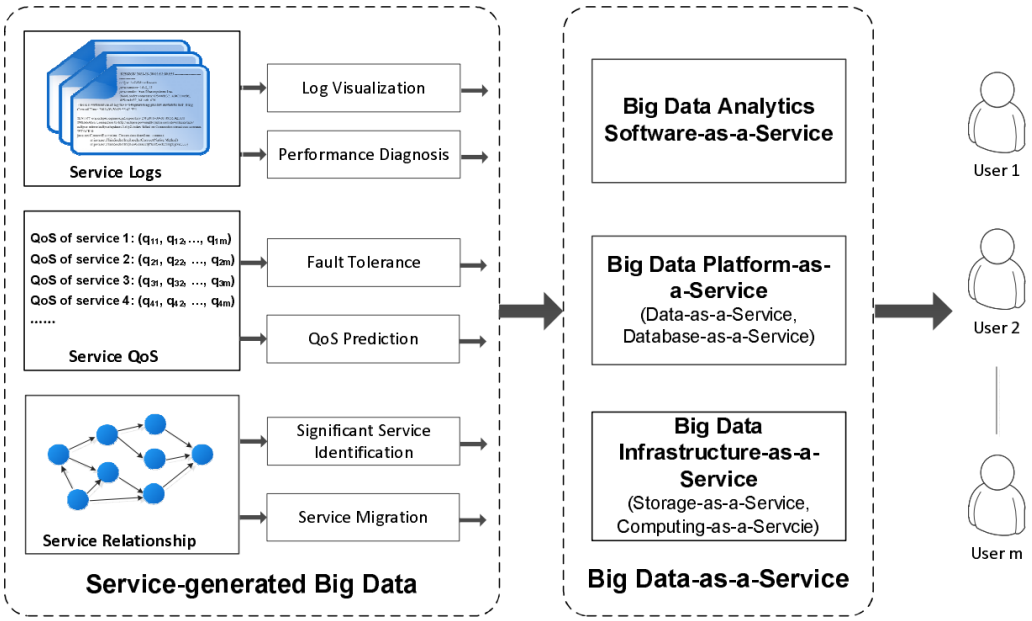
1.2.3 Technologie big data, fast data a DaaS

Technologie data-jako-služba (anglicky „Data as a Service“) (DaaS) je takovým typem služeb poskytovaných technologií *cloud computing*, kdy jsou data poskytována na požádání. Technologie DaaS typicky vystavuje sebou nabízená data uživatelům skrze aplikační programové rozhraní (anglicky „application programming interface“) (API). Jednak to mohou být různá data určená pro stažení uživatelům, nebo data, která jsou výsledkem dotazů. Používáním technologie DaaS uživatelé nemusejí vybírat a ukládat ohromné datové balíky a v nich hledat požadované informace, ale místo toho stačí najít vhodného poskytovatele technologie DaaS, který má vhodná data s chtěnou informací, a zavoláním příslušného API data pouze získat. V souvislosti s nedávným rozvojem technologie *cloud computing* je možné vybudovat technologii DaaS mnohem jednodušeji a přitom tak, že poskytuje větší datové sestavy za menší cenu, než přímo v technologii „cloud“. [122]

S technologiemi jako je *fog computing*, „cloud“ pro továrny, apod., množství zařízení, která implementují služby technologie „cloud“ a jsou schopny pracovat podle modelu služeb technologie DaaS, rychle vrůstá. Navíc, i další služby technologie „cloud“ produkují velké množství dat jako výsledek jejich monitorovacích metrik. Konečně, existuje i velké množství veřejných a privátních zdrojů dat dostupných jak v organizacích tak na síti Internet. Tato úložiště obsahují již nyní ohromné množství různých dat jejichž objem narůstá exponenciálně. Taková data jsou typicky heterogenní, nad různými datovými typy, vysoce dynamická a je možné je popsat jako *big data* a tedy je vhodné je i jako *big data* zpracovávat, tedy na to použít specifické technologie. Podle [43] technologie *big data* popisují novou generaci technologií a architektur, které jsou navrženy pro extrakci ekonomických hodnot z ohromných objemů rozmanitých dat tím, že umožní vysokorychlostní zaznamenávání, objevování a/nebo analýzu těchto dat. Proto, technologie *big data* může být charakterizována jako něco, co je dle [9] často nazýváno jako *multi-V model*:

- *Rozmanitost* (*Variety*) reprezentuje různé datové typy v technologii *big data*, které mohou být strukturované (s formálně definovanými schématy a datovými modely), nestrukturované (žádný předdefinovaný datový model), semi-strukturované (postrádají striktně vymezený datový model a strukturu), nebo smíšené (výše uvedené typy dohromady).

- *Rychlost* (*Velocity*) se odkazuje na vysokou frekvenci, s jakou jsou data produkována a zpracovávána.



Obrázek 1.10: Přehled technologie *big data*: jako technologie generovaná službami a jako služba jako taková (převzato z [129]).

- *Objem* (*Volume*) definuje *velké* množství dat.
- *Věrohodnost* (*Veracity*) se odkazuje na to, jak moc je možné datům důvěřovat vzhledem k důvěryhodnosti jejich zdroje.
- *Hodnota* (*Value*) koresponduje s monetární hodnotou, kterou společnost může získat z toho, že používá technologii *big data*.

Uvážíme-li rychlost dat, je možné zaznamenat, že, aby se to více zkomplikovalo, data mohou přicházet a vyžadovat zpracování v různých rychlostech: po dávkách v daných časových intervalech; téměř v reálném čase v malých a hodně frekventovaných časových intervalech; v reálném čase s nepřetržitým vstupem dat, zpracováním a výstupem; a v proudech datových toků. Zatímco pro některé aplikace je možné data a zpracování provést v dávkách, jiné analytické aplikace vyžadují nepřetržitou analýzu v reálném čase, kdy čas od času potřebují bezprostřední akci na základě zpracovávání vstupujících datových proudů. [9]

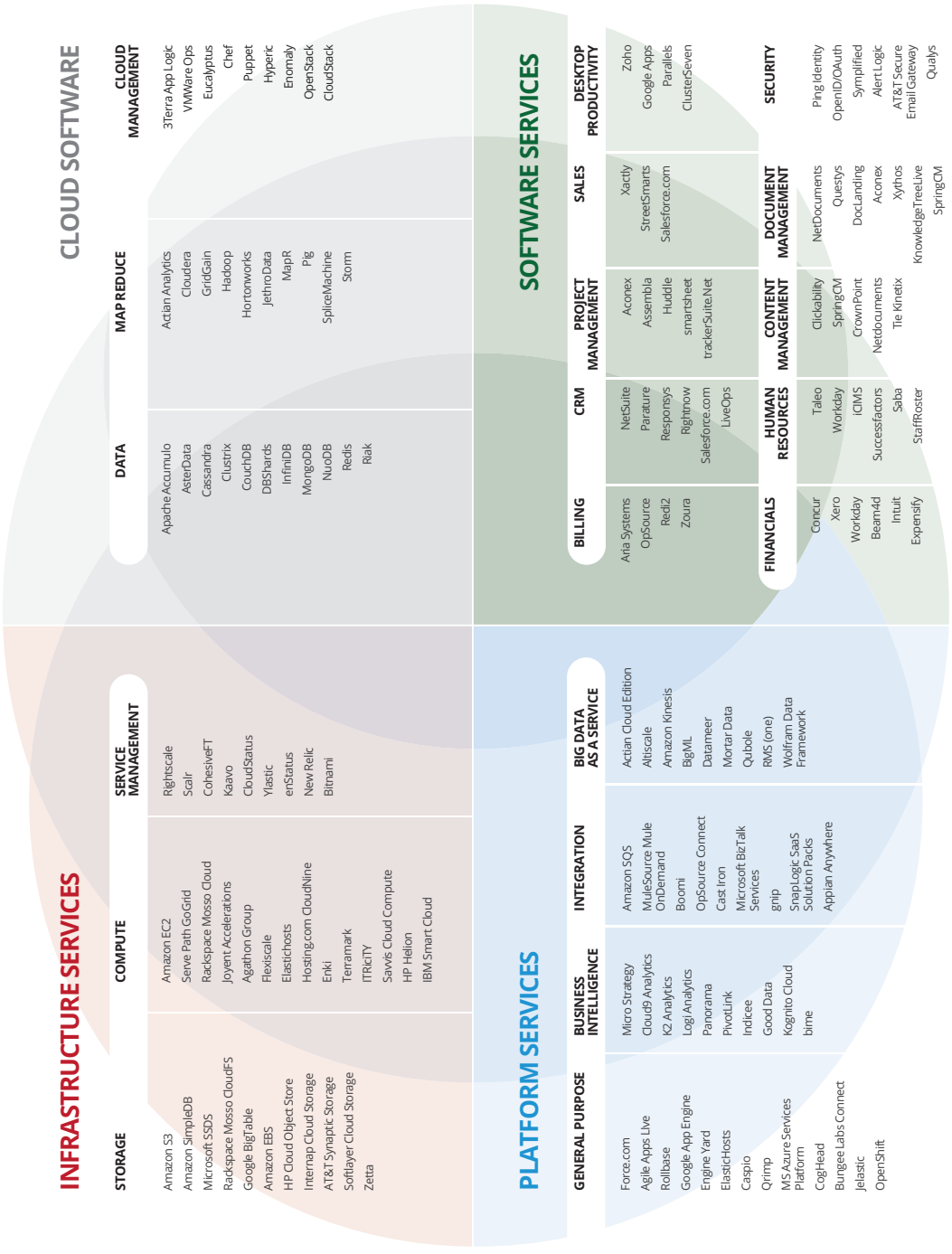
Technologie *big data*, která se zaměřuje na rychlost je známá jako technologie *fast data*, tedy vysokorychlostní datové proudy zpracovávané v reálném čase, nebo téměř v reálném čase. Primárním příkladem mohou být datové proudy ze senzorů, z burzy cenných papírů a třeba sociálních médií, jako jsou Twitter, Facebook, YouTube, Foursquare nebo Flickr. Bezpočet aplikací musí umět zpracovávat rychlá data, často s minimálním zpožděním a vysokou škálovatelností. Přitom běžné způsoby používané v technologii *big data*, jako třeba technika MapReduce v produktu Apache Hadoop, se nemusí pro tyto aplikace dobře hodit. Např. aplikace Firehose, která sleduje sociální síť Twitter pro informace o zemětřeseních, může vyžadovat relevantní informace v intervalu několika sekund od doby, kdy se objeví na síti Twitter informace o zemětřesení, a musí zvládat extrémně vysoké nárůsty objemu takových zpráv v síti Twitter během krátké doby. [69]

Nasazení technologie *big data* musí být realizováno v distribuovaném výpočetním prostředí pomocí paralelních algoritmů, aby byly schopny zvládnout vysoké rychlosti a objemy charakteristik používaných v technologii *big data*. Proto je technologie *big data* často implementována v rámci technologie *cloud computing*, obvykle jako jeden z modelů IaaS nebo

PaaS, kde poskytovatel nabízí distribuovanou IT infrastrukturu (např. výpočetní shluk /*cluster*/) nebo přímo služby výpočetních platforem užívaných v technologii *big data*, jako je např. Apache Hadoop či Apache Storm. Avšak, je možné se také setkat s nabídkou obecných ale i přizpůsobovaných služeb pro potřeby technologie *big data* zaměřené na analýzu, kdy se jedná o model SaaS. V takovém případě se může dokonce objevit nový model „Big Data ... as a Service“ (*velká data ... jako služba*), ostatně jak je znázorněno na obrázku 1.10.

1.3 Příklady technologie cloud computing v praxi

V minulosti byla technologie *cloud computing* rychle rostoucím průmyslovým odvětvím. Nyní existuje celá řada poskytovatelů technologie *cloud computing* a noví poskytovatelé se objevují spolu s novými tématy, které je třeba zpracovat, jako jsou například *big data*, IoT, apod. Taxonomie technologie „cloud“ dle institutu OpenCrowd [89] demonstruje software technologie *cloud computing* a řešení dostupná dnes pro modely jako IaaS, PaaS a SaaS (viz obrázek 1.11). Důkladná analýza a porovnání takového software a celkových řešení užívaných v technologii *cloud computing* bude náplní dalších kapitol.



Obrázek 1.11: Taxonomie technologie „cloud“ dle institutu OpenCrowd (převzato z [89]).

2 Technologie cloud computing ve výrobní organizaci

Technologie *cloud computing* přináší nové možnosti pro výrobní organizace. Výrobní organizace, které úspěšně zvládly moderní technologie v produkci, jsou připraveny adoptovat také technologii *cloud computing*. Technologie *cloud computing* se rychle přesouvá od průkopníků technologie k hlavnímu proudu uživatelů. Krom toho, globalizované výrobní organizace se začínají chovat podle filozofie Navrhni a vyrob kdekoliv (anglicky „Design Anywhere, Manufacture Anywhere“) (DAMA) (viz [55]), která vyžaduje schopnosti přesunout návrhářské a výrobní síly v krátkém čase, aby bylo možné reagovat na změny na trhu.

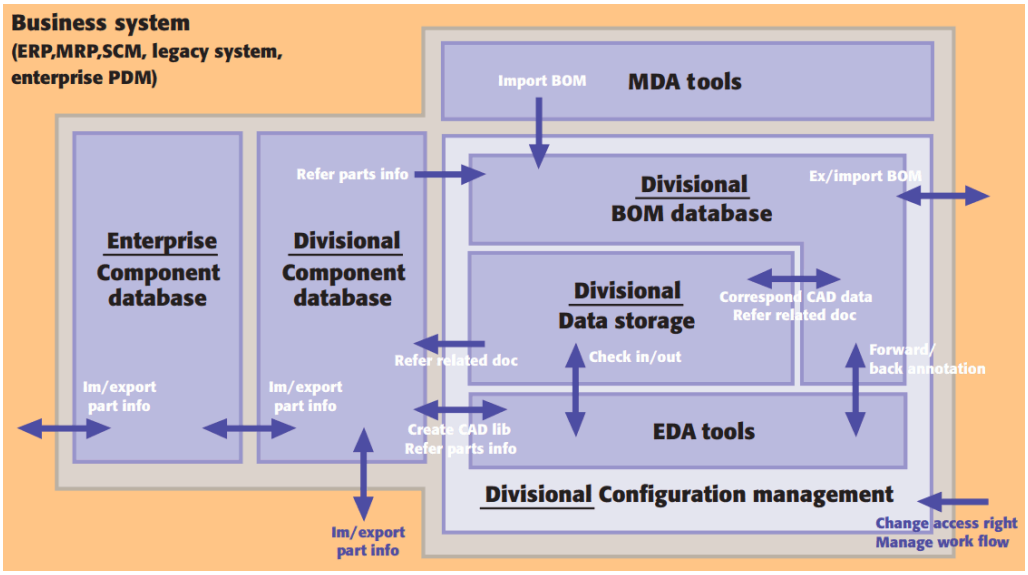
Přijmutí filozofie DAMA přináší další důvod pro užití technologie *cloud computing*, jelikož tam, kde je zapojeno do nějakého projektu více poboček, exponenciálně vzrůstá složitost managementu informací potřebná pro úspěšné uvedení produktu. Také je potřeba zvláštní IT systémy a infrastrukturu propojující různé části podniku. Mezi ně patří plánování potřeby výrobních zdrojů (anglicky „manufacturing resource/requirements planning“) (MRP), plánování podnikových zdrojů (anglicky „enterprise resource planning“) (ERP), plánování inženýrských zdrojů a řízení vztahů se zákazníky (anglicky „customer relationship management“) (CRM). Stejně tak je ale nutná vertikální integrace mezi jednotlivými součástmi, jak ukazuje obrázek 2.1.

Chytrá výroba s technologiemi cloud computing a cloud manufacturing jsou dva způsoby, jak adoptovat technologii *cloud computing* ve výrobním sektoru [126]. Prvním způsobem je výroba s přímým uplatněním nějaké součásti technologie *cloud computing*, kde uplatnění je typicky založeno na aplikacích pro procesní řízení (anglicky „Business Process Management“) (BPM) jako lidské zdroje (HR), CRM a ERP. Druhý způsob je výrobní verze technologie *cloud computing*. Technologie cloud manufacturing (CMfg) je definována ve [126] jako prosté odzrcadlení definice technologie *cloud computing* podle National Institute of Standards and Technology (NIST)[1]

Na rozdíl od chytré výroby s využitím technologie *cloud computing*, které obvykle nabízí služby v modelech software-jako-služba (anglicky „Software as a Service“) (SaaS) či platforma-jako-služba (anglicky „Platform as a Service“) (PaaS), technologie CMfg je více technologicky orientována a tedy typicky zavádí služby na nižších úrovních modelů jako je PaaS či infrastruktura-jako-služba (anglicky „Infrastructure as a Service“) (IaaS). Pro příklad technologie CMfg viz sekci 1.2.2.

Tato kapitola bude diskutovat jak chytrou výrobu založenou na technologii *cloud computing*, tak technologii CMfg se zaměřením na jejich aplikace v automobilovém a elektronickém průmyslu.

[1] původní definici technologie *cloud computing* dle NIST je možné nalézt v sekci 1.1 pro technologii *cloud computing* jako „model pro nabízení všudypřítomného přístupu k síti na vyžádání tak, aby bylo možné přistupovat ke sdílenému zdroji konfigurovatelných výpočetních zdrojů (např. sítí, serverů, datových úložišť, aplikacím, jiným službám). Přitom jde o to, že tyto zdroje jsou poskytovány rychle a rychle uvolňovány v případě nepotřeby, a to s minimálním úsilím či interakcí poskytovatele.“



Obrázek 2.1: Struktura systému implementujícího filozofii DAMA (převzato z [55]).

2.1 Technologie cloud computing v automobilovém a elektronickém průmyslu

Globalizace elektronického průmyslu přinesla mnoho výzev pro společnosti, které vyrábějí elektronické produkty (v širším významu tohoto slovního spojení). Přičemž zdaleka ne nejmenší odvětví je sdílení informací uvnitř podniků a s jejich partnery z oblasti návrhu a výroby, kteří se mohou nacházet kdekoliv na světě, podle toho, jak to vidí filozofie DAMA. Bez efektivního sdílení informací by se podniky dostaly do zmatečných situací, reagovaly by pomalu a, konec konců, nekompetentně. Proto návrh elektronického produktu a jeho výroba nemohou probíhat izolovaně. Nutné vazby mezi databázemi komponent, účty za materiál, nástroji pro návrh, managementem procesu návrhu, nástroji pro návrh strojních částí a daty o produktu jsou již tak složité. Přitom stále platí, že komunikace mezi návrháři zapojení a návrháři fyzického rozložení komponent je často nedokonalá; je to o to horší, že návrháři zapojení i fyzického rozložení spolupracující na stejném úkolu přitom mohou sedět naproti sobě a vzájemně si předávat nanicovaté kusy papíru. [55]

Podobnou úvahu, jako byla popsána výše ve [55], je možné aplikovat také na automobilový průmysl. Pokud projdeme řetězec výroby v automobilovém průmyslu, tak vidíme fáze jako návrh, dodavatelé, sestavení, koncový prodej a servis prodaných vozů. V takovém řetězci je mnoho příležitostí pro technologii *cloud computing*, jak to vidí [49]. Tyto příležitosti, spolu s možnými hrozbami, budou diskutovány v následujících sekcích. Než budou prezentovány samotné příležitosti, je nutné ale kriticky posoudit nedávný rozvoj a budoucí trendy v technologii *cloud computing*, zejména v oblasti automobilového (a elektronického) průmyslu. Toto bude učiněno jak pro chytrou výrobu založenou na technologii *cloud computing*, tak pro technologii CMfg.

2.1.1 Chytrá výroba založená na technologii cloud computing

Chytrá výroba založená na technologii *cloud computing* je především to, že z obchodního hlediska využívá služby modelu SaaS, který poskytuje hotová řešení pro management podniků nebo služby modelů PaaS/IaaS pro lepší nasazení již existujících technických řešení, jako jsou např. podnikové informační systémy, či samostatné databázové systémy, WWW

prezentace a webové portály, či elektronické obchody pro zaměstnance, obchodní partnery a samotné zákazníky. Z tohoto úhlu pohledu potřebují organizace v automobilovém či elektronickém průmyslu stejné služby technologie „cloud“ jako organizace mimo tyto obory, tedy potřebují aplikace pro BPM zaměřené na lidské zdroje (HR), CRM, a ERP. Krom toho, existují speciální aplikace, např. pro plánování výroby, pro spolupráci řetězce dodavatelů, pro skupinový návrh/design, pro simulace, apod.

Technologie *cloud computing* může přinést následující technologie, které pomáhají naplnit obchodní požadavky:

Procesní řízení (anglicky „Business Process Management“) (BPM) – SaaS

Velké společnosti stejně jako pokročilé malé a střední podniky musejí monitorovat a řídit své obchodní procesy. Technologie BPM typicky pomáhá řídit obchodní strukturu organizace a řídit konzistenci a bezpečnost obchodních procesů pro jejich účastníky. Technologie BPM zahrnuje aplikace jako CRM, správa pracovních výkonů (anglicky „workforce performance management“) (WPM), ERP, sledování podnikových aktivit (anglicky „business activity monitoring“) (BAM), portály elektronického obchodování a další. V technologii „cloud“ je technologie BPM poskytována obvykle v modelu služeb SaaS, které zvyšují flexibilitu, možnost spouštět a dovolit si zafinancovat i komplexní aplikace pro velké podniky [97]. V řadě případů přenos technologie BPM do technologie „cloud“ jakožto služby typu SaaS může umožnit lepší monitorování a řízení obchodních procesů a zvýšit znovupoužitelnost těchto procesů a jejich částí, které pomáhají podnikům maximalizovat jejich zisky, nebo zavádět některé z inteligentních/inovativních obchodních procesů, jako situační obchodní procesy [39], upravené tak, aby zvládaly nové obchodní situace: nové iniciativy, nové kampaně, nové projekty.

Příkladem technologie BPM v prostředí technologie „cloud“ může být technologie BPM firmy IBM zvaná „BPM on Cloud“[2], či služba NetSuite[3], nebo Salesforce[4].

Migrace dat a vyvažování zátěže – PaaS/IaaS

Distribuce informací k uživatelům webu efektivně a s efektivně vynaloženými náklady je náročný problém, zejména při vzrůstajících požadavcích, které vyvstávají z různých moderních aplikací, např. VoIP (přenos hlasu přes sítě typu IP), nebo přenos mediálních dat. Více a více aplikací (např. elektronické obchodování) spoléhá na Internet, ale s vysokou citlivostí na zpoždění. Zpoždění byť jen pár milisekund na webovém serveru může být netolerovatelné. Technologie síť pro doručování obsahu (anglicky „content distribution network“) (CDN) byla vyvinuta na to, aby podobné náročné úlohy řešila. Dělá to prostřednictvím škálovatelného mechanismu na urychlení dodání obsahu webového serveru, přitom s efektivně vynaloženými náklady [117].

Zatímco technologie CDN mohou být považovány za služby PaaS/IaaS technologie „cloud“, tak migrace dat do technologie „cloud“ vyžaduje pokročilejší služby, které zaručí následující cíle [97]:

- *Žádná ztráta dat*: systém musí zajistit, že s vysokou pravděpodobností nedojde k trvalé ztrátě dat.
- *Vysoká dostupnost*: data musejí být dostupná uživatelům/vlastníkům s rozumně vysokou pravděpodobností, kdykoliv je potřebují, i když zřídkavé dočasné výpadky jsou

[2] `https://www.bpm.ibmcloud.com/`
[3] `http://www.netsuite.com/`
[4] `https://www.salesforce.com/eu/`

přijatelné.

- *Vysoký výkon*: systém by neměl mít v oblasti výkonnosti výrazně horší chování než současné běžně užívané alternativy, jako např. NFS.

- *Škálovatelnost*: systém musí škálovat na velký počet klientů, velký počet „uzlů“ datových úložišť, velká agregovaná úložiště, atd.

- *Efektivní vzhledem k nákladům*: jelikož v současnosti existují levná řešení umožňující koupit větší a spolehlivé úložiště, systém nesmí být nákladný ani na hardware, ani software, ani na údržbu.

- *Bezpečnost*: systém musí být schopen zaručit důvěrnost a integritu dat a autorizační standardy, které uživatelé očekávají. Toto je zejména náročné, pokud víme, že data budou uložena na vzdálených strojích uvnitř technologie „cloud“ nějakého poskytovatele.

Většinu z těchto cílů je možné dosáhnout nákupem řešení úložiště-jako-služba (anglicky „Storage as a Service“) (StaaS) u známých poskytovatelů. (Většinu z nich technologicky vidíme jako model služeb PaaS.) Avšak, v některých případech, například z bezpečnostních důvodů, může být nutné, aby podnik sám provozoval jejich vlastní virtualizovaný softwarový balík v technologii „cloud“ jakožto službu IaaS. (V tomto případě bude bezpečnostní hledisko diskutováno podrobněji v sekci 2.3.) Řešení StaaS a technologie CDN se mohou hodit v případech specifických řešení běžících jako služba modelu IaaS. Tak bude zajištěno vyvažování zátěže a výpadky z důvodů omezených zdrojů, poruch, údržby, atd.

Příkladem řešení technologie CDN může být produkt Akamai[5] nebo od společnosti Amazon produkt CloudFront[6]. V případě technologie na bázi služeb StaaS je populárním poskytovatelem společnost Amazon a jejich „Amazon Simple Storage Service“ (S3)[7] či od společnosti Google jejich „Cloud Storage“[8].

Virtualizace – PaaS/IaaS

Virtualizací míníme abstrakci logických zdrojů od jejich fyzických prvků za účelem zlepšení hbitosti, flexibility, snížení nákladů a tak zvýšení obchodní hodnoty. Virtualizace zejména obnáší správu určitého počtu virtualizačních strojů běžících v příslušných operačních systémech, vyhodnocování a testování serverů, spouštění cílových aplikací, apod. K základním sledovaným aspektům patří centrální procesorová jednotka (anglicky „central processing unit“) (CPU), správa paměti a vstupy/výstupy (vstup/výstup (anglicky „input/output, I/O“) (V/V)), které mají největší vliv na výkon, spolehlivost a kompatibilitu. Virtualizace v prostředí technologie „cloud“ zahrnuje i virtualizaci serverů, aplikací klientských i pro desktop, úložiště (*Storage Area Network*), sítě (privátní a softwarově definované sítě, tedy VPN, SDN), služeb a aplikační infrastruktury. Virtualizace se tedy dobře hodí do dynamické infrastruktury technologie „cloud“, protože poskytuje důležité výhody při sdílení vybavení v prostředí technologie „cloud“, správě komplexních systémů, jako i oddělení dat a aplikací. Navíc, důležitým prvkem je zjištění, zda jsou, či nejsou, datová centra přimknuta k určitému operačnímu systému, pokud zvolíme určitý typ virtualizace. [117]

[5] `https://www.akamai.com/`
[6] `https://aws.amazon.com/cloudfront/`
[7] `https://aws.amazon.com/s3/`
[8] `https://cloud.google.com/storage/`

Pro podniky je virtualizace pravděpodobně tou nejzajímavější vlastností technologie *cloud computing*. Je to proto, že jim umožňuje jednoduše přenést existující „staré“ systémy do prostředí technologie „cloud“, lépe škálovat a snížit náklady na údržbu hardware (a systémového software). Toto je důležité zejména pro výrobní průmysl, kde je obvykle v činnosti spousta „starých“ systémů, které není možné nahradit, nebo znovu implementovat z řady důvodů (licence, proprietární části, závislost na systémech třetích stran, zastaralé technologie, vysoké náklady, apod.). V mnoha případech je možné takové systémy přesunout bez další modifikace do virtualizovaného prostředí za předpokladu, že virtualizace dostatečně emuluje původní běhové prostředí přenášených systémů.

Z pohledu uživatele služeb technologie „cloud“ je možné virtualizaci rozdělit na řešení PaaS nebo IaaS. V případě modelu služeb PaaS poskytuje technologie „cloud“ jednotlivé virtuální softwarové komponenty, které je možné použít pro sestavení virtualizovaných systémů (např. virtuální „HTTP Server“ od Apache, nebo virtuální databáze MySQL/Oracle, která se chová stejně, jako fyzická instance). V případě modelu služeb IaaS je virtualizace realizována na hardware, nebo operačním systémem, kam se virtualizovaný systém instaluje, či spouští. Je to stejné jako pro fyzický hardware nebo jako fyzická instalace operačního systému. Příkladem realizace služby v modelu PaaS může být „Heroku Cloud Application Platform“[9], pro model IaaS to může být „Elastic Compute Cloud“ (EC2)[10] společnosti Amazon.

Monitorování a analýza v technologii big data – SaaS/PaaS

Podle McKinsey&Company je výroba intenzivní užívání technologie *big data*, kde užívání obrovských datových sad vede k objevování nových vzorů, provádění simulací a správě komplexních systémů v reálném čase. Výroba ukládá mnohem více dat než jakýkoliv jiný sektor a to odhadem dva exabajty (tedy dva triliony bajtů, 10^{18} bajtů) pro rok 2010. Tím, že je možné provádět sofistikované simulace, které odhalí poruchy v raném stádiu, pomohla technologie *big data* firmám Toyota, Fiat, či Nissan zkrátit čas potřebný pro vývoj nových modelů o 30 až 50%. [13]

V moderním výrobním průmyslu jsou data generována z monitorování strojů a zařízení, řešení odvozených od technologie „cloud“, obchodního managementu, atd. Tato data je nutné zpracovávat v reálném čase a ukládat pro pozdější analýzy. Krom technologií jako *cloud computing* pro BPM, úložiště dat, virtualizace, apod. potřebuje technologie *big data* specifické techniky a metody pro jejich ukládání, zpracování a analýzu. Existují modely služeb pro technologii *cloud computing* přímo se zaměřující na podporu technologie *big data*, jak je například popsáno v sekci 1.2.3. Nicméně, analýza pro výrobní průmysl založená na technologii *big data* má své konkrétní cíle a aplikace, jako je technologie virtuální továrna (anglicky „virtual factory“) (VF) pro simulaci reálné továrny, nebo předvídání a řízení provozního stavu zařízení (anglicky „prognostics and health management“) (PHM) pro kyber-fyzikální systémy (výrobní stroje, zobecnění pojmu internet věcí (anglicky „Internet of Things“) (IoT)). Navíc, monitorování obchodních a produkčních procesů produkuje taktéž velký objem dat, která jsou zpracovávána pro BAM a pro rozhodovací procesy prováděné lidskými operátory vedoucí k optimalizaci výroby skrze sady pravidel a jejich zpracování.

Technologie Virtuální továrna (anglicky „virtual factory“) (VF) je definována v [62] jako čtyři dimenze:

[9] `https://www.heroku.com/`
[10] `https://aws.amazon.com/ec2/`

- *Simulace reálné továrny* pro simulované síťově plánování a řízení výrobních procesů za pomocí digitálních modelů, které byly převzaty z výrobních společností. Například, společnost Ford Motor Company implementovala vlastní systém virtuální továrny pro továrny v Evropě, aby tak zlepšila efektivitu montážní linky tím, že si udělala dopřednou prohlídku a optimalizaci systémů pomocí simulace a virtuálního prostředí, nebo společnost Volvo Group Global vyvinula nástroje pro tvorbu virtuálních továren pro validaci změn před tím, než jsou skutečně do dané továrny zavedeny. Odpovědní ředitelé mohou provést několik tisíc simulací různých konceptů, aby vyhodnotili tok procesů, pohyby robotů a stresující a rizikové faktory mající vliv na lidi před tím, než je továrna postavena.

- *Virtuální organizace* definovaná jako spojení několika reálných továren v různých místech výrobní sítě. Cílem je spojené monitorování procesů, identifikace a řešení problémů, výkonnostní metriky komunikace a sdílení mezi participujícími společnostmi virtuální továrny.

- *Reprezentace ve virtuální realitě* jako 3D prostředí, které je navrženo pro simulace, vizualizace, komunikaci a spolupráci prostřednictvím sítě, v reálném čase, pomocí 2D a 3D informací o továrně a jejích procesech. 3D reprezentaci je možné použít na monitorování procesů, virtuální inspekce, kontrolu inventáře, zákaznické prohlídky, výuku a trénink. Také je tak možné získat výkresy, plány procesů, statistiky o vybavení a procesech, případně další informace o výrobě.

- *Vybavení pro emulaci* na bezpečné simulace reálných produkčních procesů. Zejména je vhodné pro experimentální změny výrobních aktivit pomocí modelování za použití simulace diskrétních událostí (anglicky „discrete event simulation“) (DES) pro aktivity ve virtuální továrně s tím, že data jsou poskytnuta ze senzorů z reálných procesů řízených skutečnými řídicími systémy.

Programové vybavení pro návrh produktů, systémů a procesů, nebo pro simulace či vizualizace ve virtuální továrně je poskytováno hlavními prodejci z oblasti automatizace továren, jako např. Dassault Systèmes[11], Siemens PLM[12] a PTC[13].

Předvídání a řízení provozního stavu zařízení (anglicky „prognostics and health management“) (PHM) poskytuje přehled o budoucí výkonnosti vybavení a odhady o době do selhání strojů ve výrobě. Takto redukuje vliv nejistoty tohoto druhu a dává uživatelům možnost proaktivně implementovat řešení jako prevenci proti ztrátě výkonnosti výrobních systémů [71]. Podle [70] je nutné vytvořit algoritmus na pozorování změn stavu strojů a odvození nové informace na základě historie, aplikovat porovnání se stejnými stroji a předat výstupy do další úrovně (zpracování/rozhodování). Změna stavu stroje může být definována jako dramatická odchylka v jeho provozuschopnosti, zásah údržby, nebo změna pracovního režimu.

Během životního cyklu stroje (či sestavy) se ukládají snímky stavu stroje a používají se pro vytvoření historie stavu stroje v čase. Ta bude použita pro párové porovnání mezi stroji. Poté algoritmus na unifikaci vzorů prohledá historické záznamy, aby našel podobnost se současným chováním a porovnal využití a pracovní stav stroje. Nakonec dojde k predikci užitečné doby života daného stroje a pomůže tak včas naplánovat údržbu stroje a strategii údržby v celé výrobní hale. Krom toho, predikce doby života spolu s historickými záznamy

[11] `https://www.3ds.com/`
[12] `https://www.plm.automation.siemens.com/`
[13] `https://www.ptc.com/`

mohou pomoci zlepšit využití stroje na základě jeho aktuálního stavu. Historie využití podobných sestav v různých stavech provozuschopnosti potom poskytuje informaci pro simulaci možných budoucích využití dané sestavy a výsledků plynoucích z takových využití. Mezi těmito využitími jsou potom vybrána ta, která nabízejí nejefektivnější a přitom stále produktivní využití dané sestavy. [70]

2.1.2 Výroba prostřednictvím technologie cloud computing

Podle [3] je technologie CMfg založena ideově na modelu služeb výroba-jako-služba (anglicky „Manufacturing as a Service“) (MaaS), který představuje vhodné a jednolité sdílení různých druhů výrobních zdrojů jako služby pro všechny fáze výrobního cyklu produktu. V technologii CMfg jsou hlavně tři typy účastníků či uživatelů: (1) uživatel se záměrem vyrábět, (2) poskytovatel, který má zdroje na pokrytí takové výroby, nebo aspoň části té výroby, (3) operátor mezi nimi, který sehrává organizaci požadavků a dostupných zdrojů tak, aby do sebe úspěšně zapadly požadavky a zdroje. Zdroje poskytovatele, které jsou v technologii CMfg jsou dvojího typu: fyzické výrobní zdroje a výrobní možnosti (někdy také odkazovány jako „schopnosti“).

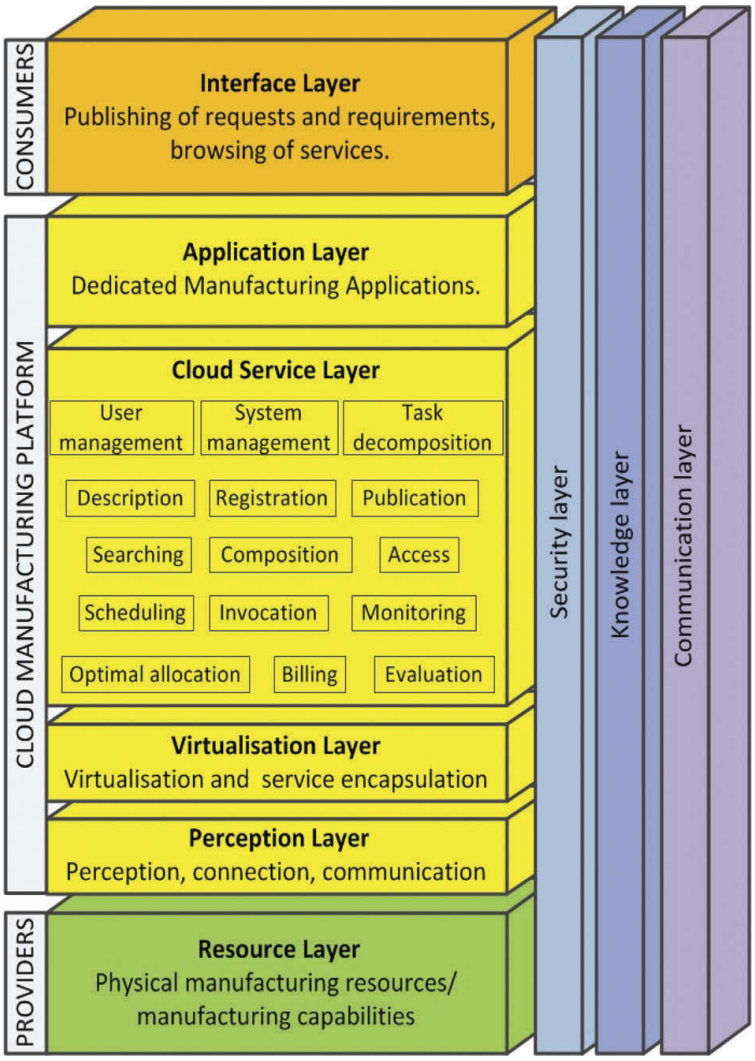
Fyzické zdroje mohou být jednak pevné (výrobní vybavení, počítače, sítě, servery, materiál, vybavení pro dopravu a skladování), nebo měkké (např. aplikace, software na design a simulaci, analytické nástroje, modely, data, standardy, lidské zdroje, jako třeba osoby různých profesí, znalostí, dovedností a zkušeností). Výrobní možnosti jsou nehmotné a dynamické zdroje, které reprezentují možnosti/schopnosti organizace uskutečnit konkrétní úkol nebo operaci kompetentně, za použití fyzických zdrojů (např. design produktu, simulace, výroba, management, údržba, komunikace). Jsou to výrobní možnosti, které určují, zda je možné dosáhnout požadavků pomocí výrobních zdrojů v průběhu vývoje produktu. Jak výrobní zdroje tak možnosti jsou následně virtualizovány a zaobaleny jako výroba prostřednictvím technologie *cloud computing*. Takto vzniklé služby jsou dostupné na požádání, jsou konfigurovatelné a soběstačné, aby pokryly uživatelské potřeby. Výrobní software (SW), aplikace a infrastruktura tak mohou být realizovány jao služby v technologii CMfg. Podobně, jako výpočetní zdroje jsou zajištěny v různých strukturách pro porovnávací kritéria (anglicky „comparison criteria, CC“) (PK) [3].

Nad fyzickými výrobními zdroji a nad výrobními možnostmi je platforma technologie CMfg, která je spolu s několika vrstvami zodpovědná za naslouchání (objevování a propojování), virtualizaci (poskytuje rozhraní pro virtualizaci), management (jejich zaobalení jak služby technologie „cloud“), agregaci a kompozici (do výrobních služeb v technologii „cloud“), no a za publikování směrem ke konzumentům. Pro všechny tyto vrstvy, bezpečnostní opatření, sdílení a management znalostí a komunikaci platí, že musejí být zajištěny podpůrnými vrstvami, jak ukazuje obrázek 2.2.

V současnosti je technologie CMfg předmětem probíhajícího výzkumu a mnoha výzkumných iniciativ, projektů a konsorcií s jak akademickými tak průmyslovými partnery. Cílem těchto aktivit je realizovat a vyhodnotit koncepty technologie CMfg v praxi. Například, tyto nedávné iniciativy mohou být zajímavé z pohledu automobilové/elektronické výroby v rámci Evropské unie[14]:

- ManuCloud (Infrastruktura pro specifikaci a realizaci dodavatelsko-výrobního řetězce v distribuované technologii „cloud“) [123]
- Diversity (Technologie CMfg a prostředí pro kontextové inženýrství ve vztahu produkt-služba založené na sociálním software určené distribuovaným podnikům)

[14] další dlouhý seznam výzkumných trendů, publikací a iniciativ je poskytován v [3]



Obrázek 2.2: Konceptuální architektura technologie Cloud manufacturing (CMfg) (převzato z [3]).

[33]

- CREAM (Rychlá a pružná výroba založená na technologii „cloud“) [29]
- SMARTER (Trvale udržitelné adaptivní služby s technologií „cloud“ pro podnikovou sféru) [108]
- cloudSME (Simulace pro výrobu a inženýring) [27]

Mnoho prodejců služeb technologie „cloud“ sebe deklaruje i jako poskytovatele technologie CMfg. Například to jsou NetSuite[15], Plex [16], KeyedIn[17], Scytex[18], Hai[19], Rootstock Software[20], QAD[21], Hudman[22]. Avšak, přes všechny jejich deklarace, většina prodejců ve skutečnosti neposkytuje služby technologie CMfg, ale chytrá výrobní řešení založená na technologii *cloud computing*, obvykle jako ERP v rámci modelu služeb SaaS.

Krom toho, existují jednotlivá otevřená nebo proprietární řešení technologií a standardů, která umožňují postavit technologii CMfg tím, že je vybudována standardní komunikační sběrnice a rozhraní pro stroje, aby bylo možné je zahrnout jako služby technologie „cloud“ typu stroj-jako-služba (anglicky „Machine as a Service“). Například lze mezi ně zařadit MTConnect[23], OCCI[24], UN/EDIFACT[25], ebXML[26], MyOpenFactory[27], RosettaNet[28], SEMI EDA/Interface A[29].

Vybraná řešení pro technologii CMfg pro automobilový/elektronický průmysl budou diskutována v kapitole 3.

2.2 Příležitosti a hrozby technologie cloud computing

Implementace technologie „cloud“ pro potřebu výroby provedená na „zelené louce“ a přechod z dobře zavedených výrobních a obchodních systémů na jejich realizace v prostředí technologie „cloud“ přináší pro výrobní organizaci mnoho příležitostí, ale také řadu hrozeb. V této sekci budou identifikovány příležitosti a hrozby a budou analyzovány jejich možné efekty a případná protiopatření. Tento text bude vycházet z již uvedeného a z odkazovaných publikací, např. [8, 74, 49, 3]. Bezpečnostní rizika a hrozby jsou náplní sekce 2.3.

2.2.1 Obecné příležitosti

O1 – Nízká počáteční investice: Jedna z významných příležitostí technologie *cloud computing* leží v jejím potenciálu pomoci rozjíždějícím se organizacím využít výhod IT v jejich obchodní činnosti bez výrazných vstupních nákladů. Místo velkých vstupních investic, které byly nutné před technologií *cloud computing*, jako nákup informačních a výrobních

[15] http://www.netsuite.com/portal/industries/manufacturing.shtml
[16] https://www.plex.com/
[17] https://www.keyedin.com/manufacturing/
[18] https://scytec.com/dataxchange-overview/
[19] http://www.hai.nl/
[20] http://www.rootstock.com/manufacturing-cloud-erp/
[21] https://www.qad.com/cloud
[22] https://www.hudmansolutions.com/
[23] https://www.mtconnect.org/
[24] https://occi-wg.org/
[25] http://www.unece.org/trade/untdid/texts/unredi.htm
[26] http://www.ebxml.org/
[27] https://www.myopenfactory.com/
[28] https://resources.gs1us.org/RosettaNet
[29] https://www.cimetrix.com/InterfaceA

SW systémů, sestavení SW infrastruktury, technologie *cloud computing* vyžaduje výrazně nižší vstupní náklady. Toto platí zejména pro model služeb SaaS, který je možné využít bez jakékoliv přípravy. Služby technologie „cloud" jsou využívány dle okamžité potřeby a placeny podle využití (průběžné platby po dobu využívání). Nízké vstupní náklady mají význam pro malé společnosti, které mohou využít aplikace jako ERP nebo obchodní analýzu, jenž je typicky nabízena jako služba modelu SaaS, nicméně i velké společnosti mohou zkusit rozličné inovace bez vysokých nákladů.

O2 – Outsourcing a management IT služeb: Pokud chce organizace sama, svými prostředky, svým IT oddělením, poskytovat služby IT, tak musí zavést management IT služeb. To znamená i vývoj nových IT služeb podle měnících se potřeb koncových uživatelů, přes přechod na tyto nové služby v praxi, až po jejich údržbu a vylepšování po dobu jejich správy. Zatímco procesy pro management IT služeb jsou dobře popsány a nacházejí se v řadě dobře zavedených metodologiích, např. ITIL či ISO/IEC 20000[30], jejich implementace vyžaduje specializované zaměstnance, procesy a infrastrukturu (např. pro zálohování a obnovu ze záloh, výměnu chybných IT komponent za běhu, správu konfigurací, apod.), které musejí dobře zapadat do celkové struktury organizace. Na rozdíl od toho, z pohledu koncového uživatele, dobře definované řešení v technologii *cloud computing* je snadno udržovatelné bez dalších IT znalostí a vybavení.

O3 – Složeniny: Schopnost rychle zkombinovat data, nebo funkcionality ze dvou či více externích zdrojů za účelem vytvoření nové „složené" služby originálním a neotřelým způsobem reprezentuje další příležitost v technologii *cloud computing*. Technologie *cloud computing* lépe adresuje potřeby agilního vývoje a agilního obchodu, protože je poměrně snadné vzít několik služeb technologie „cloud", nějaké nástroje a vytvořit z nich novou instanci technologie „cloud" narychlo, než vyvíjet aplikaci od začátku. Například je možné vzít několik specializovaných služeb privátní technologie „cloud" v modelu data-jako-služba (anglicky „Data as a Service") (DaaS) a veřejnou službu z technologie *big data* v modelu analýza-jako-služba (Analytics-as-a-Service), spojit je a rychle vytvořit hybridní službu pro analýzu dat v reálném čase. Pokud bychom neměli technologii *cloud computing*, tak vytvoření takové případové studie by bylo náročné na realizaci bez specializovaného SW, IT infrastruktury a velkých investic.

O4 – Lepší IT architektura: I pro IT organizaci je velmi náročně postavit dobrou, rozšiřitelnou a škálovatelnou IT architekturu, tím horší je to pro výrobní organizaci mimo, nebo jen částečně v IT. Tím, jak se přidávají další modifikace IT systému po dobu jeho života, jeho architektura se stává „náhodnou". Podle [19] je zamýšlená architektura nejdříve explicitně navržena a pak implementována; náhodná architektura se objevuje na základě mnoha nezávislých rozhodnutí, která se objevují v průběhu nasazení. Odtud tedy to pojmenování. Takovýto „náhodný" vývoj určitě zvýší složitost architektury a náklady na její údržbu. Také to může vést až k degradaci architektury do chybového stavu. Toto ovšem není typická situace u technologie *cloud computing*, kde rozhraní a závislosti mezi službami technologie „cloud" musejí být dobře popsány. Je také mnohem snazší znovu sestavit, či dokonce zahodit celou architekturu, nebo její část (náklady na opakovaný vývoj jsou minimální v porovnání s řešeními mimo architekturu „cloud").

O5 – Škálovatelnost: Škálovatelnost je schopnost jednoduše rozšířit, nebo zúžit systém dle okamžité potřeby a to tak rychle a efektivně, jak jen to je možné. To znamená řízeným

[30] `http://itil.co.uk/` a `https://www.iso.org/standard/51986.html`, respektive

způsobem a za minimální cenu. Toto je velmi problematická situace, protože systém musí mít k dispozici více prostředků, než jich skutečné využívá, když je ve zúženém stavu, zatímco se mu jich může nedostávat, pokud je v nejširším možném rozložení. Ať tak, nebo tak, vždy je využití zdrojů vlastně neefektivní (nadbytek/přetížení). Proto je škálovatelnost považována za velkou výhodu technologie *cloud computing*. A to proto, že rozšíření či zúžení počtu využívaných služeb se děje prakticky okamžitě a zákazník vždy platí jen tolik peněz, které odpovídají okamžité spotřebě služeb v technologii „cloud".

O6 – Energetická efektivita (zelené IT): Přesunem do technologie „cloud" může organizace redukovat svoji vlastní IT infrastrukturu. Virtualizovaná IT infrastruktura stále závisí na fyzickém HW, ale tento HW je umístěn u poskytovatele, kde je možné ho optimálně využít. Navíc, pokud dojde k modifikaci IT infrastruktury z důvodu požadavků nové aplikace, nebo jen k rozšíření či zúžení stávající aplikace, je to levnější z hlediska environmentálních zdrojů provést na virtuální, než na fyzické IT infrastruktuře. Konečně, transport počítačových služeb od producenta ke konzumentovi je mnohem efektivnější, než třeba to samé s elektřinou.

2.2.2 Příležitosti pro automobilovou výrobu a výrobu elektroniky

O7 – Připojené vozidlo: Moderní automobily jsou vybaveny vysokým počtem elektronických systémů se senzory, které generují velký objem diagnostických a transakčních dat. Vozidlo, pokud je připojené, může nahrát tato data do externího úložiště, poskytnout výrobci, nebo zaslat servisnímu centru pro další analýzu. V současnosti jsou data nahrávána obvykle v průběhu roční prohlídky vozidla, nebo jeho údržby. Pokud je vozidlo připojené do technologie *cloud computing*, data mohou být nahrávána nepřetržitě a, kromě běžné analýzy jednotlivých vozidel, výrobce může aplikovat techniky z technologie *big data* (např. dolování z dat) pro získání dalších informací na vylepšení služeb v takových oblastech jako CRM, marketing, kvalita, zákaznické služby, pozáruční služby, nebo uskutečnit libovolný výzkum a vývoj. Kromě toho, s využitím technologie *fog computing*, se může vozidlo samo, nebo jeho elektronické moduly, chovat jako služba na hraně (edge) a přímo se tak podílet na technologii „cloud/fog" (s určitou mírou zabezpečení). Např. je to možné využít pro telematiku, vzdálenou digitální údržbu, nebo pro informační a zábavní služby. V současnosti je technologie *cloud computing* pravděpodobně jediná, která umožňuje efektivně implementovat výměnu dat a služeb mezi tak velkým množstvím zařízení.

O8 – Agilní výroba (flexibilita): Vysoká a řízená flexibilita je ve výrobě chtěná vlastnost. Dle [128] by agilní výroba měla zajistit: vysokou kvalitu a vysokou zákaznickou variabilitu produktů; produkty a služby s vysokou informační a přidanou hodnotou; mobilizaci klíčových kompetencí; odpovědnost k sociálním a environmentálním otázkám; syntézu rozmanitých technologií; odpověď na změnu a nejistotu; mezi- a vnitro-podnikovou integraci. Technologie CMfg, jak byla definována v sekci 2.1.2, mnoho z těchto požadavků může naplnit. Například, robotika založená na technologii „cloud" přináší lepší monitorování, automatickou optimalizaci a rychlejší rekonfigurovatelnost robotizovaných výrobních linek.

O9 – Lepší monitorování (transparence): Kromě lepšího řízení a integrace, umožňuje technologie „cloud" pro výrobu také lepší monitorování. Jednotlivé stroje podílející se na výrobě se mohou tvářit jako služby technologie „cloud" podle modelu služeb stroj-jako-služba (anglicky „Machine as a Service") či DaaS. Data mohou být z těchto služeb nahrávána periodicky v dávkách, nebo v datových proudech. Poté jsou data agregována

a filtrována, když procházejí skrze další služby v souladu s technologiemi *fog computing* či *edge computing*, aby nakonec byla zpracována technologií *big data* vhodnými analytickými nástroji a systémy. Například, další službou v technologii „cloud“ pracující jako model služby *big data*-jako-služba (anglicky „Big Data (Analytics) as a Service“, viz sekci 1.2.3). Toto vše umožňuje plynulejší výpočet různých metrik (např. postup operací, nebo stav jednotlivých strojů) a také KPI vyšší úrovně.

2.2.3 Hrozby

T1 – Závislost a odevzdání se prodejci: V současnosti chybí konceptu technologie *cloud computing* standardizace. Existuje mnoho proprietárních a otevřených (včetně zdrojových kódů) řešení a ačkoliv mnoho z nich staví architekturu technologie *cloud computing* na otevřených standardech (např. *Web services*, tedy webové služby), tak výsledné systémy nejsou kompatibilní natolik, aby bylo možné migrovat z jednoho na druhý. S takovým odevzdáním se prodejci (*vendor lock-in*) jsou na místě obavy, že data, nebo funkcionalita v technologii „cloud“, mohou být poškozena/ztracena nebo uniknout. Například to může nastat tehdy, pokud poskytovatel technologie „cloud“ zbankrotuje, nebo se odpojí od sítě z důvodu útoků nebo závažné chyby při údržbě[31]. Také zakladatel GNU pan Richard Stallman varuje, že technologie *cloud computing* je „past“ [63]. Podle [8] je technologie *cloud computing* poskytovaná jedinou společností vlastně úzké místo a to i když má taková společnost více datových center na různých místech dostatečně vzdálených, která jsou navíc připojena do sítě různými poskytovateli, tak může mít společnou SW infrastrukturu a systém účtů. Taková společnost může ale klidně přestat provádět obchodní činnost, proto věříme, že jediné možné řešení je využití více poskytovatelů technologie *cloud computing* současně.

T2 – Strach z nových věcí: Mnoho IT oddělení větších korporací vidí v technologii *cloud computing* hrozbu pro jejich IT kulturu. Zejména spatřují hrozby v oblastech datové bezpečnosti, politiky IT auditů, nebo jen prostě z obav o ztrátu zaměstnání [74]. Proto mohou odmítat novou technologii *cloud computing*, která vyžaduje změny v dobře zaběhané struktuře a procesech.

T3 – Závislost na datech, důvěrnost dat a sdílená pověst: Dalším důsledkem nedostatečné standardizace v technologii*cloud computing* může být závislost na datech. Zákazníci konkrétní technologie „cloud“ nemohou jednoduše extrahovat data a programy z jednoho místa a spouštět je na jiném. Tato skutečnost pak brání některým organizacím v přechodu na technologii *cloud computing* [8]. Kromě toho, nastávají problémy s tím, kdo vlastně taková data vlastní. Data nahraná uživatelem do úložiště v technologii „cloud“ (např. model StaaS) patří uživateli, avšak, fyzicky jsou umístěna v IT infrastruktuře poskytovatele této služby. Poskytovatel může někdy (prakticky kdykoliv) přistupovat k takovým datům a užívat je pro své účely (např. marketing, reklama, zejména tehdy, pokud se jedná o bezplatné poskytování služeb, např. fy Google). Na druhou stranu poskytovatel nemusí být schopen zabránit únikům takových dat (např. neautorizovaný přístup v případě útoku), nebo naopak musí uchovávat data nějakou dobu i po smazání na základě určitých právních norem (např. poskytnout přístup zákonným složkám na základě konkrétního judikátu, jako

[31] Například služba technologie „cloud“ GitLab poskytuje úložiště pro správce verzí a sledování změn v týmové spolupráci vývoje SW pod názvem Git. V minulosti tito vývojáři čelili masivnímu výpadku záloh po nechtěném smazání produkčních dat [48], které vyústilo ve ztrátu dat i přes to, že byla použita standardní plně otevřená (včetně zdrojových kódů) a distribuovaná technologie Git.

např. v případě USA PATRIOT[32]). Proto může být pro nějaké organizace nepřijatelné, aby ukládaly svá data do technologie „cloud“ (nebo je, ta data, nechaly téci skrze nějaké služby v této technologii, což je samo o sobě ještě více omezující). Navíc je zde i problém se sdílenou pověstí, kde špatné chování nějakého zákazníka může postihnout ostatní, kteří používají stejnou IT infrastrukturu technologie „cloud“, jak je uvedeno v [8]. To pak může vyústit v zamezení přístupu z určitých IP adres, nebo ve ztrátu dat, nebo v únik dat, například díky (policejnímu) vyšetřovaní incidentu.

T4 – Nepřenositelná odpovědnost: Služby technologie *cloud computing* jsou obvykle poskytovány jako outsourcing. Nicméně může být náročné implementovat tyto služby jako vlastní ve veřejné, nebo hybridní technologii „cloud“. Zejména pro model služeb SaaS, kde všechny podpůrné úrovně (platforma a infrastruktura) jsou schovány ve službě samotné a není možné je řídit, nebo extrahovat, či provozovat uživateli. V jistých případech může být kritické, aby společnost provozovala své služby jako vlastní například z bezpečnostních či zákonných důvodů, nebo jen proto, aby zabránila možnému úniku svého dobře chráněného know-how. V takových případech, z pohledu zákazníka, je jediným vhodným modelem služeb typ IaaS, kde však dochází k masivnímu nasazení šifrování na všech úrovních technologie „cloud“ (virtualizace, úložiště, síťová komunikace).

T5 – Úzká místa datového přenosu: Velkou výhodou technologie *cloud computing* je lepší škálovatelnost. Není problém škálovat nahoru (rozšiřovat počet aktivních prvků) nebo dolů (zužovat počet aktivních prvků) na základě požadavků, aby byla správně podpořena aktuální či očekávaná zátěž. Jak bylo naznačeno, tak škálovatelnost v technologii *cloud computing* představuje schopnost škálovat nahoru či dolů zdroje či služby v technologii „cloud“. Ale nikoliv škálování propojovacích linek mezi těmito službami a zákazníky. Jak je navrhováno ve [8], uživatelé služeb a poskytovatelé technologie „cloud“ musejí vzít do úvahy umístění a datový provoz na každé úrovni systému, pokud chtějí minimalizovat náklady (cena za datový provoz může být vyšší, než samotné umístění dat).

T6 – Nestabilita výkonu ve víceuživatelských prostředích: Ve víceuživatelském virtuálním prostředí se používá sdílený zásobník běžně používaných zdrojů, aby pokrýval požadavky všech uživatelů bez toho, aby ovlivňovali jeden druhého. Jedna instance každého zdroje (např. fyzického HW) slouží více skupinám uživatelů pro spouštění konkrétních služeb (např. spouštění operačního systému na virtualizovaném HW poskytovaném jako model služby IaaS). Uživatelé/zákazníci mají ve svých smlouvách (SLA) garantovány určité služby, např. kapacita úložiště nebo doba odezvy. Nicméně, opravdová úroveň těchto služeb je obvykle po většinu času vyšší, než nasmlouvaná, ale často je proměnlivá, kdy se mění z minimální smluvně dané po maximální možnou. To se děje na základě celkové zátěže služeb všemi uživateli (zatížení služby). Z pohledu jednotlivých uživatelů/zákazníků je těžké odhadnout aktuální úroveň vytížení služby a zejména variace toho vytížení, což může mít nepředpokladatelné důsledky (např. rychlosti V/V a CPU poskytovaných infrastrukturou jako model služby IaaS významně ovlivňují dobu odezvy na nich běžících aplikací).

[32] `https://www.justice.gov/archive/ll/highlights.htm`

2.3 Bezpečnost v technologii cloud computing

2.3.1 Bezpečnost technologie cloud computing

V rámci technologie *cloud computing* jsou veřejná i privátní data a operace organizace přesunuta do infrastruktury technologie „cloud“. Ta je buďto využita přímo, jako IaaS, nebo jako platforma PaaS, nebo jako poskytovaná SW služba modelu služeb SaaS. Ve všech těchto případech má organizace slabší a jen nepřímou kontrolu nad svými daty a operacemi. Tento fakt významně ovlivňuje IT bezpečnost v organizaci, která musí implementovat bezpečností strategii, rámce, metody, politiky, audity apod. pro technologii „cloud“. Jedině tak může ochránit různé informace o svých zákaznících, dodavatelích a jiných obchodních partnerech, smlouvách, účetnictví, obchodní strategie a know-how.

Pokud jsou data a operace uloženy a prováděny v privátní technologii „cloud“, tak je mnohem snazší řešit bezpečnostní otázky. V takovém případě je infrastruktura technologie „cloud“ obvykle umístěna uvnitř organizace a spravována jejími zaměstnanci (pracuje v perimetru na vnitřních zdrojích podle kategorizace z kap. 1.1.4). Avšak většina organizací, které nemohou mít, nebo nechtějí mít svoji privátní technologii „cloud“, obecně provádějí operace a ukládají data do veřejných technologií „cloud“ poskytovaných určitým dodavatelem (nebo dodavateli). V takových případech je riziko bezpečnostních průlomů docela vysoké a důvěrná data mohou uniknout, což může způsobit velký propad zisku organizace, nebo dokonce odstartovat soudní spory mezi organizací a jejími zákazníky nebo obchodními partnery.

V roce 2008 popsala organizace Gartner [56, 21] sedm IT rizik technologie *cloud computing*. Soustředili se na oblasti jako datová segregace, soukromí dat, privilegovaný uživatelský přístup, životaschopnost poskytovatele, dostupnost a obnova ze záloh. Tyto oblasti by měly být posuzovány podobně jako jiné externí služby na základě nezávislosti umístěni a možnosti, kdy poskytovatel najímá na služby subkontraktora. Podle organizace Gartner je z pohledu bezpečnosti a rizik technologie *cloud computing* tou nejméně transparentní technologií. Je nejméně transparentní v dodávce externích služeb, ukládání a zpracování zákaznických dat externě, na více neznámých místech, často poskytovaných dalšími, často bezejmennými poskytovateli, přitom obsahující data od několika zákazníků, kde schopnost posoudit riziko použití konkrétní nabízené služby klesá až na úroveň transparence [56]. Některá ze sedmi IT rizik definovaných organizací Gartner se nevztahují na bezpečnost IT a již byla rozebrána v sekci 2.2.3. Patří mezi ně dlouhodobá *životaschopnost* služby ve spojení, cituji, s „Co se stane s vaší službou, když poskytovatel zkrachuje, nebo ho někdo koupí?“ [56]. Dále tam patří dostupnost služby, kam patří, cituji, „Organizace by měly definovat požadavky na úrovni služeb pro všechny netriviální IT smlouvy jak pracovní tak vyžadující služby od poskytovatele (interní IT, tradiční poskytovatel mimo vlastní zdroje, poskytovatel technologie *cloud computing*) a zajistit, že smlouva obsahuje penále, pokud smluvní požadavky na služby nejsou naplněny.“ [56]. Posledním klíčovým zmiňovaným rizikem je *umístění dat*, cituji, „které by měl brát do úvahy kdokoliv, kdo potřebuje dostát regulacím soukromí na národní úrovni“ [56]. Další rizika IT bezpečnosti jsou popsána ve [56, 21] takto:

- *Privilegovaný uživatelský přístup* by měl být zaveden proto, že technologie *cloud computing* pracující na vnějších zdrojích (*outsourced*) a mimo perimetr obvykle překlenuje všechny fyzické, logické a personální kontroly a nařízení organizace, na rozdíl od řízení přístupu zavedeného organizací do svých interních aplikací.

- *Shoda* v chování poskytovatelů služeb s externími auditory a bezpečnostními certifikacemi. Zákazníci by měli vyžadovat, aby poskytovatelé vykazovali shodu v chování

a poskytovatelé by měli dodávat informace o specifických kontrolách, které byly provedeny.

- *Datová segregace* za pomoci šifrování by měla být vynucena a s tím spojené správné užívání šifrovacích algoritmů a vlastnictví (de)šifrovacích klíčů by mělo být prověřováno audity, aby nedošlo k neautorizovanému přístupu k datům.

- *Podpora vyšetřování* by měla být umožněna všem zákazníkům technologie „cloud“, aby bylo možné vyšetřit nedovolené, nebo dokonce nelegální aktivity, případně elektronické objevování informací. Podle [56] jsou služby v technologii „cloud“ obzvláště nevhodné pro vyšetřování, protože záznamy aktivit a data více uživatelů mohou být umístěny na stejném místě, ale také mohou být rozložena přes neustále se měnící sadu hostitelských stanic a datových center.

- *Podpora snižování rizik* za účelem umožnit zákazníkům pochopit, jak bezpečně a spolehlivě používat jejich produkty, například, nastavení příslušných politik a jejich monitorování přes audity.

2.3.2 Průvodce bezpečností od CSA

Bezpečnost technologie „cloud“ z pohledu správy, managementu a implementace je popsána v [57, 26]. Ve zdroji [26] popsala Cloud Security Alliance (CSA)[33] čtrnáct domén bezpečnostní analýzy technologie „cloud“, která byla zaměřena na architekturu technologie „cloud“ (doména architektonického rámce technologie *cloud computing*), správu v prostředí technologie „cloud“ (pět domén: management rizik podniku a správy; právní otázky, jako smlouvy a elektronické objevování informací; management auditů a správného chování; management informací a bezpečnost dat; schopnost vzájemné spolupráce a přenositelnost) a práce v prostředí technologie „cloud“ (osm domén: tradiční bezpečnost, obchodní kontinuita a obnova po katastrofách; operace datového centra; reakce na incidenty; bezpečnost aplikací; šifrování a správa klíčů; správa identity, oprávnění a přístupu; virtualizace; bezpečnost jako služba). Poskytnout shrnutí a doporučení ke všem těmto doménám je mimo rozsah tohoto dokumentu, proto se zaměříme jen na určité části, které jsou relevantní pro aplikaci technologie „cloud“ ve výrobním průmyslu.

Hodnocení rizik

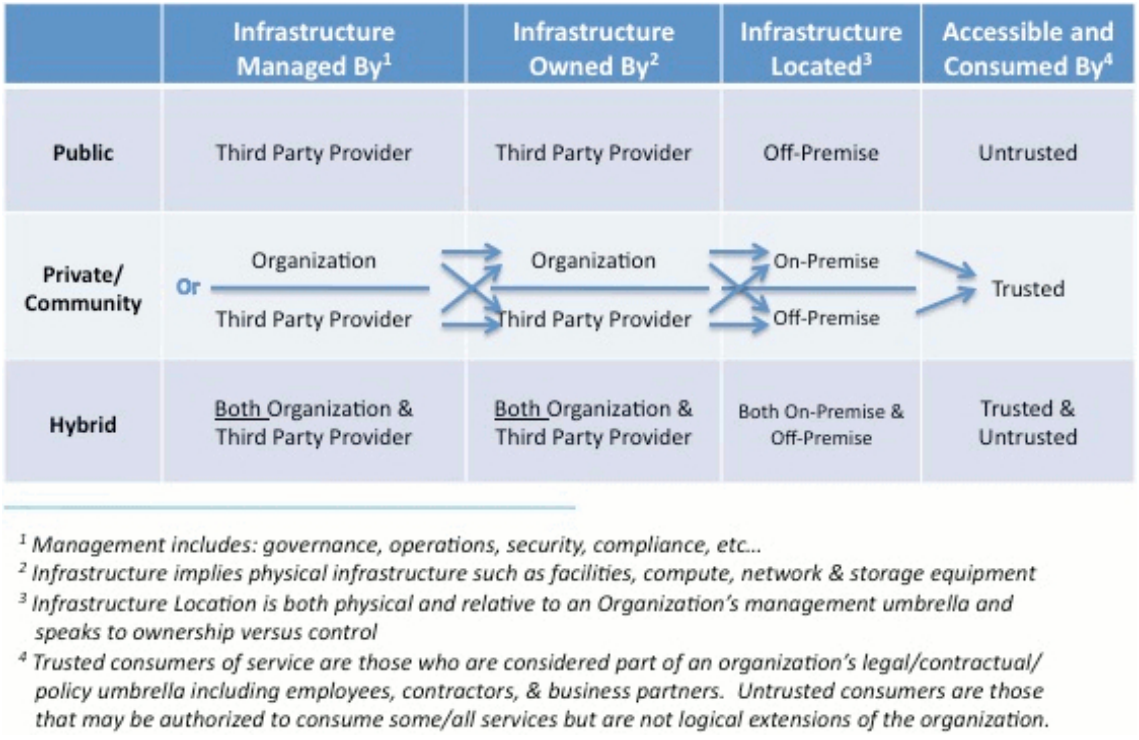
Aliance CSA ve [26] navrhla rychlou metodu pro vyhodnocení schopnosti organizace přenést svá aktiva na různé modely služeb technologie *cloud computing*. Tyto metody zahrnují následující kroky [26]:

1. *Identifikace aktiv pro nasazení v technologii „cloud“*: těmi mohou být buďto informace (data) nebo transakce/zpracování (aplikace/funkce/procesy), přitom se jedná o části funkcí až po celé aplikace. Pro každou organizaci je nutné přesně určit, která data či funkce jsou určeny pro technologii „cloud“.

2. *Vyhodnocení aktiva*: určení, jaká jsou důležitá data či funkce pro konkrétní organizaci. Je třeba si pro každá data či funkci položit otázku: Jak by byla organizace poškozena, kdyby byla porušena bezpečnost?

3. *Zobrazení aktiv do potenciálních modelů nasazení technologie „cloud“*: určení, jestli je organizace ochotná přijmout některé modely nasazení: veřejný; privátní, interní/ve

[33] `https://cloudsecurityalliance.org/`



Obrázek 2.3: Modely nasazení technologie *cloud computing* a možnosti managementu, vlastnictví, umístění a přístupu (převzato z [26]).

vlastních prostorách; privátní, externí a to i v případě dedikované nebo sdílené infrastruktury; komunitní při vzetí do úvahy umístění, potenciálního poskytovatele služeb a identifikaci dalších členů komunity; hybridní s architektonickou vizí, kde budou umístěny komponenty, funkce a data.

4. *Vyhodnocení potenciálních modelů služeb technologie „cloud" a poskytovatelů*: vyhodnocení se musí odehrát se zaměřením na stupeň řízení, kde organizace musí implementovat zmírnění rizik v různých vrstvách software/platformy/infrastruktury.

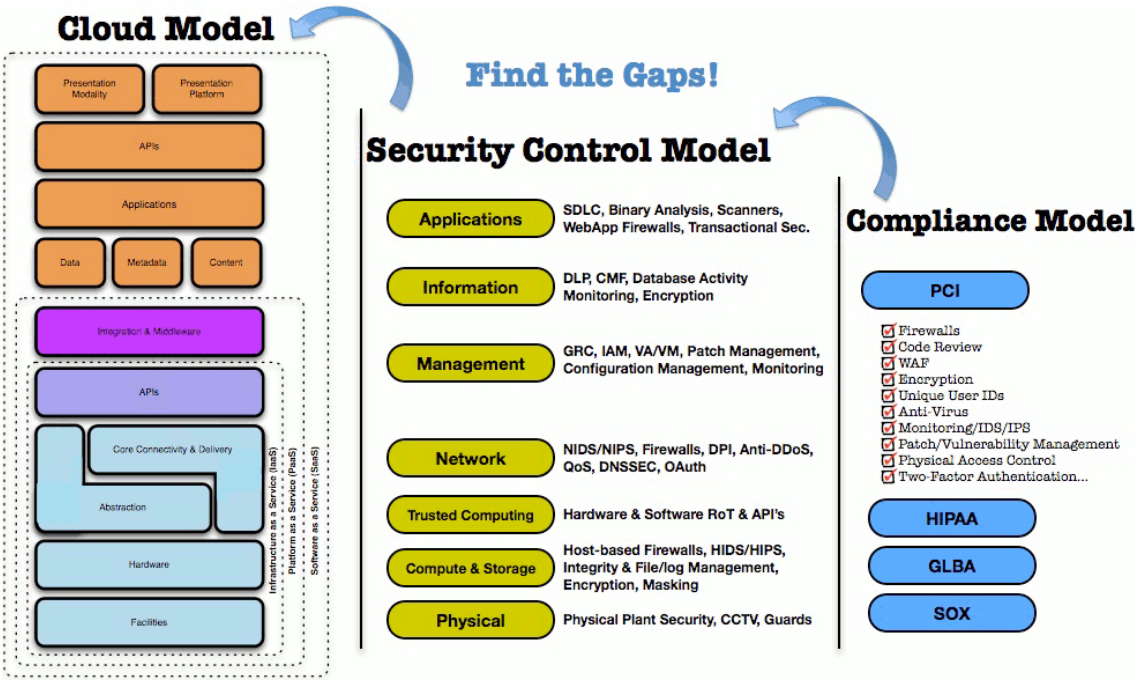
5. *Nastínění potenciálních datových toků* mezi organizací, službou technologie „cloud" a jakýmkoliv zákazníkem/jinými uzly. Cílem je pochopit jestli a jak je možné data přesouvat do a z technologie „cloud".

Rozdíly v možnosti managementu, vlastnictví, umístění a přístupu k modelům nasazení technologie „cloud" jsou popsány na obrázku 2.3.

Model bezpečnostního řízení a dodržování bezpečnosti

Jelikož jsou služby technologie *cloud computing* poskytovány a organizovány hierarchicky, na každé úrovni je individuální model služeb IaaS/PaaS/SaaS (viz sekci 1.1.2), různá řídicí a kontrolní měření a procedury kontroly dodržování správného (shoda) chování, tak mohou být přiřazeny individuálně těmto úrovním, jak ukazuje obrázek 2.4. Zatímco model pro řízení a kontrolu bezpečnosti se v dané organizaci aplikuje zejména technicky a organizačně, model kontroly shody v chování je často podchycen právními dokumenty, certifikacemi, nebo bezpečnostními standardy. Například, model shodného chování může být dán celosvětově prostřednictvím pravidel PCI[34] pro elektronické obchodování, nebo pro-

[34] `https://www.pcisecuritystandards.org/`



Obrázek 2.4: Zobrazení modelu technologie „cloud“ na bezpečnostní řízení a kontrolu dodržování shodného chování (převzato z [26]).

střednictvím pravidel pro soukromí a bezpečnost HIPAA[35], nebo prostřednictvím pravidel Sarbanes-Oxley Act (SOX)[36] na zamezení podvodům a zvýšení korporátní zodpovědnosti, zejména v USA.

Management informací a bezpečnost dat

Aliance CSA ve [26] doporučuje na implementaci bezpečnosti v technologii „cloud“ využít „Životní cyklus bezpečnosti dat“ od Securosis[37]. Tento dokument definuje šest fází od vytvoření dat po jejich destrukci. V průběhu těchto fází data prochází prostředím technologie „cloud“ a jsou manipulována: čtena, zpracovávána, ukládána. Je nutné identifikovat a řídit tyto operace v jednotlivých fázích životního cyklu bezpečnosti dat. To zahrnuje aktéry takových operací (kdo může udělat jakou operaci a má povolení ji udělat) a umístění (kde se může operace odehrát a kde je to povoleno). Operace, které je možné provádět, ale není povolené provádět, musejí být pro příslušné případy vymezeny bezpečnostní politikou.

Podle [26] od CSA je možné zajistit soukromí dat na hranici i uvnitř technologie „cloud“ prostřednictvím šifrování klienta/aplikace či dokumentu, šifrováním síťového přenosu (např. SSL nebo VPN), a šifrováním na úrovni proxy (proxy-aplikace či proxy-server, kteří šifrují data před odesláním dále do sítě). Takový způsob šifrování je možné aplikovat ve všech modelech služeb (IaaS/PaaS/SaaS) pomocí různých technických prostředků, jak je popsáno ve [26]. Krom toho existují i další doporučení, kde se bere do úvahy prevence ztráty dat (anglicky „data loss prevention“) (DLP), sledování aktivit nad databází a soubory (anglicky „database and file activity monitoring“) (DAM/FAM), správa digitálních práv (anglicky „digital rights management“) (DRM) a jiná.

[35] `https://www.hhs.gov/hipaa/`
[36] `http://csrc.nist.gov/groups/SNS/rbac/sarbanes_oxley.html`
[37] `https://www.securosis.com/blog/data-security-lifecycle-2.0`

Attack type	Attack method
Channel attack	Monitor, intercept, and tamper the data packets in public channels.
	Data replay attack, repeatedly sending the data which has been sent before.
	Message insert attack, destroy the reading of messages and the internal control data.
Denial of service attack	Node collaboration attack, malicious node prevents messages from broadcasting to certain areas of the WAMS network [16].
	Channel congestion. The attacker consumes the bandwidth of the channel, disables the sending and receiving of other nodes.
	Energy consumption. The attacker repeatedly sends the data request messages, consuming the energy of the target node [17].
Node attack	The attacker controls some nodes, analyzes and modifies them, or obtains confidential information in them [16].
Attack from malicious nodes	Sybil attack. Use the multiply IDs to deceive other nodes, so that the malicious nodes become the routing node more easily. Then attack the target node combining with other attack methods.
	Node copy attack. Steal the ID information from a legal node, then attack other nodes [18].
Protocol attack	Includes: routing protocol attack, selective forwarding attack, wormhole attack, Hello Flood attack, deceiving reply attack, and attack targets on data fusion [19], [20].

Obrázek 2.5: Hlavní bezpečnostní hrozby, které přináší systém pro sledování rozsáhlých oblastí (anglicky „wide-area monitoring system“) (WAMS) (převzato z [93]; viz zdroj pro odkazy na obrázku).

2.3.3 Bezpečnost v technologiích edge computing, fog computing a cloud computing pro výrobu

V případě technologie *edge computing* nebo *fog computing*, což jsou koncepty typicky využívané v CMfg pro propojení a integraci různých zařízení do technologie „cloud“ (výrobní stroje, roboti, brány pro bezdrátové senzory, etc.), je potřeba zvážit další bezpečnostní hledisko. Jelikož CMfg obvykle integruje mnoho malých zařízení poskytujících své služby technologii „cloud“, tato zařízení jsou propojena lokální, často bezdrátovou, sítí. Útoky, které si kladou za cíl technologii „cloud“ pro výrobu, se tak mohou soustředit právě na tuto síťovou infrastrukturu, aby poškodili služby uvnitř.

Zatímco drátová/kabelová síťová infrastruktura může být fyzicky chráněna docela jednoduše, ochrana bezdrátové síťové infrastruktury je mnohem náročnější. Na nižších vrstvách využívají bezdrátové sítě obvykle proprietární komunikační technologie, proprietární rozšíření otevřených protokolů, nebo proprietární firmware a ovladače jinak standardních technologií. To mohou například být různé implementace standardu ZigBee/IEEE 802.15.4[38]. Tyto technologie a protokoly implementují vrstvy nízkých úrovní síťového protokolu (např. IEEE 802.15.4 pracuje s fyzickou a spojovou vrstvou a ZigBee pracuje na síťové a aplikační vrstvě). Nad těmito vrstvami jsou postaveny vysokoúrovňové komunikační sběrnice, které implementují technologii CMfg, jak je popsáno v sekci 2.1.2. Ačkoliv tyto vysokoúrovňové komunikační sběrnice obvykle mají velmi dobré a nastavitelné zabezpečení, takováto zabezpečení nemohou zabránit všem vlivům bezpečnostních průlomů na nižších vrstvách.

Například, obrázek 2.5 popisuje bezpečnostní hrozby z [93] zaznamenané ve WAMS realizovaném jako smart grid, který je velmi podobný konceptu technologie CMfg[39].

Některým útokům lze zabránit na úrovni vysokoúrovňové komunikační sběrnice, například, aplikací silného šifrování a zaobalováním přenášených dat do šifrovaných obálek. Avšak, tento přístup má minimálně dvě slabé stránky: (1) tímto se nezvýší bezpečnost operací, které zůstávají na nižších vrstvách (např. směrování paketů) a (2) šifrování a dešifrování, které musí probíhat na hraničních (edge) uzlech, bude u nízkopříkonových zařízení spotřebovávat příliš mnoho procesorového času, operační paměti a jistě také elektrické energie, což pro bezdrátová zařízení může být kritické. Tyto problémy jsou diskutovány

[38] `http://www.zigbee.org/`

[39] pro porovnání „grid computing“ a *cloud computing* viz [41]

v [93] pro nízké vrstvy síťových protokolů a v [94] pro vyšší vrstvy. Druhá zmiňovaná publikace také popisuje typy potenciálních útoků proti WAMS uvnitř technologie smart grid takto [94]:

- *Ztráta důvěrnosti* díky (i) odposlechu a analýze bezdrátového přenosu; (ii) zachytávání a replikaci uzlů.
- *Ztráta autentičnosti* díky (i) modifikací zpráv a vkládání; odpovídáním na zprávy; (ii) zachytávání a replikaci uzlů; (iii) aplikaci Sybilina útoku, kdy malý počet útočících uzlů padělá velké množství identifikací, aby podvrhlo a porušilo směrování zpráv.
- *Ztráta integrity* díky modifikaci zpráv.
- *Ztráta dostupnosti* díky (i) blokování zpráv pomocí spolupráce útočících uzlů, zarušení bezdrátových kanálů; (ii) podvržení datových požadavků na senzory, které způsobí zbytečné čerpání energie.

Před tím, než budou díky výzkumné komunitě vyřešeny všechny bezpečnostní hrozby na všech úrovních komunikace v technologii CMfg a než budou přijaty prodejci, je silně doporučeno zůstat u konzervativních metod síťového provozu v technologii „cloud“. Tedy preferovat drátové/kabelové sítě před bezdrátovými a udržovat kritická data a operace na vysoce zabezpečených privátních technologiích „cloud“. A to tedy rozhodně raději, než pracovat na hybridních či veřejně poskytovaných službách technologie „cloud“. V opačném případě totiž úspěšné útoky na zařízení připojená do technologie „cloud“ pro výrobu mohou způsobit ne jen ztrátu dat, nebo prolomení dat, ale také atakovat přímo zařízení, jako jsou výrobní stroje a roboti. Útok může tyto stroje/roboty navést tak, že budou pracovat (sebe)destruktivně a tak způsobit velké škody na majetku.

3 Přehled a srovnávací analýza existujících cloud computing systémů

V předchozí kapitole byly prezentovány teoretické základy technologie *cloud computing* včetně praktických aspektů důležitých pro výrobní průmysl. Popsali jsme několik modelů služeb a způsobů jejich nasazení, jejich kategorizace, architektur, trendů a dalších. V uvedeném popisu bylo zmíněno několik *cloud computing* řešení, a to proprietárních poskytovaných různými komerčními společnostmi i otevřených vyvíjených komunitou. V této kapitole bude přehled dostupných *cloud computing* řešení pro výrobní průmysl, jejich kategorizace a srovnání podle účelu a dalších kritérií. Vybrané *cloud computing* služby obzvláště vhodné pro technologii cloud manufacturing (CMfg) budou analyzovány podrobněji a bude vyhodnoceno, jak naplňují principy technologie CMfg a řeší možné příležitosti a rizika.

Porovnávací kritéria (anglicky „comparison criteria, CC“) (PK) budou definována a použita při komparativní analýze popsané výše. Cílem těchto kritérií není popsat nejlepší charakteristické rysy daných *cloud computing* řešení, ale stanovit společné oblasti pro nezbytné objektivní porovnání, přestože charakteristické rysy mohou mít svůj význam pro konkrétní uživatele a oblasti nasazení. Vycházíme z toho, že porovnání a vyhodnocení *cloud computing* řešení by mělo být vždy provedeno v kontextu jejich společných způsobů použití, nebo podle velmi přesně definovaných potřeb aplikací konkrétního cílového uživatele, pokud je toto možné. Zmiňovaná PK jsou následující:

PK1 *Charakteristický model služeb* (IaaS/PaaS/SaaS) – Poskytovatelé služeb *cloud computing* často nabízejí společně různé služby na různých úrovních a modelech, konkrétně infrastruktura-jako-služba (anglicky „Infrastructure as a Service“) (IaaS), platforma-jako-služba (anglicky „Platform as a Service“) (PaaS) a software-jako-služba (anglicky „Software as a Service“) (SaaS). Přesto, pouze jeden z těchto modelů je obvykle charakteristický pro hlavní služby, tedy takové služby, které významně pomáhají obchodním nebo výrobním procesům organizace zákazníka. Ostatní služby s odlišnými modely pak hrají většinou pouze roli pomocných služeb pro služby hlavní, nebo jsou určené pro speciální případy užití, např. jako robot-jako-služba (anglicky „Robot as a Service“) (RaaS). Během srovnávací analýzy bude pro každé řešení vždy určen pouze jeden model, a to ten, který je charakteristický pro hlavní služby.

PK2 *Architektura technologie „cloud“* (statická/edge/fog) – Infrastruktura pro technologii *cloud computing* a příslušné služby jsou organizovány do vrstev od nejnižší pro IaaS po nejvyšší pro SaaS. V zavedených *cloud computing* řešeních se statickou architekturou je klasická infrastruktura distribuována a virtualizována především tak, aby vždy poskytla uživatelům stejné služby, nezávisle na jejich geografické lokaci. V případě technologií *edge/fog computing* je architektura především složena z různorodých jednoduchých zařízení, jako je programovatelný logický automat (anglicky „programmable logic controller“) (PLC) nebo virtuální řídící jednotka robota (anglicky „virtual robot controller“) (VRC), a až poté z rozsáhlých distribuovaných platforem použitých u statických architektur, které společně implementují služby

různých modelů, jako je data-jako-služba (anglicky „Data as a Service“) (DaaS), výroba-jako-služba (anglicky „Manufacturing as a Service“) (MaaS) aj. Je proto užitečné rozlišovat mezi takovými různými architekturami. Navíc, za účelem srovnání, budeme rozlišovat mezi technologiemi „edge“ a *fog computing*. V prvním případě „edge“ zařízení pouze zasílají data službám technologie *cloud computing* (např. samotná služba modelu DaaS) nebo umožňují řízení připojených strojů pro chytrou výrobu, viz kap. 2.1.1. V druhém případě, technologie *fog computing*, stejná „edge“ zařízení poskytují služby ostatním a zároveň využívají jiné služby v technologii *cloud computing* pro svou potřebu (viz CMfg v kap. 2.1.2).

PK3 *Cloud Cube Model (CCM) klasifikace* (I/E, P/O, Per/D-p, In/Out) – Pro analýzu aspektů nasazení u jednotlivých *cloud computing* řešení použijeme CCM od Fóra Jericho (viz kap. 1.1.4). Pomocí tohoto modelu bude u každého *cloud computing* řešení přiřazena jedna od každé z následujících charakteristik: interní/externí (I/E) dle fyzického umístění dat v technologii „cloud“; proprietární/otevřené (P/O) dle způsobu vlastnictví infrastruktury a služeb; v perimetru nebo mimo, což je anglicky „perimeterised/de-perimeterised“ (Per/D-p), podle toho, odkud jsou řízena data a funkce v technologii „cloud“ (např. pro kontrolu oprávnění přístupu), jestli uvnitř infrastruktury organizace zákazníka nebo vně; a insourcing/outsourcing (In/Out) dle způsobu řešení realizace technologie *cloud computing*, buď vlastními nebo cizími zaměstnanci organizace zákazníka.

PK4 *Analýza dat* (žádná/předdefinovaná/libovolná/big data) – Služby *cloud computing* spravují a generují množství dat, která představují hodnoty metrik obchodních nebo výrobních procesů, data senzorů z monitoringu, data přístupná způsobem DaaS, data uložená v „cloud“ službách úložišť a další. Také pro CMfg je typické velké množství za běhu generovaných dat. Analýza takových dat je složitá úloha, která by měla být podporována v rámci *cloud computing* řešení. Služba technologie *cloud computing* proto může poskytovat předdefinované analýzy dat pro zavedený klíčový ukazatel výkonnosti (anglicky „key performance indicator“) (KPI) nebo může být umožněno zákazníkům naprogramovat si jejich vlastní libovolné analýzy. Navíc, často je potřeba také zpracování a analýza pomocí technologie big data tak, jak bylo popsáno v kap. 1.2.3.

PK5 *Bezpečnost* (řízení přístupu, šifrování atd.) – Bezpečnost v technologii *cloud computing* je důležitá a měla by být vynucena jak poskytovateli služeb, tak jejich zákazníky (viz kap. 2.3). Obvykle je bezpečnost řešena striktním řízením přístupu se záznamem spotřeby služeb a šifrováním úložiště a komunikace. Existuje mnoho možností jak implementovat tyto bezpečnostní prvky. Navíc, existují také další bezpečnostní řešení, jako je správa identit, služby jednotného přihlášení (anglicky „single sign-on services“) nebo distribuované sítě důvěry. Důsledkem různorodosti pak je obtížné porovnání *cloud computing* řešení na základě bezpečnosti.

PK6 *Příležitosti* a *hrozby* (viz seznam v kap. 2.2) – V předchozích částech této zprávy bylo identifikováno několik příležitostí a hrozeb pro technologii *cloud computing* (a pro CMfg). Zatímco mnoho z nich je úspěšně řešeno v rámci porovnávaných *cloud computing* řešení, další neřešené představují příležitosti zisku nebo rizika ztrát, která je potřeba při porovnání zvážit.

3.1 Služby cloud computing pro výrobní průmysl

Na základě analýzy současného stavu vypracované v předchozích kapitolách (zejména v kap. 2.1) se jeví nejvíce slibné pro výrobní průmysl automobilů/elektroniky uplatnění technologie *cloud computing* pro chytrou výrobu (pro sledování, řízení a optimalizace obchodních, řídicích a podpůrných procesů) a CMfg (pro sledování, řízení a optimalizace výrobních procesů a využitá prostředků pro výrobu; viz kapitoly 2.1.1 a 2.1.2). Řešení pro *cloud computing* pro výrobní průmysl, která jsou dostupná v současné době na trhu, se zaměřují zejména na chytrou výrobu, ne na CMfg, a využívají koncept internet věcí (anglicky „Internet of Things“) (IoT). Přesto, jejich konkrétní nasazení v konkrétních výrobních organizacích s pečlivým uplatněním principů CMfg může posunout zmiňovaná běžně dostupná řešení směrem k CMfg.

Tato kapitola poskytuje stručný přehled několika aktuálně dostupných technologií *cloud computing*, které mohou být vhodné pro výrobní průmysl, jak je popsáno v odstavci výše[1]. Další tři nejvíce slibná řešení jsou detailněji popsána v kap. 3.2. Celkový přehled výsledků porovnání je v tab. 3.1.

3.1.1 AWS IoT

Amazon Web Services (AWS) IoT je platforma pro *cloud computing*, která umožňuje připojeným zařízením jednoduše a bezpečně interagovat s aplikacemi technologie *cloud computing* a jinými zařízeními. Platforma AWS IoT umí takto podpořit bilióny zařízení a triliony zpráv, které umí zpracovat a spolehlivě a bezpečně směrovat do koncových bodů AWS a k jiným zařízením. Platforma AWS IoT zjednodušuje použití samotných služeb AWS, jako jsou AWS Lambda, Amazon Kinesis[2], Amazon S3[3], Amazon DynamoDB[4] a další k tvorbě aplikací dle konceptu IoT bez potřeby vlastní infrastruktury. Takové aplikace sbírají, zpracovávají, analyzují data generovaná připojenými zařízeními a jednají na jejich základě. [6]

Podle [7], platforma AWS IoT poskytuje bezpečnou obousměrnou komunikaci mezi zařízeními konceptu IoT (jako jsou senzory, regulátory, zabudovaná či chytrá zařízení) a AWS, který ze zařízení sbírá data a tato ukládá a analyzuje. Systémy AWS IoT mohou být sestaveny z několika komponent: brána zařízení (umožní zařízením bezpečnou a rychlou komunikaci), zprostředkovatel zpráv (aplikace pomocí něj mezi sebou publikují a odebírají zprávy přes Message Queue Telemetry Transport (MQTT) protokol), vykonavatel pravidel (pro tvorbu pravidel zpracovávajících a integrujících zprávy), služba pro bezpečnost a identity (pro sdílenou zodpovědnost za bezpečnost), registr zařízení (organizuje zdroje přiřazené jednotlivých zařízením, např. certifikáty či klientské identifikátory pro MQTT), stín zařízení (pro uchování a obnovu aktuálního stavu jednotlivých zařízení) a služba stínu zařízení (pro perzistentní reprezentaci zařízení v technologii „cloud“).

Technologie AWS IoT s pomocí ostatních služeb AWS je služba PaaS v technologii *edge computing*, která může být nasazena jako externí, proprietární, vně perimetru a provozována jako insourcing podle CCM od Fóra Jericho (viz kap. 1.1.4). Řešení umožňuje implementovat vlastní analýzu dat či použít big data analýzy poskytované příslušnými AWS službami. Z hlediska bezpečnosti nabízí řešení šifrovanou komunikaci, autentizaci a řízení přístupu se správou identit (pomocí služby pro bezpečnost a identity). Jedná se o vhodné řešení pro příležitosti O1, O3, O5, O7 a O9 a rizika T3 a T6 podle kap. 2.2. Avšak rizika

[1] Technické porovnání některých z technologií diskutovaných v této kapitole lze nalézt v [31].
[2] `https://aws.amazon.com/kinesis/`
[3] `https://aws.amazon.com/s3/`
[4] `https://aws.amazon.com/dynamodb/`

Název sužby	PK1 Model	PK2 Arch.	PK3 CCM	PK4 Analýza	PK5 Bezpečnost	PK6 Přílež.	PK6 Hrozby
AWS IoT (Sec 3.1.1)	PaaS	edge	E, P, D-p, In	libovolná / big data	šifrovaná kom., auten., řízení přist., správa identit	$O1+$, $O3+$, $O5+$, $O7+$, $O9+$	$T3+$, $T6+$; $T1-$, $T4-$, $T5-$
IBM BlueMix, Watson IoT (Sec 3.1.2)	PaaS	edge	E, O/P, Per/D-p, In	libovolná / big data	šifrovaná kom., auten., řízení přist., správa identit	$O1+$, $O2+$, $O3+$, $O4+$, $O5+$, $O6+$, $O7+$, $O9+$	$T1+$, $T3+$, $T4+$, $T5+$; $T6-$
Microsoft Azure IoT (Sec 3.1.3)	PaaS	edge	E, O/P, D-p, In	libovolná	šifrovaná kom.	$O3+$, $O5+$, $O8+$, $O9+$; $O1-$, $O2-$, $O7-$	$T5+$, $T6+$; $T1-$, $T3-$, $T4-$
Google Cloud IoT (Sec 3.1.4)	PaaS	edge	E, P, De-p, In/Out	big data	šifrovaná kom.	$O1+$, $O3+$, $O8+$, $O9+$; $O7$; $O2-$, $O4-$	$T3+$, $T6+$; $T1-$, $T4-$, $T5-$
SAP Cloud Platform for IoT (Sec 3.1.5)	PaaS	edge	E, P, De-p, In	libovolná / big data	šifrovaná kom., auten.	$O4+$, $O5+$, $O8+$, $O9+$; $O1-$, $O3-$	$T3+$; $T1-$, $T4-$, $T5-$, $T6-$
Mnubo (Sec 3.1.6)	SaaS	není	E, P, De-p, Out	libovolná	šifrovaná kom., auten.	$O5+$, $O9+$	$T1+$; $T3-$, $T4-$
PTC ThingWorx (Sec 3.2.1)	PaaS	edge	E/I, P, De-p, In/Out	předdef. / libovolná	šifrovaná kom., auten., řízení přist.	$O1+$, $O2+$, $O3+$, $O5+$, $O7+$, $O9+$	$T4+$, $T6+$; $T3$; $T1-$, $T5-$
Siemens MindSphere (Sec 3.2.2)	SaaS (PaaS)	edge	E/I, P, De-p, In	libovolná / big data	šifrovaná kom., šifrované úlož., auten., řízení přist.	$O1+$, $O3+$, $O5+$, $O9+$; $O2-$	$T5+$, $T6+$; $T4$, $T3$; $T1-$
GE Predix (Sec 3.2.3)	PaaS	edge	I, P, De-p, In	libovolná	šifrovaná kom., auten., řízení přist., správa identit	$O1+$, $O2+$, $O3+$, $O5+$, $O9+$; $O7-$, $O8-$	$T1+$, $T3+$, $T4+$, $T6+$; $T5-$

Tabulka 3.1: Porovnání služeb *cloud computing* pro výrobní průmysl. PK jsou popsána v kap. 3. Znaménka plus/mínus (+/−) ve sloupci PK6 značí podporované/zanedbané příležitosti a hrozby (viz kap. 2.2).

T1, T4 a T5 nejsou adekvátně řešena, zejména pro přílišnou závislost na proprietárních technologiích společnosti Amazon.

Technologie AWS IoT není vhodná pro implementaci platformy CMfg, protože postrádá průmyslová aplikační programová rozhraní (anglicky „application programming interfaces“) (APIs) a schopnost interního hybridního či privátního nasazení technologie *cloud computing*. Existuje sice platforma Amazon Virtual Private Cloud, ta je však pro zmiňované nasazení nedostatečná (není to „privatní“ nasazení, ale externí hybridní nasazení uvnitř perimetru, dle kap. 1.1.3).

3.1.2 IBM BlueMix / Watson IoT Platform

IBM BlueMix je technologie *cloud computing* od společnosti IBM, která nabízí velké množství různých služeb[5]. Řešení je založeno na otevřené technologii Cloud Foundry[6]. Podle [59], jsou v platformě Watson IoT zařízení připojena do technologie BlueMix přímo nebo prostřednictvím brány pomocí protokolu zasílání zpráv založeném na otevřeném MQTT nebo proprietárním Hypertext Transfer Protocol (HTTP) Messaging API. Data poskytnutá zařízením jsou zpracována službami technologie *cloud computing*, jejichž funkce a výsledná data jsou pak dostupná přes Representational State Transfer (REST) rozhraní. BlueMix poskytuje služby pro správu zařízení, správu uživatelů a jejich rolí, pro řízení přístupu (uživatelů, rolí, aplikací a služeb), datové analýzy zpracovánané v reálném čase včetně (částečných) analýz prováděných přímo na „edge“ zařízeních (na branách IoT s nainstalovanou aplikací Watson IoT Edge Analytics Agent), pro vizualizaci a další.

Pro výrobní průmysl poskytuje technologie BlueMix několik služeb nebo celé rámce služeb, jak je zmiňovaná platforma IBM Watson IoT Platform[7] či její specializace pro automobilový a elektronický průmysl[8]. Poskytovány jsou také další služby připravené k okamžitému použití v různých průmyslových aplikacích využívající IoT pro chytrou výrobu pomoci technologie *cloud computing* nebo CMfg (viz kapitoly 2.1.1 a 2.1.2). Zařízení jsou však zapojena do technologie *cloud computing* především jako datové zdroje, nikoliv klienti využívající ostatní služby tak, jak je tomu např. u technologie *fog computing* popsané v kap. 1.2.1.

Platforma Watson IoT společně s technologií IBM BlueMix může být kategorizována jako řešení typu PaaS pro technologii *edge computing*, které umožňuje externí nasazení s otevřenou technologií IoT a proprietární technologie „cloud“, uvnitř či vně perimetru, provozované jako insourcing tak, jak tyto pojmy definuje CCM od Fóra Jericho (viz kap. 1.1.4). Provoz uvnitř či vně perimetru závisí na zvolené architektuře, kdy technologie *cloud computing* může být provozována výrobcem ve veřejném nasazení nebo samotným zákazníkem v privátním nasazení. V případě privátního nasazení se použijí služby technologie BlueMix Local [58] pro provoz virtuálního stroje, který běží na infrastruktuře informační technologie (IT) zákazníka a který pracuje většinou lokálně a pouze v některých případech komunikuje s veřejným nasazením technologie *cloud computing* výrobce (např. pro operační správu IT a služeb). Takové řešení výrazně zlepšuje bezpečnost.

Služby BlueMix dále umožňují implementovat vlastní datové analýzy či využít big data analytické nástroje, poskytují šifrovanou komunikaci mezi zařízeními IoT a službami technologie *cloud computing* a také autentizaci a řízení přístupu se správou identit. Technologie BlueMix s platformou Watson IoT vhodně řeší příležitosti O1 až O6 (díky otevřenosti

[5] viz `https://console.bluemix.net/catalog/`

[6] `https://www.cloudfoundry.org/`

[7] `https://console.bluemix.net/catalog/services/internet-of-things-platform`

[8] viz `https://console.bluemix.net/catalog/services/iot-for-automotive/` a `https://console.bluemix.net/catalog/services/iot-for-electronics/`

a flexibilní architektuře), O7 (protože podporuje IoT pro automobilový průmysl zmiňované výše) a O9 (díky dobrým službám pro analýzu dat a jejich vizualizaci) v označení dle kap. 2.2. Co se týká hrozeb uvedených v téže kapitole, hrozba T1 je řešena dobře, přestože ne perfektně (většina technologie IBM BlueMix / Watson IoT Platform je open-source), a také řešení hrozeb T3, T4 a T5 je přijatelné (díky flexibilní architektuře). Přesto, některé další nepokryté hrozby, jako je T6, by si zasluhovaly větší pozornost.

3.1.3 Microsoft Azure IoT Suite

V roce 2015 uvedla společnost Microsoft *cloud computing* řešení Azure IoT Suite založené na platformě Azure Cloud[9]. Aplikace vytvořené pomocí platformy Azure IoT Suite mohou využívat služby Azure IoT Hub nebo Azure IoT Edge pro správu zařízení a jejich nasazení, či další služby Azure Machine Learning[10], Stream Analytics[11] a Time Series Insight[12] pro pokročilé datové analýzy.

Podle [17], je služba Azure IoT Hub most pro bezpečnou, spolehlivou, obousměrnou komunikaci mezi zařízeními konceptu IoT a službami technologie *cloud computing* pomocí protokolů MQTT, REST a Advanced Message Queuing Protocol over TLS/SSL (AMQPS). Tento most umožní zařízením vytvořit bezpečné spojení a posílat či přijímat zprávy k nebo od služeb, např. pro jejich uložení, analýzy a zpracování v reálném čase. Technologie Azure IoT Edge[13] umožňuje číst data průmyslových zařízení pomocí standardních průmyslových komunikačních protokolů, jako jsou OPC Unified Architecture (OPC-UA), Modbus a MQTT [14], a předzpracovávat tato data v lokálně umístěných branách s nainstalovaným software (SW) Azure IoT Edge nad operačními systémy Linux nebo Windows. Předzpracování je provedeno na branách předtím, než jsou data odeslána ke službám technologie *cloud computing*, kde mohou být díky předzpracování nahrána pouze nejdůležitější data. Navíc, díky tomuto konceptu, jednotlivá zařízení pracují spolehlivě a bezpečně i při výpadcích spojení ke službám technologie *cloud computing* tak, že po opětovném připojení automaticky synchronizují svůj stav a dále bezchybně fungují společně [47]. V kombinaci se službou Azure Stream Analytics mohou být data při předzpracování nejen odfiltrována, ale také agregována v daných časových intervalech nebo s využitím uživatelsky definované funkce, nebo dokonce přímo zpracována na zařízení bez předání službám technologie *cloud computing* [14].

Podle společnosti Microsoft je Azure IoT Suite řešení typu PaaS pro technologii *edge computing*, které může být nasazeno externě, je otevřené i proprietární (Azure IoT Edge je otevřený, avšak technologie *cloud computing* je proprietární, založená na Microsoft technologiích), vně perimetru a provozovaný jako insourcing podle CCM od Fóra Jericho (viz kap. 1.1.4). Řešení umožňuje implementovat vlastní datové analýzy (pomocí služby Azure Stream Analytics pro technologii *edge computing*) a používá šifrovanou komunikaci. Platforma Azure IoT Suite se nezaměřuje na autentizaci a řízení přístupu či správu identit, přestože tyto lze řešit v rámci platformy Azure Cloud. Vhodně jsou pokryty příležitosti O3, O5, O8 a O9 a hrozby T5 a T6 dle kap. 2.2. Příležitosti O1, O2 a O7 a hrozby T1, T3 a T4 však nejsou řešeny, zejména kvůli silné zavislosti na proprietárních technologiích Microsoft. Na rozdíl od většiny ostatních řešení pro technologii *cloud computing* v této zprávě, technologie Azure IoT Edge částečně řeší riziko T5 díky (před-)zpracování dat na „edge“ zařízeních i bez spojení se službami, jak bylo popsáno výše.

[9] viz `https://www.microsoft.com/en-us/internet-of-things/azure-iot-suite`
[10] `https://azure.microsoft.com/services/machine-learning/`
[11] `https://azure.microsoft.com/services/stream-analytics/`
[12] `https://azure.microsoft.com/services/time-series-insights/`
[13] `https://github.com/azure/iot-edge`

3.1.4 Google Cloud IoT

Google Cloud IoT je skupina integrovaných služeb technologie *cloud computing* pro snadné a bezpečné propojení, správu a získávání dat z globálně rozmístěných zařízení konceptu IoT. Služby umožňují zpracovat a analyzovat/vizualizovat taková data v reálné čase a na jejich základě provést provozní změny a různé potřebné akce. Data ze zařízení jsou zachycena komponentou Cloud IoT Core a publikována pomocí služby Cloud Pub/Sub pro následné analýzy. Jednorázové analýzy mohou být provedeny pomocí platformy Google BigQuery[14], pokročilé analýzy a aplikace strojového učení pomocí technologie Cloud Machine Learning Engine[15]. Vizualizace výsledků datových analýz v dokumentech souhrnných zpráv a živých přehledech lze vytvořit pomocí nástroje Google Data Studio[16]. [51]

Podle [52], technologie Google Cloud IoT spravuje, uchovává a analyzuje metadata zařízení (jako je identifikátor, model, nebo sériové číslo hardware (HW)), stavové informace, telemetrická data (data ze senzorů odesílaná ke službám technologie *cloud computing*) a provozní informace (jako je teplota, kterou vykazuje centrální procesorová jednotka (anglicky „central processing unit“) (CPU), nebo stav napájecí baterie). Zařízení mohou být připojena na služby technologie *cloud computing* přímo[17] nebo pomocí HW rozhraní bran pro senzory. Zařízení může zpracovat senzorová data před jejich odesláním ke službám technologie *cloud computing*, např. data konvertovat, zabalit, validovat, setřídit, rozšířit, shrnout či zkombinovat data z více senzorů či více časových intervalů. Poté jsou tato data odeslána ke službám přes šifrované spojení pomocí služby Google Cloud Pub/Sub[18] pro jakákoliv trvale dostupná globálně využitelná data, nebo pomocí služby Stackdriver Monitoring/Logging[19] pro provozní data a události. Službami technologie *cloud computing* mohou být data zpracována v posloupnosti operací (transformována, agregována, obohacena a přesunuta do trvalých úložišť) pomocí služeb Cloud Functions[20] nebo Cloud Dataflow[21]. Posloupnosti operací, kterými procházejí data, mohou zahrnovat jejich uložení na platformě Firebase[22] nebo v službách Cloud Storage Nearline[23] a Cloud Bigtable[24], ale také datové analýzy pomocí služeb Cloud Datalab[25], BigQuery a jiných popsaných v předchozím odstavci.

Na rozdíl od některých ostatních *cloud computing* řešení popsaných v této zprávě, technologie Google Cloud IoT poskytuje pouze základní služby typu PaaS bez specializací na konkrétní aplikační domény, jako je výrobní průmysl. Přesto, že existují experimentální aplikace pro technologii Google Cloud IoT, např. platforma pro připojení vozidel popsaná v [50], předpokládá se, že praktické aplikace poskytnou především HW a SW partneři, jako je Mnubo (viz kap. 3.1.6). Technologie Google Cloud IoT implementuje přístup *edge computing* (přestože ne tak dobře, jako např. Azure IoT Edge z kap. 3.1.3) a může být nasazena jako externí, proprietární řešení vně perimetru poskytované jako insourcing či outsourcing (což záleží na konkrétní implementaci) podle CCM od Fóra Jericho (viz kap. 1.1.4). Řešení umožňuje implementovat libovolné vlastní datové analýzy vč. analýz big data (ty jsou

[14] `https://cloud.google.com/bigquery/`
[15] `https://cloud.google.com/ml-engine/`
[16] `https://www.google.com/analytics/data-studio/`
[17] Pro přehled dodavatelů HW a SW, který lze připojit do technologie Google Cloud IoT, viz `https://cloud.google.com/iot/partners/`.
[18] `https://cloud.google.com/pubsub/`
[19] `https://cloud.google.com/stackdriver/`
[20] `https://cloud.google.com/functions/`
[21] `https://cloud.google.com/dataflow/`
[22] `https://firebase.google.com/`
[23] `https://cloud.google.com/storage-nearline/`
[24] `https://cloud.google.com/bigtable/`
[25] `https://cloud.google.com/datalab/`

popsány v odstavci výše). Bezpečnost je řešena jen šifrovanou komunikací a jiné bezpečnostní prvky, jako je pokročilá autentizace, řízení přístupu a správa identit musí být řešeny explicitně, např. integrací služeb Google Cloud Identity & Access Management service[26] nebo jiných služeb třetích stran.

Technologie Google Cloud IoT dobře řeší příležitosti O1 (běží na levném komoditním HW), O3, O5, O8 a O9 a dále hrozby T3 (díky otevřeným datům) a T6, při označení dle kap. 2.2. Dobře nejsou řešeny příležitosti O2 (protože je to proprietární řešení) a O4 (protože je poměrně volná architektura) a také hrozby T1, T4 a T5 (protože data jsou zpracovávána většinou až službami technologie *cloud computing*). V případě příležitosti O7 existuje platforma pro připojení vozidel [50], která je však spíše ukázkovým experimentem, než řešením připraveným k okamžitému praktickému použití.

3.1.5 SAP Cloud Platform for IoT

SAP Cloud Platform for IoT je platforma vycházející z technologie SAP HANA Cloud Platform pro rychlý vývoj, nasazení a správu aplikací pro IoT a komunikace stroje se strojem (anglicky „machine-to-machine“) (M2M) v reálném čase. Technologie SAP HANA Cloud Platform je založená na databázi SAP HANA, která umožnila uvedené platformě pro IoT rychlé zpracování datových proudů v paměti v reálném čase s podporou metod zpracování textu, prostorových dat a datových řad, či lokalizačních služeb a grafových algoritmů. [99]

Podle [100], zařízení konceptu IoT se může zaregistrovat do technologie SAP Cloud Platform pomocí služby Remote Device Management Service. Po takové registraci může zařízení odesílat zprávy do či přijímat zprávy od aplikací technologie *cloud computing* komunikací se službou Message Management Service. Zprávy přijaté službami technologie *cloud computing* mohou být přímo zpracovány službami třetích stran (jako je např. služba pro tvorbu dokumentů) a jsou uložené do databáze SAP HANA[27], případně do relačních databází SAP MaxDB[28] a SAP ASE[29]. Data zpráv poté mohou být získána z těchto databází aplikacemi konceptu IoT běžícími nad technologií *cloud computing*, nebo mohou aplikace obdržet zprávy s daty přímo od zařízení (bez uložení v databázích) komunikací se službou Message Management Service. Zařízení i aplikace mohou komunikovat se zmiňovanou službou Message Management Service přes HTTP a Hypertext Transfer Protocol over Transport Layer Security (HTTPS) nebo pomocí protokolu WebSocket či MQTT. Komunikace je šifrovaná pomocí Transport Layer Security (TLS), přičemž zařízení jsou autentizována pomocí OAuth nebo klientských certifikátů a aplikace pomocí uživatelského jména a hesla nebo také přes OAuth. Pro bezpečné řešení registrace zařízení pomocí uživatelského rozhraní IoT Service Cockpit je využit Security Assertion Markup Language (SAML).

Technologie SAP Cloud Platform for IoT je PaaS řešení pro technologii *edge computing* s veřejným nasazením externího, proprietárního „cloud“ řešení vně perimetru provozovaného jako insourcing dle CCM od Fóra Jericho (viz kap. 1.1.4). Přestože řešení označujeme za technologii *edge computing*, data ze zařízení jsou zpracovávána výhradně až službami technologie *cloud computing*, nikoliv na „edge“ zařízeních, která pouze odesílají nebo přijímají tato data (na rozdíl od některých ostatních *edge computing* řešení). Data přijatá od zařízení konceptu IoT mohou být uložena v úložišti SAP HANA pro analýzy big data nebo libovolně analyzována uživatelsky implementovanými službami (přímo nebo uložením

[26] `https://cloud.google.com/iam/`
[27] `https://www.sap.com/products/hana.html`
[28] `http://maxdb.sap.com/`
[29] `https://www.sap.com/products/sybase-ase.html`

a dotazováním pomocí relačních databází). Bezpečnost je zajištěna šifrovanou komunikací a autentizací. Případné řízení přístupu a správu identit lze řešit v externí OAuth službě.

Platforma vhodně řeší příležitosti O4 (architektura je předdefinována), O5, O8 a O9 a dále hrozby T3 (díky otevřeným databázím) dle značení z kap. 2.2. Zbytek uvedených příležitostí a hrozeb však není řešen, zejména kvůli proprietárním technologiím, příliš jednoduché bezpečnosti a fixní architektuře jen se základními službami poskytovanými platformou SAP Cloud Platform for IoT. Přestože v rámci platformy SAP HANA Cloud Platform existují použitelné služby a případy užití pro různé aplikační domény, tyto mají většinou nedostatečnou veřejně dostupnou dokumentaci a žádnou nebo příliš slabou integraci s technologií SAP Cloud Platform for IoT (bez možnosti využití technologií *edge/fog computing*).

3.1.6 Mnubo: Analýza pro průmyslové vybavení

Mnubo je řešení typu SaaS nabízející sofistikovanou platformu big data zaměřenou na IoT pomocí tří prvků: mnubo SmartObjects cloud, mnulabs a mnubo SmartObjects analytics. Platforma mnubo uplatňuje modelování business logiky a big data analýzy. Podle slov provozovatele je to zajímavá platforma pro vývoj dle konceptu IoT, nasazení a správu dle skutečných business pravidel a aplikací používajících data zařízení, kdy poskytuje pokročilé analýzy a business pohled na budoucí inovace. [116]

Podle [77] je mnubo SmartObjects řešení pro IoT s technologií „cloud“, které umožňuje příjem, zpracování a analýzu událostí (dat) z objektů (aktiv) a jejich vlastníků (zákazníků). Objekty jsou např. zařízení konceptu IoT z platforem partnerů společnosti[30] (např. zařízení s podporou technologie Google Cloud IoT). Přijatá a zpracovávaná událost se skládá z typu (což je zdroj nějaké změny), časového údaje a volitelně jedné či více číselných nebo nečíselných hodnot uspořádaných v čase. Taková událost pak upozorní služby SmartObjects, že došlo ke změně daného objektu. Při hybridním nasazení objekty posílají události přes REST API na privátní server, který je připojen k veřejným službám technologie *cloud computing*, nebo jsou události zaslány objekty přímo k veřejným službám bez účasti privátního serveru. V obou případech probíhají datové analýzy v prostředí veřejně nasazených služeb. Komunikace je šifrovaná pomocí HTTPS a každá událost je zabezpečena pomocí příznaku oprávnění daného klienta (anglicky „a client access token“), který klient obdrží po úspěšné registraci u služeb technologie *cloud computing*, kdy se prokáže platným identifikátorem a tajným heslem. Technologie SmartObjects zahrnuje veřejně nasazené služby Activity/Inactivity Analytics (analýzy stavu zařízení), Enrichment (obohacení kontextu zařízení o informace k jeho geografické poloze a počasí), Life Cycle Analytics (analýzy provozního stavu), Scoring (ohodnocení vlastníky), Session Analytics (analýzy dat mezi počáteční a koncovou událostí), Time-series Predictions (predikce na časovými řadami) a službu AI/ML Workbench, kde se používá umělá inteligence (anglicky „artificial intelligence, AI“) (UI) a strojové učení (anglicky „machine learning, ML“) (SU), např. pro predikce.

Jak bylo zmíněno výše, platforma mnubo je řešení typu SaaS pro veřejné nebo hybridní nasazení technologie *cloud computing*. Je založeno na partnerském řešení typu PaaS konkrétní platformy konceptu IoT, jako je technologie Google Cloud IoT. V souladu s CCM od Fóra Jericho (viz kap. 1.1.4) můžeme zařadit platformu mnubo jako externí, proprietární řešení umístěné vně perimetru a provozované jako outsourcing. Z hlediska bezpečnosti mnubo šifruje komunikaci a vyžaduje autentizaci zařízení pomocí příznaků oprávnění nebo tajných hesel. V současné době není uživatelům umožněna vlastní správa identit nebo řízení přístupu.

[30] `http://mnubo.com/partners/`

Platforma mnubo vhodně řeší příležitosti O5 a O9 a dále hrozbu T1 (protože podporuje různé partnerské řešení typu PaaS) dle značení z kap. 2.2. Hrozby T3 a T4 nejsou pokryty, protože dané řešení typu SaaS je proprietární a uzavřené (kromě knihoven zapojených klientů, které jsou open-source). Způsob řešení ostatních příležitostí a hrozeb závisí na použitém partnerském řešení typu PaaS a jím podporovaných službách.

3.2 Srovnávací analýza vybraných řešení

Po konzultaci s budoucími čtenáři tohoto dokumentu byla vybrána tři řešení služeb *cloud computing* pro podrobnou analýzu a porovnání, a to: ThingWorx od PTC, MindSphere od Siemens a Predix od General Electric (GE). Všechny tyto platformy podporují průmyslové technologie *edge computing* pomocí konceptu IoT a mohou poskytovat služby různé složitosti, od jednoduché integrace zařízení pro IoT v případě ThingWorx po PaaS pro analýzy v případě Predix.

3.2.1 PTC ThingWorx

V květnu 2017 vydala společnost PTC[31] verzi číslo 8 platformy pro IoT, kde lze využít i takové technologie jako rozšířená realita (anglicky „augmented reality“) (AR), nazvanou ThingWorx[32]. Platforma ThingWorx je považována za otevřené řešení typu PaaS zaměřené na IoT a AR, které bylo vytvořeno kolem jádra platformy ThingWorx Foundation. Platforma umožňuje propojení různých zařízení konceptu IoT (zejména jejich senzorů) a doručení jejich dat kdykoliv dle potřeb zákazníka. Společně se souborem dalších aplikací a nástrojů poskytuje ThingWorx řešení pro technologii *edge computing* a průmyslové provozní zpravodajství v reálném čase pro podporu aktivního a rychlého rozhodování. Jsou také připraveny jednotlivé nástroje a jejich sady pro obecný vývoj uživatelských aplikací pro AR a IoT. Jádro platformy ThingWorx Foundation je obklopeno různými nástroji, jako je ThingWorx Analytics, ThingWorx Utilities, ThingWorx Studio, a ThingWorx Industrial Connectivity[33]. Pro rozšíření technologií ThingWorx konceptu IoT na aplikace M2M, v roce 2014 PTC koupilo společnost Axeda Corporation a její produkt Axeda Machine Cloud[34] byl začleněn do technologie PTC ThingWorx.

ThingWorx může běžet buď na serverech provozovaných PTC, nebo může být nasazen na platformy AWS IoT[35] [6] či Microsoft Azure IoT Hub[36]. Kromě těchto je pravděpodobně možné i nasazená na jiné technologie *cloud computing* poskytnuté uživatelem pokud splňují stanovené požadavky. Po nasazení poskytuje technologie ThingWorx PaaS okamžitě použitelné prostředí, kde lze umístit a propojit různé komponenty, jako jsou uživatelsky definovaná datová úložiště (nabízí se několik databázových systémů, včetně řešení od společnosti SAP), průmyslové analytické aplikace, aplikace AR pro koncové uživatele a dalších.

Charakteristický model služeb: PaaS

V případě technologie ThingWorx obdrží uživatelé platformu s mnoha rozšířeními a vývojovými nástroji, okamžitě použitelnou pro vývoj vlastních aplikací. Pomocí platformy

[31] `https://www.ptc.com/`
[32] `https://www.thingworx.com/`
[33] viz `https://www.thingworx.com/platforms/thingworx-foundation/` a tam odkazované informace
[34] https://www.ptc.com/axeda
[35] `https://aws.amazon.com/iot/`
[36] `https://azure.microsoft.com/en-us/services/iot-hub/`

mohou uživatelé stejným způsobem komunikovat s mnoha zařízeními konceptu IoT a získávat analytické informace o užití a provozním stavu těchto zařízení, včetně včasné predikce jejich případných selhání. Dalším typickým případem užití jsou aplikace AR pro podporu činností koncových uživatelů (např. mohou ukazovat uživatelům v reálném čase, jak doplnit chladicí kapalinu v autě) nebo techniků (např. jak vyměnit v autě pokažené čerpadlo).

Všechny nástroje a okamžitě použitelné služby jsou vystavěny kolem jádra technologie ThingWorx Foundation. Nástroj ThingWorx Studio slouží k vývoji aplikací, přičemž aplikace AR jsou určeny pro systémy iOS, Android a HoloLens[37].

Architektura technologie „cloud“: edge

Technologie ThingWorx má poměrně jednoduchou architekturu, kde propojuje zařízení konceptu IoT s cílovými aplikacemi, které konzumují data z těchto zařízení. Jsou zde v podstatě tři komponenty, a to zdrojové zařízení konceptu IoT, ThingWorx PaaS technologie *cloud computing* a jakákoliv cílová aplikace.

Jádro technologie ThingWorx Foundation tvoří tyto tři komponenty následovně:

1. ThingWorx Foundation Core, které zahrnuje Application Enablement Platform (AEP) a služby platformy.
2. ThingWorx Foundation Connection Services, které zahrnují servery pro spojení, zařízení a jejich adaptéry pro technologii *cloud computing* a tunelovací servery.
3. ThingWorx Foundation Edge, který obsahuje Edge MicroServer a Edge „Always On“ soubor nástrojů pro vývoj software (anglicky „software development kit“) (SDK).

Na jádro technologie ThingWorx Foundation jsou dále napojeny čtyři SW aplikace či sady nástrojů pro tvorbu aplikací, připojení SW zařízení, vykonávání analytických operací a jiné. Aplikace AR lze snadno vytvořit v nástroji ThingWorx Studio [113]. Balík ThingWorx Industrial Connectivity pak slouží k připojení různých zařízení a poskytuje jediný zdroj dat průmyslové automatizace[38]. Komponenta ThingWorx Analytics[39] poskytuje analytické a prediktivní operace pomocí služeb ThingWatcher, ThingPredictor, ThingAnalyzer a ThingWorx Analytics Server. A poslední služba ThingWorx Utilities[40] umožňuje správu připojených zařízení konceptu IoT, včetně správy jejich procesních workflow a integrace na úrovni IoT.

CCM klasifikace: externí/interní, proprietární, vně perimetru, insourcing/outsourcing

Podle CCM od Fóra Jericho (viz kap. 1.1.4), může být technologie ThingWorx zařazena mezi externí i interní řešení technologie *cloud computing* (implicitně je ThingWorx nasazen na infrastruktuře PTC, avšak může být nasazen také v AWS nebo Microsoft Azure). Jedná se o proprietární řešení s uzavřeným kódem, které lze vnímat jako umístěné vně perimetru organizace (autentizace a řízení přístupu jsou implementovány vývojářem aplikace, avšak při spojení do ThingWorx Foundation se mohou posílat data téměř kamkoliv). Technologie ThingWorx může být provozována jako insourcing (tj. privátní řešení technologie *cloud computing* provozované, je-li potřeba, zaměstnanci organizace) avšak je možný i jiný způsob provozu, tedy outsourcing.

[37] `https://www.microsoft.com/microsoft-hololens/en-us`
[38] viz `https://www.kepware.com/en-us/`
[39] `https://www.thingworx.com/platforms/thingworx-analytics/`
[40] `https://www.thingworx.com/platforms/thingworx-utilities/`

Díky externímu i internímu nasazení a provozování jako insourcing i outsourcing je možností implementace ThingWorx aplikací. Pro usnadnění výběru správné možnosti nabízí PTC zkušenosti [115] a řešení svých zákazníků včetně několika certifikací na PTC/ThingWorx. Konkrétně se uvádí „... ThingWorx Platform (může být) poskytovaná buď vlastními prostředky nebo pomocí centra SSAE 16/SOC 2 poskytujícího služby na vyžádání prověřených certifikačními systémy ISO27001:2013 a provozním týmem (skupinou) se závazkem zabezpečit naše (PTC) služby pro naše (PTC) zákazníky“ [114].

Analýza dat: předdefinovaná nebo libovolná

Platforma ThingWorx nabízí službu ThingWorx Analytics jako svoji základní část. Mimo to jsou k dispozici různé, jednoduché i složitější, sady nástrojů pro vizualizaci v prostředí ThingWorx Studio, které mohou být součástí případných aplikací pro AR vytvořených pro zařízení konceptu IoT.

Jak bylo již zmíněno výše, služby ThingWorx Analytics obsahují několik komponent, které umožňují např. zkoumání dat, predikci budoucího chování zařízení, správu workflow a jiné.

Mimo uvedené, platforma ThingWorx umožňuje zejména dobré propojení různých komponent. Proto lze pro analýzy použít také libovolné nástroje a aplikace pro big data, uživatelsky implementované či dodané třetími stranami, které lze napojit na datové proudy poskytované platformou ThingWorx. Mimo jiné mohou být napojeny také produkty SAP [99] a mohou být tak využity jejich analytické schopnosti.

Bezpečnost: šifrovaná komunikace, autentizace a řízení přístupu

Platforma ThingWorx Platform slouží jako prostředek pro přenos dat jednotným způsobem mezi zdrojem (kterým je obvykle zařízení konceptu IoT) a cílem (monitorovací aplikace, úložiště a jiné). Tento přenos je zranitelný pouze dvěma způsoby a to ohrožením komunikační linky a samotné platformy ThingWorx. Pokud nebereme v úvahu útok na platformu ThingWorx, tedy ji považujeme za bezpečnou a spolehlivě fungující, zbývá zabezpečit komunikační linku. Jak již dříve bylo zmíněno [114], PTC podporuje komplexní řešení a nástroje, jak nejenom zabezpečit přenos dat, ale také zajistit jejich bezpečné uložení, zpracování a další. Způsob zabezpečení tedy závisí hlavně na vývojářích aplikací a jejich dovednostech, které v tomto ThingWorx a PTC plně podporuje.

Pro výše uvedené má platforma ThingWorx velmi podrobný bezpečností model pro izolaci dat a spouštění služeb [114]. Tento umožňuje zejména HTTPS autentizaci, napojení na Lightweight Directory Access Protocol (LDAP), použití průmyslových standardů, jako je SAML a jednotné přihlášení (single sign-on) a integraci s jinými bezpečnostními nástroji, naprř. od SAP. Platforma ThingWorx používá seznam přístupových práv uživatelů pro řízení přístupu prakticky ke všem možným operacím.

Příležitosti

Následující příležitosti dle kap. 2.2 mohou být řešeny prostředky platformy ThingWorx:

O1 *Nízká počáteční investice* – Ceníky nejsou veřejné a Česká republika není mezi státy, kde je pronájem technologie ThingWorx oficiálně dostupný. ThingWorx Studio je nabízeno se zkušební lhůtou nejméně 90 dnů (může být rozšířena až na 120 dnů). PTC nabízí mnoho služeb poskytovaných online bez nutnosti vlastních prostředků lokální IT. Absence lokální IT však nepřipadá v úvahu pro produkční nasazení. Proto lze nějaké počáteční investice v případě produkčního nasazení očekávat.

O2 *Outsourcing a management IT služeb* – Všechny služby mohou být provozovány jako outsourcing a poskytovány třetími stranami. Např. ThingWorx Platform může být poskytována PTC a datové úložiště jiným poskytovatelem.

O3 *Složeniny* – Platforma ThingWorx je určena hlavně pro jednotné propojení poskytovatelů dat a jejich konzumentů. Vytváření složenin s existujícími aplikacemi by proto mělo být možné.

O5 *Škálovatelnost* – Platforma ThingWorx je platformou technologie *cloud computing*, a proto by zde obecně neměl být problém se škálovatelností.

O7 *Připojené vozidlo* – Je možné použít platformu ThingWorx společně s vlastními aplikacemi takovým způsobem, že bude podporovat připojené vozidlo pomocí technologií IoT a *edge computing*. Data získaná z vozidla mohou být, po předzpracování, odeslána jednotným způsobem pomocí platformy ThingWorx k dalšímu zpracování a analýze aplikacemi, např. pro optimalizaci dopravy, predikci poruch a jiné.

O9 *Lepší monitorování (transparence)* – Platforma ThingWorx se snaží zajistit jednotný přístup k datovým proudům pro různé cílové aplikace. Monitorování takových dat je proto pro příslušné aplikace jednodušší. Aplikace mohou být vyvíjeny buď vlastními silami zákazníkem, nebo lze použít již hotová dostupná řešení.

Hrozby

Platforma ThingWorx již řeší následující hrozby zmiňované v kap. 2.2, nebo by tyto hrozby měly být řešeny při nasazení a uživatelskými aplikacemi:

T1 *Závislost a odevzdání se prodejci* – Platforma ThingWorx je proprietární SW, a proto je zde riziko. Přestože aplikace vyvinuté na této platformě budou patřit zákazníkovi, pokud se něco stane s platformou, tak bude nezbytné větší část aplikací implementovat znovu kvůli jejich závislosti na uzavřeném proprietárním řešení.

T3 *Závislost na datech, důvěrnost dat, sdílená pověst* – Pokud jsou použita datové úložiště poskytovaná PTC, může být problém se závislostí a důvěrností dat. Na druhou stranu, neustálý přenos dat mezi vlastními zařízeními konceptu IoT a platformou ThingWorx umístěnou u PTC má také své nevýhody. Data by měla být šifrována a platforma ThingWorx pro toto poskytuje vhodné prostředky. Šifrování však může zpomalit následná zpracování dat.

T4 *Nepřenositelná odpovědnost* – Pokud je platforma ThingWorx provozována lokálně, není problém s netransparentní odpovědností. Pokud však je využit některý z poskytovatelů technologie *cloud computing* (např. PTC či Amazon), je tu hrozba, která musí být vhodně řešena příslušnými smlouvami.

T5 *Úzká místa datového přenosu* – Platforma ThingWorx podporuje rozsáhlé sítě a velké množství dat může být přenášeno do vzdálených lokací. Pokud je aplikace citlivá na správné načasování doručení dat, může náročnost jejich přenosu způsobovat problémy. Ale to je problém obecně, nejen u platformy ThingWorx.

T6 *Nestabilita výkonu ve víceuživatelských prostředích* – Platforma ThingWorx není určena pro operace v reálném čase ve smyslu dodržování určitých dob trvání operací. Z toho důvodu není případná nestabilita výkonu ve víceuživatelských prostředích žádný problém.

Shrnutí

Platforma ThingWorx nabízí mnoho možností jak monitorovat, řídit, prezentovat uživatelům, analyzovat a udržovat zařízení konceptu IoT. Toto platí nejen pro jednotlivá zařízení, ale také pro jejich skupiny/posloupnosti a celé workflow vykonávající uvedené akce. Platforma ThingWorx pro toto poskytuje předdefinované a připravené nástroje, ale také především jednotný způsob přístupu k datům poskytovaným zařízeními konceptu IoT a tvorby různých aplikací nad daty. Takovými aplikacemi může být monitorování a predikce chyb zařízení i využití AR s cílem pomoci pracovníkům zákazníka nebo jeho koncovým uživatelům. Můžeme tedy říci, že platforma ThingWorx je rozsáhlý rámec umožňující provozovat technologii *edge computing* a obsluhu zařízení konceptu IoT jednotným způsobem s mnoha (vývojovými) nástroji a programy pro tvorbu aplikací.

Technologie ThingWorx je zavedená platforma, která umožňuje použití existujících prvků, např. použití souborů pro počítačem podporované projektování (anglicky „computer-aided design“) (CAD) pro tvorbu aplikací AR, úložišť a analytických nástrojů, třeba ve spojení s produkty SAP. Navíc, PTC nabízí předem připravené stavební bloky pro vývoj uživatelských aplikací různých účelů a zaměření.

3.2.2 Siemens MindSphere

V červenci 2016 spustil Siemens platformu pro průmyslové využití technologie *cloud computing* nazvanou „MindSphere – otevřený operační systém pro IoT založený na *cloud computing* od Siemens“. Podle [105] je MindSphere otevřenou platformou technologie *cloud computing*, která je nabízena formou PaaS a navržena jako operační systém pro IoT s datovými analýzami a možnostmi různých napojení, nástroji pro vývojáře, aplikacemi a službami. Platforma MindSphere pomáhá vyhodnotit a využít průmyslová data a získat nový vhled, např. pro provedení optimalizace výkonnosti zařízení pro jejich maximální nepřerušovaný běh. Navzdory prohlášení, že „MindSphere nabízí zákazníkům vývojové prostředí, ve kterém mohou integrovat jejich vlastní aplikace a služby“ [105], platforma MindSphere a její nadstavba MindApps, což jsou aplikace poskytnuté společností Siemens a běžící na platformě MindSphere, jsou nyní (červen 2017) stále ve stavu neveřejné beta verze s omezeným přístupem bez žádného obchodu s aplikacemi a dokumentace pro jejich vývoj[41].

V této kapitole bude platforma Siemens MindSphere analyzována a vyhodnocena pro srovnání ve své aktuální uzavřené beta verzi, společně s platformou SAP Cloud Platform založené na technologii SAP HANA pro analýzu dat. Obě tato řešení s technologií *cloud computing* využívají platformu Cloud Foundry[42], takže mohou být nasazena v libovolném prostředí technologie *cloud computing* s podporou Cloud Foundry[43]. Zatímco platforma Siemens MindSphere není dosud veřejně dostupná k nasazení na technologii Cloud Foundry, platforma SAP Cloud Platform je na technologii Cloud Foundry nasazena a její produkty typu SaaS, jako je SAP S/4 HANA nebo SAP Business ByDesign, jsou do technologie Cloud Foundry dobře začleněny a připraveny v tomto prostředí k okamžitému použití.

Charakteristický model služeb: SaaS (výhledově PaaS)

V současné době implementuje technologie MindSphere model typu SaaS, kde je zákazníkovi poskytnut SW běžící na technologii *cloud computing* (MindSphere Launchpad, viz

[41] viz `https://community.plm.automation.siemens.com/t5/x/x/m-p/409469` a `https://community.plm.automation.siemens.com/t5/x/x/m-p/412773`

[42] `https://www.cloudfoundry.org/`

[43] Ve skutečnosti je platforma Siemens MindSphere založena na platformě SAP HANA Cloud Platform, která využívá technologii Cloud Foundry.

kap. 3.2.2). Přestože zákazníci musejí instalovat „edge“ zařízení (MindConnect prvky, také v kap. 3.2.2), která by byla dobře přizpůsobitelná pro složité aplikace, tato zařízení nyní pouze odesílají data službám technologie *cloud computing* a sama neposkytují žádné služby. Také vývoj vlastních aplikací běžících na platformě MindSphere (tj. MindApps) není dosud v uzavřené beta verzi podporován. Z toho důvodu jsou v současné době k dispozici pouze předdefinované aplikace od Siemens poskytované modelem SaaS.

Přesto, jak uvádí [105], MindSphere je navržen jako PaaS model a v blízké době bude k dispozici jak přizpůsobení „edge“ zařízení, tak vývoj uživatelských aplikací technologie *cloud computing* běžících na platformě MindSphere.

Architektura technologie „cloud“: edge

Podle [106] je architektura MindSphere rozdělena do třech vrstev: MindSphere „cloud“, prvky MindConnect a průmyslová zařízení. V prostřední vrstvě prvků MindConnect, MindConnect Nano a menší MindConnect IoT2040 zařízení čtou monitorovaná data průmyslových zařízení ze serverů SIMATIC S7-300/400 PLC a OPC-UA ve spodní vrstvě architektury pomocí průmyslové sítě Ethernet. Poté, co prvky MindConnect navážou spojení se službami platformy MindSphere technologie *cloud computing* přes internet (na dalším rozhraní sítě Ethernet), data posbíraná ze zařízení jsou přenesena k MindSphere službám. Ve vrchní vrstvě architektury, služby MindSphere technologie *cloud computing* nabízejí přes webové uživatelské rozhraní MindSphere prostředky služby Launchpad pro sledování stavu zařízení na základě sesbíraných a přijatých dat.

Služba MindSphere Launchpad je vstupním bodem k dalším uživatelským rozhraním aplikací MindApps pro vizualizaci dat a konfiguraci. Aplikace MindApps mohou být otevřeny z libovolného dostatečně aktuálního webového prohlížeče se schopnostmi HTML5. V platformě MindSphere mohou uživatelé přes grafické uživatelské rozhraní vytvářet, konfigurovat, prozkoumat a vizualizovat „digitální dvojče“ (anglicky „digital twin“) jakéhokoliv průmyslového zařízení. [106]

V současné době, v uzavřené beta verzi, služba MindSphere Launchpad poskytuje tři systémové aplikace MindApps: MindSphere Asset Configuration, MindApp Fleet Manager a MindSphere User and Customer Management (tedy česky: konfiguraci jednotlivých zařízení, správu všech zařízení a správu uživatelů a zákazníků). Podle [106], aplikace Asset Configuration poskytuje prostředky pro konfiguraci průmyslového zařízení a zařízení MindConnect Nano/IoT2040, pro definici struktury monitorovaných dat a jejich vlastností, pro nastavení napojení MindConnect Nano/IoT2040 zařízení k monitorovaných průmyslovým zařízením a ke službám MindSphere technologie *cloud computing* a pro správu metadat průmyslových zařízení (např. jejich geografických umístění). Aplikace Fleet Manager je používána pro přehled existujících zařízení a jejich základních informací, ale také k vizualizaci monitorovaných dat včetně jejich analýz – pro pohled na různé proměnné a různými aspekty a jejich zobrazení ve tří různých typech grafů (čárový, koláčový a sloupcový graf) v různých časových intervalech. Uživatelé služby Fleet Manager mohou také vytvářet ručně požadavky, jako jsou varování nebo požadavky na údržbu, nebo definovat pravidla pro jejich automatické generování. Poslední služba MindApps je nazvaná User Management and Customer Management a slouží pro přidávání a správu uživatelů služeb MindSphere Launchpad ve dvou rolích („admin“ a běžný uživatel „user“) a také pro přidávání a správu zákazníků, kdy uživatelé v roli „admin“ mohou vytvářet účty pro své zákazníky a přiřazovat jim průmyslová zařízení.

Tato architektura je v souladu s přístupem *edge computing*, kde jsou data extrahována z průmyslových zařízení pomocí „edge“ zařízení (MindConnect prvků) a přenášena ke službám technologie *cloud computing* pro další zpracování (MindSphere „cloud“). Zařízení

„edge“ konceptu IoT jsou spravována pomocí služby MindSphere Asset Configuration. Architektura není ani statická (účast „edge“ zařízení je dynamická), ani to není architektura *fog computing* („edge“ zařízení jen slouží službám technologie *cloud computing*).

CCM klasifikace: externí/interní, proprietární, vně perimetru, insourcing

Podle CCM od Fóra Jericho (viz kap. 1.1.4) může být MindSphere v uzavřené beta verzi zařazen jako externí i interní (implicitně je nasazen na infrastruktuře Siemens, nebo může být v privátním nasazení), proprietární (uzavřené řešení od Siemens včetně HW zařízení pro MindConnect prvky), vně perimetru (autentizace a řízení přístupu je implementováno dodavatelem v aplikaci MindSphere User and Customer Management, tj. mimo perimetr infrastruktury zákazníka) a poskytovaný jako insourcing (privátní nasazení může být obsluhováno pracovníky zákazníka, je-li to vyžadované).

Toto zařazení je však neformální a nestálé, protože platforma MindSphere je v uzavřené beta verzi plně dostupná pouze vybraným partnerům a pravděpodobně silně přizpůsobena jejich individuálním potřebám. V těchto případech může individuální přizpůsobení platformy MindSphere zahrnovat různé další aplikace MindApps v hybridně nasazené technologii *cloud computing* a to interní i externí, poskytované jako insourcing i outsourcing a integrované s otevřenými technologiemi, jako je Cloud Foundry.

Analýza dat: předdefinovaná nebo big data (SAP HANA Cloud Platform)

Uvnitř je platforma MindSphere postavena na technologii SAP HANA Cloud Platform[44], což je platforma SAP Cloud Platform s databází SAP HANA pro práci s daty v paměti poskytovaná modelem PaaS. Technologie SAP HANA nabízí běhové prostředí pro technologie *cloud computing* aplikacím, které ukládají, manipulují a dotazují data v souladu s konceptem big data a fast data z kap. 1.2.3. I přes tento fakt, uzavřená beta verze platformy MindSphere ve své aplikaci MindApp Fleet Manager umožňuje uživatelům pouze základní pohledy na data, vizualizace a analýzy (nikoliv big data). Podle [106] je možné filtrovat data na základě jejich zdroje, času a dalších aspektů, zobrazit různé proměnné s různými aspekty a to číselně nebo ve třech typech grafů (čárový, koláčový a sloupcový graf) v různých časových intervalech. Jak již také bylo uvedeno výše, uživatelé aplikace Fleet Manager mohou vytvářet požadavky a to ručně, nebo v rámci automatických analýz na základě vstupních dat.

Analytické schopnosti popsané výše jsou poměrně jednoduché s přednastaveným způsobem, jak se dotazovat a zobrazovat a analyzovat data. Tyto analýzy fungují poměrně dobře, zejména v případě časové posloupnosti dat, tedy pro sekvenci po sobě jdoucích měřených hodnot z datových zdrojů [106]. Analýzy aplikace MindApp Fleet Manager by byly však jen stěží dostatečné pro rozsáhlé monitorování, např. v CMfg. Oproti tomu schopnosti datových analýz a vizualizace v platformě SAP HANA Cloud Platform by přinesly plnou podporu big data analytiky a velmi dobrou integraci se systémy pro zpracování big data, jako je SAP Vora[45]. Očekáváme, že big data analýzy budou dostupné v budoucích verzích platformy MindSphere (nebo v případě vysoce individuálně upravených nasazení uzavřené beta verze).

[44] `https://www.sap.com/products/hana-enterprise-cloud.html`
[45] `https://www.sap.com/products/hana-vora-hadoop.html`

Bezpečnost: šifrovaná komunikace a úložiště, autentizace, řízení přístupu

Komunikace mezi prvky MindConnect, tj. zařízeními MindConnect Nano/IoT2040, a službami platformy MindSphere technologie *cloud computing* je šifrována v HTTPS. Na každém zařízení je pouze jedno otevřené odchozí HTTPS spojení (tzn. žádné příchozí či jiná odchozí spojení) a konfigurace zařízení je prováděna přes lokální HW port nebo vzdáleně v aplikaci MindSphere Asset Configuration přístupné z MindSphere Launchpad. Autentizace a řízení přístupu je vykonáváno aplikací MindSphere User and Customer Management opět přístupné z prostředí služby MindSphere Launchpad s uživateli dvou předdefinovaných rolí („admin“ a obyčejný uživatel „user“). Bohužel nejsou k dispozici žádné informace ohledně pokročilé konfigurace těchto bezpečnostních rysů, jako je nastavení vlastního certifikátu pro HTTPS šifrovanou komunikaci, vlastních uživatelských rolí a jiných nastavení řízení přístupu, nebo využití externích služeb pro správu identit a autentizaci pro jednotné přihlášení (anglicky „single sign-on“) a další.

Také bezpečnost infrastruktury technologie *cloud computing* není detailně diskutována v uzavřené beta verzi platformy MindSphere. Přesto lze očekávat dostupnost bezpečnostních rysů implementovaných podpůrnými technologiemi, tj. v SAP HANA Cloud Platform a v Cloud Foundry. Například platforma SAP Cloud Platform [101] implementuje mnoho bezpečnostních opatření, jako je izolace daných aplikací a sítí, oddělení uživatelů a jejich sítí, bezpečnou komunikaci, zabezpečené kontejnery aplikací, bezpečnější systémová nastavení, šifrování prostoru klientů a bezpečnost záloh a logů. Podobně, také Cloud Foundry [25] může nabídnout virtualizaci, izolaci kontejnerů a šifrování, stejně jako služby pro správu identit a autentizaci.

Příležitosti

Následující příležitosti, v označení podle kap. 2.2, jsou řešeny v platformách Siemens MindSphere a SAP Cloud Platform:

O1 *Nízká počáteční investice* – Platforma Siemens MindSphere může být používána v minimální konfiguraci jedné licence MindAccess User[46] při veřejném nasazení na infrastruktuře MindSphere a s jedním zařízení MindConnect Nano/IoT2040, kam budou připojena průmyslová zařízení, např. PLC. Licence MindAccess User umožňuje zákazníkovi přístup a použití platformy MindSphere a zahrnutých aplikací MindApps za fixní měsíční poplatek (za prvních 50 uživatelů zákazníka) a další měsíční poplatek dle konfigurace (další uživatelé, datový model a počet připojených průmyslových zařízení, míra používání MindApps). V dubnu 2017 stálo jedno MindConnect Nano zařízení 990 EUR a licence MindAccess User 150 EUR měsíčně[47]. V případě privátního nasazení, např. kvůli větší bezpečností, bude počáteční investice výrazně větší.

O2 *Outsourcing a management IT služeb* – Platforma MindSphere je nabízena ve výchozí konfiguraci jako okamžitě použitelné veřejné nasazení technologie *cloud computing* u společnosti Siemens a je tedy již provozována jako outsourcing uvedenou společností. Přestože je platforma MindSphere založena na platformách Cloud Foundry a SAP HANA Cloud Platform, které mohou být nasazené na jakékoliv infrastruktuře IT kompatibilní s Cloud Foundry včetně řešení IaaS, přesun od Siemens k jinému poskytovateli nemusí být z mnoha důvodů lehký, zejména v případě uzavřené beta verze platformy MindSphere (důvodem jsou proprietární protokoly, nedostatečná dokumentace a další).

[46] see `https://support.industry.siemens.com/cs/products/9ac2513-3mj11-4nd4`
[47] see `https://community.plm.automation.siemens.com/t5/x/x/ta-p/403910`

O3 *Složeniny* – V současné době není uzavřená beta verze platformy MindSphere připravena na integraci s jinými službami technologie *cloud computing* od Siemens či jiných poskytovatelů. Proto je tvorba složených řešení problematická.

O5 *Škálovatelnost* – Protože běží platforma MindSphere na technologiích Cloud Foundry a SAP HANA Cloud Platform, její škálovatelnost je velmi dobrá.

O9 *Lepší monitorování (transparence)* – Siemens MindSphere je platforma navržená pro sbírání, zpracování, uchování a prezentaci analýz a vizualizací monitorovaných dat od připojených průmyslových zařízení. Z toho důvodu významně vylepšuje monitoring průmyslových zařízení ve výrobě a zvyšuje transparentnost běžících výrobních procesů.

V současné době je Siemens MindSphere jen platforma pro monitorování a analýzu průmyslových dat bez podpory CMfg dle definice v kap. 2.1.2. Z toho důvodu nemůže platforma Siemens MindSphere řešit příležitosti O7 (připojené vozidlo) a O8 (agilní výroba), které by mohly být zajímavé pro výrobní průmysl. Avšak s otevřením platformy a možností vlastního vývoje aplikací MindApps pro platformu MindSphere se pravděpodobně objeví i lepší podpora pro CMfg a integraci s dalšími produkty Siemens, např. pro výrobu automobilů.

Hrozby

Následující hrozby, označené podle kap. 2.2, jsou řešeny platformami Siemens MindSphere a SAP Cloud Platform, nebo jsou na uvedených platformách problematické:

T1 *Závislost a odevzdání se prodejci* – Platforma Siemens MindSphere přináší silnou závislost na technologiích Siemens (např. MindConnect Nano/IoT2040 jsou proprietární uzavřená HW zařízení), stejně jako na v ní použitých komerčních produktech ze SAP HANA Cloud Platform. Hrozí zde závislost a odevzdání se prodejci.

T3 *Závislost na datech, důvěrnost dat, sdílená pověst* – V případě veřejného nasazení Siemens MindSphere může být obtížné chránit data v souladu se zavedenými bezpečnostními předpisy organizace zákazníka, ale také data přesunout k jinému poskytovateli jiných služeb technologie *cloud computing*. Tento problém však může být vyřešen privátním nasazením technologie Cloud Foundry a SAP HANA Cloud Platform pro platformu MindSphere, kde jsou pak data plně ovládána organizací zákazníka.

T4 *Nepřenositelná odpovědnost* – V případě privátního nasazení platformy Siemens MindSphere není nepřenositelná odpovědnost problém. Situace však může být jiná v případě implicitního veřejného nasazení, kdy musí být odpovědnosti formálně definovány v rámci dokumentu dohoda o úrovni služeb (anglicky „Service Level Agreement“) (SLA).

T5 *Úzká místa datového přenosu* – Pro komunikaci mezi prvky MindConnect, tj. zařízeními MindConnect Nano/IoT2040, a službami MindSphere technologie *cloud computing*, je vyžadováno přímé nebo směrované propojení přes síť internet. Toto síťové spojení může být úzkým místem datového přenosu pro svou omezenou kapacitu a dostupnost. Přesto, dočasně chybějící či nedostatečné připojení do sítě internet by nemělo být problém, protože prvky MindConnect jsou schopné dočasně uchovat odesílaná data, pokud jsou bez připojení, a odeslat je jakmile bude internetové připojení opět k dispozici.

T6 *Nestabilita výkonu ve víceuživatelských prostředích* – Protože je platforma MindSphere využívána pouze k analýzám monitorovacích dat (filtrování, prezentace a vizualizace), nikoliv pro úlohy řešené v reálném (či téměř reálném) čase, jako je PLC nebo VRC, nestabilita výkonu zde není validní hrozbou.

Shrnutí

Přestože je platforma Siemens MindSphere vybudována na technologiích SAP HANA Cloud Platform a otevřené Cloud Foundry, které jsou využívány jako služby modelu PaaS/IaaS, je platforma MindSphere uzavřené proprietární řešení. Platforma MindSphere o sobě prohlašuje, že nabízí služby dle modelu PaaS pro vývoj aplikací MindApps, ale ve skutečnosti v uzavřené beta verzi je to SaaS řešení bez veřejně dostupné vývojářské dokumentace a nástrojů. Tyto dvě nevýhody lze považovat za velký handicap a měly by být odstraněny. Navíc není MindSphere vhodná pro plně funkční výrobní „cloud“ dle CMfg, protože je primárně navržena pro monitorování spíše než pro řízení připojených průmyslových zařízení. MindSphere také v současné době umožňuje pouze jednoduché analýzy monitorovacích dat v předdefinovaných MindApps. Vývoj vlastních aplikací MindApps s podporou big data analýz je problematický z důvodu chybějící dokumentace, nástrojů a integrace s big data SW systémy pro zpracování velkých dat.

I přes výše uvedené nevýhody je platforma Siemens MindSphere zajímavý projekt se smysluplnými aplikacemi pro monitorování a správu průmyslových/výrobních zařízení ve výrobním průmyslu, zejména, pokud tato zařízení také používají technologie Siemens, např. pro PLC.

3.2.3 GE Predix

Predix od GE je platforma technologie *cloud computing* pro sběr, analýzu a prezentaci dat z průmyslových zařízení za účelem predikce případných problémů, provádění preventivní údržby a snížení neplánovaných výpadků [46].

Charakteristický model služeb: PaaS

Jak uvádí [46], jádrem platformy Predix pro průmyslový internet, tedy síť průmyslových zařízení, je technologie Predix Cloud založená na škálovatelné infrastruktuře technologie *cloud computing*, která je základem pro model PaaS. Vývojáři využívají platformu Predix Cloud pro tvorbu, nasazení a spouštění aplikací průmyslového internetu a to aplikací předdefinovaných v Predix i nově implementovaných v programovacích jazycích Java, Matlab nebo Python. Sama technologie Predix neposkytuje vlastní nízkoúrovňovou platformu nebo infrastrukturu jako službu, tj. PaaS/IaaS; toto je delegováno na uvnitř použitý rámec Cloud Foundry[48]. Platforma Predix tedy může běžet na jakékoliv privátně, veřejně, či hybridně nasazené infrastruktuře technologie *cloud computing*, pokud tato podporuje technologie Cloud Foundry. Také SaaS není model služeb nabízených v rámci platformy Predix, protože takové služby jsou v platformě Predix obvykle nově implementované nebo složené z komponent platformy Predix, navzdory skutečnosti, že existuje několik již připravených aplikací technologie *cloud computing*.

Architektura technologie „cloud“: edge

Architektura technologie *cloud computing* se v platformě Predix skládá z komponent pěti typů: Predix Machine, Predix Connectivity, Predix EdgeManager, Predix Cloud a Predix

[48] `https://www.cloudfoundry.org/`

Services.

Predix Machine je SW, který komunikuje s průmyslovými přístroji a se službami Predix Cloud a kde běží lokální aplikace technologie *edge computing*, např. pro analýzu. Predix Connectivity slouží pro síťové propojení komponent Predix Machine se službami Predix Cloud, pokud není k dispozici vlastní přímé spojení přes síť internet (v opačném případě jsou SW komponenty Predix Machine a služby Predix Cloud spojeny přímo přes internet, bez Predix Connectivity). Predix EdgeManager spravuje zařízení technologie *edge computing*, na kterých běží Predix Machine. Predix Cloud je globální infrastruktura technologie *cloud computing* pro běh služeb Predix Services a jejich katalogu, kde mohou vývojáři publikovat své služby i konzumovat a integrovat služby poskytnuté třetími stranami. Predix Services jsou průmyslové služby, které mohou vývojáři použít ke tvorbě, testování a ke běhu aplikací průmyslového internetu.

Tato architektura je v souladu s principy *edge computing*, kde jsou data přijímána z „edge" zařízení (kde běží Predix Machine) a přenášena ke službám technologie *cloud computing* pro další zpracování (tj. přenášena přes internet nebo pomocí Predix Connectivity do Predix Cloud pro zpracování službami Predix Services). Zařízení „edge" konceptu IoT jsou spravována v aplikaci Predix EdgeManager. Platforma Predix nemá statickou architekturu (účast „edge" zařízení je dynamická) ani architekturu *fog computing* („edge" zařízení pouze slouží ostatním službám).

CCM klasifikace: interní, proprietární, vně perimetru, insourcing

Podle CCM od Fóra Jericho (viz kap. 1.1.4), může být Predix zařazen mezi interní (může být privátně nasazen na Cloud Foundry) a proprietární (uzavřené řešení poskytované společností GE) řešení umístěné vně perimetru (autentizace a řízení přístupu jsou řešeny předdefinovanými službami User Account and Authentication Service a Access Control Service, které obě běží na technologii Predix Cloud u jejího poskytovatele, tedy mimo perimetr IT infrastruktury zákazníka). Řešení může být provozováno jako insourcing (tedy privátně nasazené a udržované zaměstnanci zákazníka, je-li to potřeba).

V případě jiného než privátního nasazení Predix Cloud nad Cloud Foundry PaaS/IaaS službou nasazenou veřejně nebo hybridně může být klasifikace jiná, např. může být platforma Predix provozována externě jako outsourcing (data jsou pak uložená a spravovaná třetí stranou, tedy poskytovatelem IaaS, kde Predix běží).

Analýza dat: libovolná

Vstupním bode pro všechna data přicházející z různých zdrojů je fronta příjmu. Podle [46], přijímá tato fronta data přes HTTP proudy v reálném, či téměř reálném, čase (pro fast data dle kap. 1.2.3) nebo pomocí File Transfer Protocol (FTP) v případě dávkového zpracování dat. Mimo to, předtím něž jsou data uložena, mohou být ve frontě zpracována, např. anotována, kombinována s jinými daty, nebo zpracována jako komplexní události (systém pak hledá kombinace určitých typů událostí, aby vytvořil vysokoúrovňovou business událost). Data mohou být uložena v distribuovaném škálovatelném datovém úložišti pro časové řady (vhodné např. pro senzorová data s posloupnostmi změřených hodnot), úložišti pro data typu velký binární objekt (anglicky „binary large object") (BLOB) (pro velká obrazová data do velikosti 10 GB) a v PostgreSQL[49] otevřené relační databázi (pro relační data).

Data mohou být analyzována seskupeními více předdefinovaných a vlastních analytických služeb zanesených v analytickém katalogu. Analytické služby mohou provádět provozní analýzy aktuálních dat a historické analýzy dat z datových úložišť popsaných výše.

[49] `https://www.postgresql.org/`

V katalogu je skupina předdefinovaných analytických služeb zahrnující implementace komplikovaných algoritmů pro problémy, jako jsou detekce anomálií či SU [46]. Mimo uvedené mohou být vytvořeny další vlastní služby v jazycích Java, Matlab a Python. Seskupení analytických služeb jsou popsána v Business Process Modelling Notation (BPMN) verze 2.0 a na vyžádání spuštěna službou běhového prostředí. Seskupením služeb pro provozní i historickou analýzu je možné implementovat složité analýzy trendů a další.

Jak bylo popsáno výše, fronta příjmu se v Predix zaměřuje na příjem dat typu fast data, na přenos dat a jejich zpracování. Úložiště pro časové řady a data typu BLOB podporuje uložení dat z fronty jako big data. Predix však není vhodná platforma pro analýzy typu big data dle kap. 1.2.3. Podrobné analýzy dat typu big data/fast data by měly být provedeny se speciálních nástrojích pro zpracování dat typu big data, jako je Apache Spark[50], které budou volány z vlastních analytických služeb.

Bezpečnost: šifrovaná komunikace, identity, autentizace, řízení přístupu

Podle [46] provádí šifrování dat a autentizaci/autorizaci pro řízení přístupu komponenta Predix Machine. Pro vysokou bezpečnost komunikace dvou stran podporuje komponenta Predix Machine správu certifikátů pro Secure Sockets Layer (SSL) spojení na služby technologie Predix Cloud. Mimo to je zde podpora bezpečnostních profilů, autentizace, správy identit a řízení přístupu pomocí dvou služeb orientovaných na bezpečnost, kterými jsou služba pro uživatelský účet a autentizace (anglicky „user account and authentication“) (UAA) a služba pro řízení přístupu (anglicky „UAA Service“ a „Access Control Service“).

Pomocí služby pro UAA, jsou schopny Predix aplikace identifikovat a autentizovat uživatele a to přímo, nebo pomocí standardů System for Cross-domain Identity Management (SCIM) pro správu identit a OAuth pro autentizaci. Kromě toho podporuje služba UAA také SAML, který umožňuje uživatelům se přihlašovat pomocí služeb třetích stran. Služba pro řízení přístupu v Predix (anglicky „Access Control Service“) je autorizační služba řízená pravidly. Tato služba umožňuje vytvořit pro aplikace přístupová omezení ke zdrojům na základě pravidel souvisejících se službou UAA. Jazyk pro popis těchto pravidel je založen na JavaScript Object Notation (JSON) a byl vyvinut jako odpověď na nedostatky v eXtensible Access Control Markup Language (XACML). [46]

Bezpečnostní prvky platformy Predix popsané výše se zaměřují na bezpečný přenos dat mezi komponentou Predix Machine a službami technologie *cloud computing* a na bezpečný přístup uživatelů ke službám. Neřeší bezpečnost infrastruktury služeb, např. bezpečnost a spolehlivost datových úložišť, což ale může být řešeno uvnitř použitou technologií Cloud Foundry. Technologie Cloud Foundry [25] může nabídnout izolaci virtuálních kontejnerů a jejich šifrování i vlastní službu UAA, která může být sdílena s Predix. Pokud však máme plný outsourcing jak technologie Cloud Foundry modelu PaaS/IaaS, tak platformy Predix modelu PaaS, ani zmiňované bezpečnostní prvky nemusí být dostačující pro zabezpečení dat v souladu se zavedenými bezpečnostními předpisy většiny průmyslových organizací.

Příležitosti

Následující příležitosti z kap. 2.2 mohou být řešeny použitím Predix:

O1 *Nízká počáteční investice* – Platforma Predix i v ní použitá technologie Cloud Foundry může být zprovozněna s minimálními náklady, až na případné investice do jednoúčelového HW pro komponenty Predix Machine, pokud není k dipozici již existující kompatibilní HW.

[50] `https://spark.apache.org/`

O2 *Outsourcing a management IT služeb* – Nasazení platformy Predix je jednoduché a platforma je založena na otevřené technologii Cloud Foundry, což usnadňuje případný outsourcing, je-li nezbytný. Je třeba poznamenat, že v případě provozu jako outsourcing, klasifikace podle CCM od Fóra Jericho může být jiná, než je popsáno výše, a mohou nastat další bezpečnostní problémy.

O3 *Složeniny* – V případě platformy Predix je jednoduché na vyžádání míchat a skládat různé služby této platformy, např. pro datové analýzy, jak bylo popsáno výše.

O5 *Škálovatelnost* – Služby technologie Predix modelu PaaS i použitá technologie Cloud Foundry modelu PaaS/IaaS jsou dobře škálovatelné.

O9 *Lepší monitorování (transparence)* – Predix silně podporuje sledování průmyslových zařízení, jejichž data jsou monitorována pomocí komponenty Predix Machine a odesílána službám Predix technologie *cloud computing* pro následné analýzy.

Jelikož je platforma Predix zaměřena na sledování a analýzy, nikoliv na všechny vlastnosti CMfg (viz kap. 2.1.2), pravděpodobně neumí řešit příležitosti O7 (připojené vozidlo) a O8 (agilní výroba), které mohou být zajímavé pro výrobní průmysl.

Hrozby

Následující hrozby dle kap. 2.2 jsou pomocí platformy Predix dobře řešitelné, nebo jsou opomenuty a je třeba je řešit:

T1 *Závislost a odevzdání se prodejci* – Díky použití otevřené technologie Cloud Foundry modelu PaaS/IaaS nehrozí na této úrovni odevzdání se prodejci. Přesto, na úrovni modelu PaaS je platforma Predix uzavřené proprietární řešení, kde by hrozba závislosti a odevzdání se prodejci měla být brána v potaz a řešena.

T3 *Závislost na datech, důvěrnost dat, sdílená pověst* – Tato hrozba je minimalizována vnitřním použitím otevřené technologie Cloud Foundry modelu PaaS/IaaS. Platforma Predix může být nasazena privátně a vlastními silami a provozována uvnitř organizace zákazníka.

T4 *Nepřenositelná odpovědnost* – Podobně, jako předchozí hrozba, také nepřenositelná odpovědnost není v případě platformy Predix problém.

T5 *Úzká místa datového přenosu* – Spojení komponenty Predix Machine na služby platformy Predix technologie *cloud computing* může být úzkým místem datového přenosu. Tento problém však může být řešen nasazením služby Predix Connectivity.

T6 *Nestabilita výkonu ve víceuživatelských prostředích* – Platforma Predix je používána pouze pro analýzy monitorovacích dat, nikoliv pro úlohy reálného (či téměř reálného) času, jako je PLC nebo VRC. Proto není nestabilita výkonu žádnou hrozbou.

Shrnutí

Díky dobré a flexibilní architektuře s mnoha předdefinovanými a přizpůsobitelnými komponentami a také díky využití otevřené technologie Cloud Foundry modelu PaaS/IaaS je platforma Predix velmi dobrým řešením pro sledování průmyslových zařízení a analýzu monitorovacích dat, zejména v kombinaci s dalšími jinými daty, např. pro strategický či obchodní management. Platforma Predix není vhodná pro důkladné uplatnění technologie CMfg, protože komponenta Predix Machine je primárně navržena pro sledování a nikoliv pro řízení připojených průmyslových zařízení.

3.2.4 Závěr

Přestože žádné z porovnávaných řešení nepodporuje plně koncept CMfg tak, jak byl zadefinován v kap. 2.1.2, mohou být úspěšně využity ve výrobním průmyslu pro sledování kritických výrobních zařízení, např. postupu v rámci výrobního procesu, opotřebení výrobních prostředků, či pro analýzu incidentů a optimalizaci výroby. Pro rychlé zpracování velkého množství dat generovaných zařízeními přináší použití služeb big data technologie *cloud computing* pro zpracování a analýzu dat výrazné úspory a schopnost dělat provozní a strategická rozhodnutí nad aktuálními daty. Taková funkcionalita zpracování a analýzy dat typu big data je (nebo bude) podporovaná všemi srovnávanými řešeními. Všechna tato řešení také umožňují privátní a veřejné nasazení, což je důležité pro minimalizaci rizik diskutovaných v kap. 2.2. V těchto aspektech jsou všechna tři srovnávaná řešení celkem zralá.

Přesto bychom z vybraných řešení technologie *cloud computing* pro výrobní průmysl v kap. 3.2 doporučili zvolit GE Predix, protože je to již zavedené řešení (ve srovnání s PTC Thingworx i Siemens MindSphere) s výbornou dokumentací. Navíc je toto řešení založené na otevřené technologii Cloud Foundry bez dalších proprietárních závislostí (na rozdíl od platformy Siemens MindSphere, která je založena na SAP HANA Cloud Platform a má minimální dokumentaci). Platforma Predix také disponuje prostředky pro flexibilní datové analýzy, kterými lze těsně integrovat SW pro zpracování dat typu big data a další služby technologie *cloud computing* (na rozdíl od PTC Thingworx i Siemens MindSphere).

Z dalších platforem technologie *cloud computing* z kap. 3.1 a podle souhrnných výsledků z tab. 3.1 je nejslibnější pro vývoj řešení konceptu CMfg platforma IBM BlueMix / Watson IoT Platform.

4 Manažerské shrnutí

Technologie *cloud computing* se snaží vyřešit dobře známé problémy systémů informační technologie (IT), jako je vysoká cena údržby a infrastruktury IT, nízká škálovatelnost a pružnost řešení, problematický outsourcing a další. Pro řešení těchto problémů používá technologie *cloud computing* progresivní přístupy, jako je uplatnění distribuovaných výpočtů, virtualizace, virtuální soukromé sítě atd. Kombinace těchto přístupů umožňuje vybudovat systémy technologie *cloud computing* s šesti charakteristickými rysy: vlastní obsluha na vyžádání, širokopásmové síťové připojení, sdílení prostředků, vysoká pružnost, měřitelné služby a souběh uživatelů (využitelnost pro více uživatelů). Systémy jsou implementovány v jednom ze třech modelů služeb podle toho, jaké komponenty IT (infrastruktura, platforma nebo software (SW)) jsou řešeny pomocí technologie *cloud computing*: infrastruktura-jako-služba (anglicky „Infrastructure as a Service“) (IaaS), platforma-jako-služba (anglicky „Platform as a Service“) (PaaS) a software-jako-služba (anglicky „Software as a Service“) (SaaS). Dále můžeme podle umístění hardware (HW) a SW, na kterém běží systém technologie *cloud computing*, rozlišit privátní, veřejné a hybridní nasazení, kdy jsou HW a SW vlastněny zákazníkem, poskytovatelem, nebo oběma. V praxi je bezpečnost použití technologie *cloud computing* výrazně ovlivněna různými kombinacemi těchto modelů služeb a druhy nasazení, společně s fyzickým umístěním technologií, jejich otevřeností, odpovědností za autentizaci a řízení přístupu, způsobem doručení služeb a dalšími.

Aktuální trendy v technologii *cloud computing* se snaží řešit vyšší požadavky na pružnost a škálovatelnost. V případě technologie *edge computing* využívá infrastruktura ve větší míře výpočetní zařízení na kraji sítě z pohledu poskytovatele služeb, tedy blíže zákazníka. Tato „edge“ zařízení jsou obvykle spravována (nebo rovnou vlastněna) zákazníkem v jeho umístění a mohou např. zpracovávat vstupní data předtím, něž jsou tato odeslána službám technologie *cloud computing*, spravovat citlivá data, která nemohou být vůbec odeslána takovým službám k uložení, nebo přímo poskytují některé ze služeb s vysokou spolehlivostí i v případě chybného a nestabilního připojení do sítě. V případě technologie *fog computing* poskytují tato zařízení vlastní služby ostatním zařízení a uživatelům (a to nejen „edge“) v síti, která se tak stane „mlžným oparem“ s různými službami technologie *cloud computing*. Technologie *edge computing* i *fog computing* často využívají zařízení konceptu internet věcí (anglicky „Internet of Things“) (IoT), např. pro monitorování a řízení průmyslových zařízení ve výrobě, což vede k novým modelům poskytování služeb, jako je robot-jako-služba (anglicky „Robot as a Service“) (RaaS). Kromě toho vyžaduje použití takových „edge“ zařízení, která sbírají nebo generují množství dat, také lepší zpracování a analýzy dat pomocí technologie *cloud computing*. Přístup big data pracuje s velkými objemy dat, zatímco fast data přístup se zaměřuje na rychlost datových proudů pro zpracování a analýzy dat v reálném (nebo skoro reálném) čase. V těchto případech implementuje technologie *cloud computing* modely služeb data-jako-služba (anglicky „Data as a Service“) (DaaS) nebo „Big Data ... as a Service“.

Technologie *cloud computing* může být využita ve výrobním průmyslu na dvou úrovních: (1) chytrá výroba s technologiemi *cloud computing* a (2) cloud manufacturing (CMfg). V prvním případě technologie *cloud computing* pouze pomáhá se zavedenými úlohami ve výrobní organizaci. Na příklad může chytrá výroba s technologiemi *cloud computing* zlepšit procesní řízení (anglicky „Business Process Management“) (BPM) a jiné business aplikace

nebo poskytnout prostředky pro migraci dat a vyvažování zátěže, virtualizaci, monitorování a big data analýzy, implementovat koncept virtuální továrna (anglicky „virtual factory“) (VF) nebo předvídání a řízení provozního stavu zařízení (anglicky „prognostics and health management“) (PHM). Na rozdíl od chytré výroby s technologiemi *cloud computing* využívá CMfg technologií *edge computing* a *fog computing* k rozšíření infrastruktury technologií *cloud computing* směrem k průmyslovým zařízením. Na příklad pro datové analýzy použije technologie *edge computing* zařízení konceptu IoT připojená k průmyslovým zařízení nejen pro čtení dat a jejich zasílání službám technologie *cloud computing*, ale také k vlastnímu vyhodnocení dat a k operacím s rychlou odezvou. V případe technologie *fog computing* nebude žádná viditelná hranice mezi středem a krajem řešení technologie *cloud computing* s bezešvou integrací služeb poskytovaných infrastrukturou ve středu a „edge“ zařízeními na kraji. Plně vybavená CMfg řešení jsou v současné době předmětem mnoha výzkumných projektů.

Abychom mohli analyzovat vhodnost technologie *cloud computing* pro výrobní průmysl automobilů a elektroniky, kategorizovali jsme řešení s technologií *cloud computing* a vyhodnotili, jak jsou (nebo nejsou) vhodná pro řešení nalezených příležitostí a hrozeb. Detailní výsledky tohoto srovnání jsou k dispozici v kap. 3 a tab. 3.1. Byla analyzována a srovnána následující řešení nabízející služby technologie *cloud computing* pro výrobní průmysl: AWS IoT (kap. 3.1.1); IBM BlueMix, Watson IoT (kap. 3.1.2); Microsoft Azure IoT (kap. 3.1.3); Google Cloud IoT (kap. 3.1.4); SAP Cloud Platform for IoT (kap. 3.1.5); Mnubo (kap. 3.1.6); PTC ThingWorx (kap. 3.2.1); Siemens MindSphere (kap. 3.2.2) a GE Predix (kap. 3.2.3).

Na základě konzultací s budoucími čtenáři této zprávy poslední tři z výše uvedených řešení byla analyzována podrobněji. Z těchto tří vybraných řešení služeb technologie *cloud computing* bychom doporučili zvolit General Electric (GE) Predix, protože je to zavedené řešení (na rozdíl od PTC Thingworx a Siemens MindSphere) s výbornou dokumentací a je založené na otevřené platformě Cloud Foundry bez dalších proprietárních závislostí (na rozdíl od Siemens MindSphere, která je založena na SAP HANA Cloud Platform). Navíc disponuje pružnou datovou analytikou, která může hladce integrovat SW pro zpracování big data a podobné služby technologie *cloud computing* (narozdíl od PTC Thingworx a Siemens MindSphere). Z dalších řešení s technologií *cloud computing* je nejvíce slibná pro možný vývoj CMfg platforma IBM BlueMix / Watson IoT Platform.

5 Závěr a doporučení

V této zprávě byl diskutován aktuální stav použití technologie *cloud computing* ve výrobním průmyslu. Po krátkém úvodu do terminologie technologie *cloud computing* a příslušných konceptů v kap. 1 byly diskutovány aktuální trendy aplikací technologie *cloud computing* ve výrobním průmyslu v kap. 2. Existující řešení pro takové aplikace byla analyzována a srovnána v kap. 3.

Technologie *cloud computing* přináší pro výrobní průmysl mnoho příležitostí, jak bylo popsáno v kap. 2.1. Nové systémy technologie *cloud computing* mohou být vytvořeny a zavedené systémy informační technologie (IT) mohou být převedeny na technologii *cloud computing*, aby čelily těmto výzvám. Avšak předtím, než organizace přijme konečné rozhodnutí o využití technologie *cloud computing*, zejména v případě převodu existujícího systému na technologii *cloud computing*, je nezbytné zvážit několik věcí. Výrobní organizace by měla zvážit, mimo jiné faktory, praktickou využitelnost technologie *cloud computing* a možné hrozby a bezpečnostní aspekty popsané v této zprávě. Mnoho z těchto faktorů bylo diskutováno v kap. 2. Z pohledu bezpečnosti IT bychom doporučili provést vyhodnocení bezpečnostních rizik dle Cloud Security Alliance (CSA) (viz kap. 2.3.2), přijmout příslušné modely pro řízení bezpečnosti a certifikace nebo je vyžadovat a ověřit jejich dodržování u poskytovatelů služeb technologie *cloud computing*, implementovat správu bezpečnosti informací a dat a používat otevřená řešení a technologie, které je snazší privátně nasadit a řídit jejich bezpečnost. Kromě toho musí být implementováno a vyžadováno dodržování běžných předpisů bezpečnosti IT, např. k ochraně lokální infrastruktury IT a zařízení přistupujících ke službám technologie *cloud computing*.

Ve srovnání existujících řešení pro aplikaci technologie *cloud computing* ve výrobním průmyslu byla, na základě konzultací s budoucími čtenáři této zprávy, vybrána pro podrobnější analýzu tři řešení s technologií *cloud computing*. Z těchto tří vybraných řešení bychom doporučili zvolit General Electric (GE) Predix, protože je to zavedené řešení s výbornou dokumentací a je založené na otevřené platformě Cloud Foundry bez dalších proprietárních závislostí, navíc s flexibilní datovou analytikou, která může hladce integrovat software (SW) pro zpracování dat typu big data a další služby. Z ostatních se jeví jako nejvíce slibné řešení pro případný vývoj cloud manufacturing (CMfg) platforma IBM BlueMix/Watson IoT Platform.

Přestože výše zmiňovaná řešení aplikace technologie *cloud computing* jsou dobrá, optimální řešení by bylo, alespoň z pohledu flexibility a bezpečnosti, následující: interní, privátně nasazené, otevřené, v perimetru a provozované jako insourcing (viz kap. 1.1.4). Avšak takové optimální řešení nyní nikdo neposkytuje a je nezbytné udělat kompromis mezi cenou a bezpečností: umístit systémy technologie *cloud computing* vně perimetru organizace u důvěryhodného poskytovatele, kde lze správně implementovat bezpečnostní prostředky; nasadit hybridně s umístěním a zpracováním citlivých dat na „edge“ zařízeních uvnitř perimetru organizace, kde lze prosadit bezpečnostní předpisy; a spravovat služby technologie *cloud computing* jako outsourcing u poskytovatele služeb nebo důvěryhodné třetí strany pro používání služeb bez dalších nákladů.

Literatura

[1] A. Freier, P. K., P. Karlton: The Secure Sockets Layer (SSL) Protocol Version 3.0. RFC 6101, Srpen 2011.
URL https://tools.ietf.org/html/rfc6101

[2] ABB: What is a smart grid? http://new.abb.com/smartgrids/what-is-a-smart-grid [cit. 16. srpna 2017], 2017.

[3] Adamson, G.; Wang, L.; Holm, M.; aj.: Cloud manufacturing – a critical review of recent development and future trends. *International Journal of Computer Integrated Manufacturing*, ročník 30, č. 4-5, 2017: s. 347–380, doi:10.1080/0951192X.2015.1031704.
URL http://dx.doi.org/10.1080/0951192X.2015.1031704

[4] Ali, M.; Khan, S. U.; Vasilakos, A. V.: Security in cloud computing: Opportunities and challenges. *Information Sciences*, ročník 305, 2015: s. 357–383, ISSN 0020-0255, doi:10.1016/j.ins.2015.01.025.
URL http://www.sciencedirect.com/science/article/pii/S0020025515000638

[5] Altintas, Y.: *Computer Numerical Control*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, ISBN 978-3-642-20617-7, s. 249–252, doi:10.1007/978-3-642-20617-7_6524.
URL https://doi.org/10.1007/978-3-642-20617-7_6524

[6] Amazon Web Services: AWS IoT. https://aws.amazon.com/iot-platform/how-it-works/ [cit. 3. července 2017], 2017.

[7] Amazon Web Services: What is AWS IoT? https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html [cit. 5. července 2017], 2017.

[8] Armbrust, M.; Fox, A.; Griffith, R.; aj.: A View of Cloud Computing. *Commun. ACM*, ročník 53, č. 4, Duben 2010: s. 50–58, ISSN 0001-0782, doi:10.1145/1721654.1721672.
URL http://doi.acm.org/10.1145/1721654.1721672

[9] Assunção, M. D.; Calheiros, R. N.; Bianchi, S.; aj.: Big Data computing and clouds: Trends and future directions. *Journal of Parallel and Distributed Computing*, ročník 79-80, 2015: s. 3–15, ISSN 0743-7315, doi:10.1016/j.jpdc.2014.08.003, special Issue on Scalable Systems for Big Data Management and Analytics.
URL http://www.sciencedirect.com/science/article/pii/S0743731514001452

[10] Atzori, L.; Iera, A.; Morabito, G.: The Internet of Things: A survey. *Computer Networks*, ročník 54, č. 15, 2010: s. 2787–2805, ISSN 1389-1286, doi:10.1016/j.comnet.2010.05.010.
URL http://www.sciencedirect.com/science/article/pii/S1389128610001568

[11] AXELOS: ITIL glossary and abbreviations English v.1.0. https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_GB-v1-0.pdf [cit. 16. srpna 2017], 2011.

[12] AXELOS: What is ITIL Best Practice? https://www.axelos.com/best-practice-solutions/itil/what-is-itil [cit. 16. srpna 2017], 2017.

[13] Baily, M.; Manyika, J.: Is manufacturing'cool'again. *McKinsey Global Institute*, Leden 2013.
URL http://www.mckinsey.com/mgi/overview/in-the-news/is-manufacturing-cool-again

[14] Balasubramanian, S.: Announcing Azure Stream Analytics on edge devices (preview). https://azure.microsoft.com/en-us/blog/announcing-azure-stream-analytics-on-edge-devices-preview/ [cit. 6. července 2017], Duben 2017.

[15] Barry, D. K.: Network as a Service (NaaS). http://www.service-architecture.com/articles/cloud-computing/network_as_a_service_naas.html [cit. 16. srpna 2017], 2017.

[16] Bhardwaj, S.; Jain, L.; Jain, S.: Cloud computing: A study of infrastructure as a service (IAAS). *International Journal of engineering and information Technology*, ročník 2, č. 1, 2010: s. 60–63, ISSN 0976-0253.

[17] Bloch, O.: Developer's introduction to Azure IoT. https://azure.microsoft.com/blog/developer-s-introduction-to-azure-iot/ [cit. 6. července 2017], Březen 2016.

[18] Bonomi, F.; Milito, R.; Zhu, J.; aj.: Fog Computing and Its Role in the Internet of Things. In *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, MCC '12, New York, NY, USA: ACM, 2012, ISBN 978-1-4503-1519-7, s. 13–16, doi:10.1145/2342509.2342513.
URL http://doi.acm.org/10.1145/2342509.2342513

[19] Booch, G.: The Accidental Architecture. *IEEE Software*, ročník 23, č. 3, Květen 2006: s. 9–11, ISSN 0740-7459, doi:10.1109/MS.2006.86.
URL http://dx.doi.org/10.1109/MS.2006.86

[20] Bray, T.; Paoli, J.; Sperberg-McQueen, C. M.; aj.: Extensible Markup Language (XML) 1.1 (Second Edition). W3c recommendation, W3C, 2006.
URL http://www.w3.org/TR/2006/REC-xml11-20060816

[21] Brodkin, J.: Gartner: Seven cloud-computing security risks. *Network World*, Červenec 2008.
URL http://www.networkworld.com/article/2281535/data-center/gartner--seven-cloud-computing-security-risks.html

[22] Chang, V.; Bacigalupo, D.; Wills, G.; aj.: A Categorisation of Cloud Computing Business Models. In *Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing*, CCGRID '10, Washington, DC, USA: IEEE Computer Society, 2010, ISBN 978-0-7695-4039-9, s. 509–512, doi:10.1109/CCGRID.2010.132.
URL http://dx.doi.org/10.1109/CCGRID.2010.132

[23] Chen, Y.; Du, Z.; García-Acosta, M.: Robot as a Service in Cloud Computing. In *2010 Fifth IEEE International Symposium on Service Oriented System Engineering*, Červen 2010, s. 151–158, doi:10.1109/SOSE.2010.44.
URL `http://dx.doi.org/10.1109/SOSE.2010.44`

[24] Chung, S. H.; Snyder, C. A.: ERP adoption: a technological evolution approach. *International Journal of Agile Management Systems*, ročník 2, č. 1, 2000: s. 24–32, doi:10.1108/14654650010312570.
URL `https://doi.org/10.1108/14654650010312570`

[25] Cloud Foundry Foundation: Cloud Foundry Documentation. `https://docs.cloudfoundry.org/` [cit. 29. června 2017], 2017.

[26] Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. Technická zpráva, Cloud Security Alliance, 2011.
URL `http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf`

[27] cloudSME: Simulation for manufacturing & engineering. `http://www.cloudsme-project.eu/` [cit. 12. června 2017], 2016.

[28] Cocchia, A.: *Smart and Digital City: A Systematic Literature Review*. Cham: Springer International Publishing, 2014, ISBN 978-3-319-06160-3, s. 13–43, doi:10.1007/978-3-319-06160-3_2.
URL `https://doi.org/10.1007/978-3-319-06160-3_2`

[29] H2020 CREMA project: Providing Cloud-based Rapid Elastic MAnufacturing based on the XaaS and Cloud model. `http://www.crema-project.eu/Cloud-Manufacturing/` [cit. 12. června 2017], 2015.

[30] Davis, A.; Parikh, J.; Weihl, W. E.: EdgeComputing: Extending Enterprise Applications to the Edge of the Internet. In *Proceedings of the 13th International World Wide Web Conference on Alternate Track Papers & Posters*, WWW Alt. '04, New York, NY, USA: ACM, 2004, ISBN 1-58113-912-8, s. 180–187, doi:10.1145/1013367.1013397.
URL `http://doi.acm.org/10.1145/1013367.1013397`

[31] Dayarathna, M.: Comparing 11 IoT Development Platforms. `https://dzone.com/articles/iot-software-platform-comparison` [cit. 3. července 2017], Únor 2016.

[32] Dean, J.; Ghemawat, S.: MapReduce: Simplified Data Processing on Large Clusters. *Commun. ACM*, ročník 51, č. 1, Leden 2008: s. 107–113, ISSN 0001-0782, doi:10.1145/1327452.1327492.
URL `http://doi.acm.org/10.1145/1327452.1327492`

[33] Diversity (Cloud Manufacturing and Social Software Based Context Sensitive Product-Service Engineering Environment for Globally Distributed Enterprise). `https://www.diversity-project.eu/` [cit. 12. června 2017], 2015.

[34] Emig, C.; Brandt, F.; Kreuzer, S.; aj.: *Identity as a Service – Towards a Service-Oriented Identity Management Architecture*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, ISBN 978-3-540-73530-4, s. 1–8, doi:10.1007/978-3-540-73530-4_1.
URL `https://doi.org/10.1007/978-3-540-73530-4_1`

[35] FDA: Radio Frequency Identification (RFID). https://www.fda.gov/RadiationEmittingProducts/RadiationSafety/ElectromagneticCompatibilityEMC/ucm116647.htm [cit. 16. srpna 2017], 2017.

[36] Fette, I.; Melnikov, A.: The WebSocket Protocol. RFC 6455, Prosinec 2011.
URL https://tools.ietf.org/html/rfc6455

[37] Fielding, R.; Reschke, J.: Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing. RFC 7230, Červen 2014.
URL https://tools.ietf.org/html/rfc7230

[38] Fielding, R. T.: *Architectural styles and the design of network-based software architectures*. Dizertační práce, University of California, Irvine, 2000.
URL http://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf

[39] Fingar, P.: Extreme Competition: Cloud Oriented Business Architecture. *Business Process Trends*, Červen 2009.
URL http://www.bptrends.com/publicationfiles/ONE%2006-09-COL-Extreme%20Competition-Cloud%20Oriented%20Arch-Fingar-final.pdf

[40] Foster, I.: What is the Grid? – a three point checklist. *GRIDtoday*, ročník 1, č. 6, Červenec 2002.
URL http://www-fp.mcs.anl.gov/~foster/Articles/WhatIsTheGrid.pdf

[41] Foster, I.; Zhao, Y.; Raicu, I.; aj.: Cloud Computing and Grid Computing 360-Degree Compared. In *2008 Grid Computing Environments Workshop*, Listopad 2008, ISSN 2152-1085, s. 1–10, doi:10.1109/GCE.2008.4738445.
URL http://dx.doi.org/10.1109/GCE.2008.4738445

[42] Furht, B.; Escalante, A.: *Handbook of Cloud Computing*. Springer Publishing Company, Incorporated, první vydání, 2010, ISBN 1441965238, 9781441965233, doi:10.1007/978-1-4419-6524-0.
URL http://dx.doi.org/10.1007/978-1-4419-6524-0

[43] Gantz, J.; Reinsel, D.: Extracting value from chaos. *IDC iview*, ročník 1142, č. 2011, 2011: s. 1–12.
URL https://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf

[44] Garcia Lopez, P.; Montresor, A.; Epema, D.; aj.: Edge-centric Computing: Vision and Challenges. *SIGCOMM Comput. Commun. Rev.*, ročník 45, č. 5, Září 2015: s. 37–42, ISSN 0146-4833, doi:10.1145/2831347.2831354.
URL http://doi.acm.org/10.1145/2831347.2831354

[45] Gartner: IT Glossary. https://www.gartner.com/it-glossary/ [cit. 16. srpna 2017], 2017.

[46] Predix Architecture and Services, updated 11/28/2016. Technická zpráva, General Electric Company, Listopad 2016.
URL https://d154rjc49kgakj.cloudfront.net/GE_Predix_Architecture_and_Services-20161128.pdf

[47] George, S.: Microsoft Azure IoT Edge – Extending cloud intelligence to edge devices. https://blogs.microsoft.com/iot/2017/05/10/microsoft-azure-iot-edge-extending-cloud-intelligence-to-edge-devices/ [cit. 6. července 2017], Květen 2017.

[48] GitLab.com Database Incident – 2017/01/31. https://docs.google.com/document/d/1GCK53YDcBWQveod9kfzW-VCxIABGiryG7_z_6jHdVik/pub [cit. 12. června 2017], Únor 2017.

[49] Glowik, M. W.; Mentuccia, L.; Tamietti, M.: A new era for the automotive industry: How cloud computing will enable automotive companies to change the game. https://www.accenture.com/t20150914T170053__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_18/Accenture-Cloud-Automative-PoV.pdf [cit. 12. června 2017], 2014.

[50] Google: Designing a Connected Vehicle Platform on Cloud IoT Core. https://cloud.google.com/solutions/designing-connected-vehicle-platform [cit. 7. července 2017], 2017.

[51] Google: Google Cloud IoT. https://cloud.google.com/solutions/iot/ [cit. 3. července 2017], 2017.

[52] Google: Overview of Internet of Things. https://cloud.google.com/solutions/iot-overview [cit. 7. července 2017], 2017.

[53] Hall, P.: Creative Cities and Economic Development. *Urban Studies*, ročník 37, č. 4, 2000: s. 639–649, doi:10.1080/00420980050003946.
URL http://dx.doi.org/10.1080/00420980050003946

[54] Hardt, D.: The OAuth 2.0 Authorization Framework. RFC 6749, Říjen 2012.
URL https://tools.ietf.org/html/rfc6749

[55] Heinrichs, W.: Design management - Do it anywhere. *Electronics Systems and Software*, ročník 3, č. 4, Srpen 2005: s. 30–33, ISSN 1479-8336, doi:10.1049/ess:20050405.
URL http://dx.doi.org/10.1049/ess:20050405

[56] Heiser, J.; Nicolett, M.: Assessing the Security Risks of Cloud Computing. Technická Zpráva G00157782, Gartner, Červen 2008.
URL https://www.gartner.com/doc/685308/assessing-security-risks-cloud-computing

[57] Hwang, K.; Li, D.: Trusted Cloud Computing with Secure Resources and Data Coloring. *IEEE Internet Computing*, ročník 14, č. 5, Září 2010: s. 14–22, ISSN 1089-7801, doi:10.1109/MIC.2010.86.
URL http://dx.doi.org/10.1109/MIC.2010.86

[58] IBM: The Architect's Guide to Bluemix Local. https://www.ibm.com/cloud-computing/bluemix/sites/default/files/assets/docs/the-architects-guide-to-bluemix-local_0_0.pdf [cit. 5. července 2017], 2017.

[59] IBM: Bluemix Docs / Internet of Things Platform. https://console.bluemix.net/docs/services/IoT/index.html [cit. 5. července 2017], 2017.

[60] IETF: SCIM: System for Cross-domain Identity Management. http://www.simplecloud.info/ [cit. 16. srpna 2017], 2017.

[61] Jain, S.; Choong, N. F.; Aye, K. M.; aj.: Virtual factory: an integrated approach to manufacturing systems modeling. *International Journal of Operations & Production Management*, ročník 21, č. 5/6, 2001: s. 594–608, doi:10.1108/01443570110390354.
URL https://doi.org/10.1108/01443570110390354

[62] Jain, S.; Shao, G.: Virtual Factory Revisited for Manufacturing Data Analytics. In *Proceedings of the 2014 Winter Simulation Conference*, WSC '14, Piscataway, NJ, USA: IEEE Press, 2014, s. 887–898.
URL http://dl.acm.org/citation.cfm?id=2693848.2693966

[63] Johnson, B.: Cloud computing is a trap, warns GNU founder Richard Stallman. *The Guardian*, Září 2008.
URL https://www.theguardian.com/technology/2008/sep/29/cloud.computing.richard.stallman

[64] JSON: Introducing JSON. http://json.org/ [cit. 16. srpna 2017], 2017.

[65] Kaazing: websocket.org. https://www.websocket.org/ [cit. 16. srpna 2017], 2017.

[66] Karnon, J.; Stahl, J.; Brennan, A.; aj.: Modeling Using Discrete Event Simulation. *Medical Decision Making*, ročník 32, č. 5, 2012: s. 701–711, doi:10.1177/0272989X12455462.
URL http://dx.doi.org/10.1177/0272989X12455462

[67] Kephart, J. O.; Chess, D. M.: The Vision of Autonomic Computing. *Computer*, ročník 36, č. 1, Leden 2003: s. 41–50, ISSN 0018-9162, doi:10.1109/MC.2003.1160055.
URL http://dx.doi.org/10.1109/MC.2003.1160055

[68] Kirkpatrick, K.: Software-defined Networking. *Commun. ACM*, ročník 56, č. 9, Září 2013: s. 16–19, ISSN 0001-0782, doi:10.1145/2500468.2500473.
URL http://doi.acm.org/10.1145/2500468.2500473

[69] Lam, W.; Liu, L.; Prasad, S.; aj.: Muppet: MapReduce-style Processing of Fast Data. *Proc. VLDB Endow.*, ročník 5, č. 12, Srpen 2012: s. 1814–1825, ISSN 2150-8097, doi:10.14778/2367502.2367520.
URL http://dx.doi.org/10.14778/2367502.2367520

[70] Lee, J.; Bagheri, B.; Kao, H.-A.: A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, ročník 3, 2015: s. 18–23, ISSN 2213-8463, doi:10.1016/j.mfglet.2014.12.001.
URL http://www.sciencedirect.com/science/article/pii/S221384631400025X

[71] Lee, J.; Lapira, E.; Bagheri, B.; aj.: Recent advances and trends in predictive manufacturing systems in Big Data environment. *Manufacturing Letters*, ročník 1, č. 1, 2013: s. 38–41, ISSN 2213-8463, doi:10.1016/j.mfglet.2013.09.005.
URL http://www.sciencedirect.com/science/article/pii/S2213846313000114

[72] Lom, M.; Pribyl, O.; Svitek, M.: Industry 4.0 as a part of smart cities. In *2016 Smart Cities Symposium Prague (SCSP)*, Květen 2016, s. 1–6, doi:10.1109/SCSP.2016.7501015.
URL http://dx.doi.org/10.1109/SCSP.2016.7501015

[73] Luan, T. H.; Gao, L.; Li, Z.; aj.: Fog Computing: Focusing on Mobile Users at the Edge. *CoRR*, ročník abs/1502.01815, 2015.
URL http://arxiv.org/abs/1502.01815

[74] Marston, S.; Li, Z.; Bandyopadhyay, S.; aj.: Cloud computing – The business perspective. *Decision Support Systems*, ročník 51, č. 1, 2011: s. 176–189, ISSN 0167-9236, doi:https://doi.org/10.1016/j.dss.2010.12.006.
URL http://www.sciencedirect.com/science/article/pii/S0167923610002393

[75] Mell, P. M.; Grance, T.: The NIST Definition of Cloud Computing. Technická Zpráva SP 800-145, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2011.
URL http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[76] Milenkovic, M.; Robinson, S. H.; Knauerhase, R. C.; aj.: Toward Internet Distributed Computing. *Computer*, ročník 36, č. 5, Květen 2003: s. 38–46, ISSN 0018-9162, doi:10.1109/MC.2003.1198235.
URL http://dx.doi.org/10.1109/MC.2003.1198235

[77] mnubo: Welcome to SmartObjects documentation! https://smartobjects.mnubo.com/apps/doc/ [cit. 7. července 2017], 2017.

[78] MODBUS: MODBUS Application Protocol Specification V1.1b3. Duben 2012.
URL http://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

[79] Monostori, L.: Cyber-physical Production Systems: Roots, Expectations and R&D Challenges. *Procedia CIRP*, ročník 17, 2014: s. 9–13, ISSN 2212-8271, doi:http://dx.doi.org/10.1016/j.procir.2014.03.115, variety Management in Manufacturing.
URL http://www.sciencedirect.com/science/article/pii/S2212827114003497

[80] Noble, A. P.; Kopaee, R.; Melek, A.; aj.: Data Leak Prevention. Technická zpráva, ISACA, Září 2010.
URL http://www.isaca.org/Groups/Professional-English/security-trend/GroupDocuments/DLP-WP-14Sept2010-Research.pdf

[81] eXtensible Access Control Markup Language (XACML) Version 2.0. Technická zpráva, OASIS, Únor 2005.
URL http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[82] MQTT Version 3.1.1. Technická zpráva, OASIS, Říjen 2014.
URL http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf

[83] OASIS: AMQP – Advanced Message Queuing Protocol. https://www.amqp.org/ [cit. 16. srpna 2017], 2017.

[84] OASIS: SAML XML.org. http://saml.xml.org/ [cit. 16. srpna 2017], 2017.

[85] OMG: Object Management Group – Business Process Model and Notation. http://www.bpmn.org/ [cit. 16. srpna 2017], 2017.

[86] OPC Foundation: Unified Architecture. https://opcfoundation.org/about/opc-technologies/opc-ua/ [cit. 16. srpna 2017], 2017.

[87] Jericho Forum Commandments, Version 1.2. Technická Zpráva W124, The Open Group Jericho Forum, 2007.
URL https://www2.opengroup.org/ogsys/catalog/W124

[88] Jericho Forum Cloud Cube Model, Version 1.0: Select Cloud Type for Secure Collaboration. Technická Zpráva W126, The Open Group Jericho Forum, 2009.
URL https://www2.opengroup.org/ogsys/catalog/W126

[89] OpenCrowd: Cloud Taxonomy. http://cloudtaxonomy.opencrowd.com/ [cit. 12. června 2017], Červen 2017.

[90] Pearson Education Limited: Longman Dictionary of Contemporary English Online. http://www.ldoceonline.com/ [cit. 16. srpna 2017], 2017.

[91] Postel, J.: Internet Protocol. RFC 791, Září 1981.
URL https://tools.ietf.org/html/rfc791

[92] Postel, J.; Reynolds, J. K.: File Transfer Protocol. RFC 959, Říjen 1985.
URL https://tools.ietf.org/html/rfc959

[93] Qiu, M.; Gao, W.; Chen, M.; aj.: Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System. *IEEE Transactions on Smart Grid*, ročník 2, č. 4, Prosinec 2011: s. 715–723, ISSN 1949-3053, doi:10.1109/TSG.2011.2160298.
URL http://dx.doi.org/10.1109/TSG.2011.2160298

[94] Qiu, M.; Su, H.; Chen, M.; aj.: Balance of security strength and energy for a PMU monitoring system in smart grid. *IEEE Communications Magazine*, ročník 50, č. 5, Květen 2012: s. 142–149, ISSN 0163-6804, doi:10.1109/MCOM.2012.6194395.
URL http://dx.doi.org/10.1109/MCOM.2012.6194395

[95] Rauschecker, U.; Meier, M.; Muckenhirn, R.; aj.: Cloud-based manufacturing-as-a-service environment for customized products. In *eChallenges e-2011 Conference Proceedings*, editace P. Cunningham; M. Cunningham, IIMC International Information Management Corporation, 2011.
URL http://strathprints.strath.ac.uk/38573/

[96] Rescorla, E.: HTTP Over TLS. RFC 2818, Květen 2000.
URL https://tools.ietf.org/html/rfc2818

[97] Rimal, B. P.; Jukan, A.; Katsaros, D.; aj.: Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. *Journal of Grid Computing*, ročník 9, č. 1, 2011: s. 3–26, ISSN 1572-9184, doi:10.1007/s10723-010-9171-y.
URL http://dx.doi.org/10.1007/s10723-010-9171-y

[98] Ross, J. W.; Westerman, G.: Preparing for utility computing: The role of IT architecture and relationship management. *IBM Systems Journal*, ročník 43, č. 1, 2004: s. 5–19, ISSN 0018-8670, doi:10.1147/sj.431.0005.
URL http://dx.doi.org/10.1147/sj.431.0005

[99] SAP: SAP Cloud Platform for the Internet of Things. https://www.sap.com/products/iot-platform-cloud.html [cit. 3. července 2017], 2017.

[100] SAP: SAP Cloud Platform Internet of Things Service. https://help.hana.ondemand.com/iot/frameset.htm [cit. 7. července 2017], 2017.

[101] SAP SE: Security in SAP Cloud Platform: Trust Matters. `https://assets.cdn.sap.com/sapcom/docs/2017/05/a470d0b2-b87c-0010-82c7-eda71af511fa.pdf`, Květen 2017.

[102] Schleifenbaum, H.; Uam, J.-Y.; Schuh, G.; aj.: Turbulence in Production Systems – Fluid Dynamics and its Contributions to Production Theory. In *Proceedings of the World Congress on Engineering and Computer Science*, ročník 2, San Francisco, USA, Říjen 2009, ISBN 978-988-18210-2-7.
URL `http://www.iaeng.org/publication/WCECS2009/WCECS2009_pp1140-1145.pdf`

[103] Schlick, J.: Cyber-physical systems in factory automation – Towards the 4th industrial revolution. In *2012 9th IEEE International Workshop on Factory Communication Systems*, Květen 2012, ISSN Pending, s. 55–55, doi:10.1109/WFCS.2012.6242540.
URL `http://dx.doi.org/10.1109/WFCS.2012.6242540`

[104] Sermersheim, J.: Lightweight Directory Access Protocol (LDAP): The Protocol. RFC 4511, Červen 2006.
URL `https://tools.ietf.org/html/rfc4511`

[105] MindSphere – Industry Mall. `https://mall.industry.siemens.com/mall/en/de/Catalog/Products/10011477` [cit. 2. července 2017], 2016.

[106] Siemens AG: MindSphere with MindConnect Nano and MindConnect IoT2040 – Getting Started. `https://support.industry.siemens.com/cs/document/109483499`, Březen 2017.

[107] Simon, D.; Espiau, B.; Castillo, E.; aj.: Computer-aided design of a generic robot controller handling reactivity and real-time control issues. *IEEE Transactions on Control Systems Technology*, ročník 1, č. 4, Prosinec 1993: s. 213–229, ISSN 1063-6536, doi:10.1109/87.260267.
URL `https://doi.org/10.1109/87.260267`

[108] Sustainable Manufacturing Adaptive Services with Cloud Architectures for Enterprises. `http://fp7smarter.eu/` [cit. 12. června 2017], 2017.

[109] Smith, M.: Workforce Performance Management: Efficiency and Effectiveness. *InformationWeek*, Listopad 2004, ISSN 8750-6874.
URL `http://www.informationweek.com/d/d-id/1028711`

[110] SPI: Open MPI: Open Source High Performance Computing. `https://www.open-mpi.org/` [cit. 16. srpna 2017], 2017.

[111] Stojmenovic, I.; Wen, S.; Huang, X.; aj.: An overview of Fog computing and its security issues. *Concurrency and Computation: Practice and Experience*, ročník 28, č. 10, 2016: s. 2991–3005, ISSN 1532-0634, doi:10.1002/cpe.3485.
URL `http://dx.doi.org/10.1002/cpe.3485`

[112] T. Dierks, E. R.: The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246, Srpen 2008.
URL `https://tools.ietf.org/html/rfc5246`

[113] ThingWorx: ThingWorx Studio. https://s3.amazonaws.com/tpg-thingworx/files/uploads/20161114135055/DS_thingworx-studio_J07272_EN.pdf [cit. 4. července 2017].

[114] Providing Secure Connected Products. https://www.thingworx.com/wp-content/uploads/2016/05/WP_thingworx_providing-secure-connected-products-whitepaper_J5194_EN.pdf [cit. 4. července 2017], Duben 2015.

[115] Securing the Internet of Things: Seven Steps to Minimize IoT Risk in the Cloud. https://www.ptc.com/-/media/Files/PDFs/Services/PTC_IoT_CloudSecurity_WP.ashx [cit. 4. července 2017], Leden 2016.

[116] Toll, W.: Top 49 Tools For The Internet of Things. https://blog.profitbricks.com/top-49-tools-internet-of-things/ [cit. 3. července 2017], Červenec 2014.

[117] Vakali, A.; Katsaros, D.; Stamos, K.; aj.: CDNs Content Outsourcing via Generalized Communities. *IEEE Transactions on Knowledge & Data Engineering*, ročník 21, 2008: s. 137–151, ISSN 1041-4347, doi:10.1109/TKDE.2008.92.
URL http://dx.doi.org/10.1109/TKDE.2008.92

[118] Vaquero, L. M.; Rodero-Merino, L.: Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing. *SIGCOMM Comput. Commun. Rev.*, ročník 44, č. 5, Říjen 2014: s. 27–32, ISSN 0146-4833, doi:10.1145/2677046.2677052.
URL http://doi.acm.org/10.1145/2677046.2677052

[119] Vasters, C.: Introduction to AMQP 1.0: AMQP Foundations. http://1drv.ms/1KVIJ1X [cit. 16. srpna 2017], Říjen 2015.

[120] Vichare, N. M.; Pecht, M. G.: Prognostics and health management of electronics. *IEEE Transactions on Components and Packaging Technologies*, ročník 29, č. 1, Březen 2006: s. 222–229, ISSN 1521-3331, doi:10.1109/TCAPT.2006.870387.
URL https://doi.org/10.1109/TCAPT.2006.870387

[121] Vick, A.; Horn, C.; Rudorfer, M.; aj.: Control of robots and machine tools with an extended factory cloud. In *2015 IEEE World Conference on Factory Communication Systems (WFCS)*, Květen 2015, s. 1–4, doi:10.1109/WFCS.2015.7160575.
URL http://dx.doi.org/10.1109/WFCS.2015.7160575

[122] Vu, Q. H.; Pham, T. V.; Truong, H. L.; aj.: DEMODS: A Description Model for Data-as-a-Service. In *2012 IEEE 26th International Conference on Advanced Information Networking and Applications*, Březen 2012, ISSN 1550-445X, s. 605–612, doi:10.1109/AINA.2012.91.
URL http://dx.doi.org/10.1109/AINA.2012.91

[123] Walter, K.: Final Report Summary – MANUCLOUD (Distributed Cloud product specification and supply chain manufacturing execution infrastructure). FP7-NMP Project Report Summary 260142, European Commission, Germany, 2014.
URL http://cordis.europa.eu/result/rcn/59193_en.html

[124] Weber, R. H.; Weber, R.: *Introduction*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, ISBN 978-3-642-11710-7, s. 1–22, doi:10.1007/978-3-642-11710-7_1.
URL https://doi.org/10.1007/978-3-642-11710-7_1

[125] Wu, J.; Ping, L.; Ge, X.; aj.: Cloud Storage as the Infrastructure of Cloud Computing. In *2010 International Conference on Intelligent Computing and Cognitive Informatics*, Červen 2010, s. 380–383, doi:10.1109/ICICCI.2010.119.

[126] Xu, X.: From cloud computing to cloud manufacturing. *Robotics and Computer-Integrated Manufacturing*, ročník 28, č. 1, 2012: s. 75–86, ISSN 0736-5845, doi:10.1016/j.rcim.2011.07.002.
URL `http://www.sciencedirect.com/science/article/pii/S0736584511000949`

[127] Youseff, L.; Butrico, M.; Silva, D. D.: Toward a Unified Ontology of Cloud Computing. In *2008 Grid Computing Environments Workshop*, Listopad 2008, ISSN 2152-1085, s. 1–10, doi:10.1109/GCE.2008.4738443.
URL `https://doi.org/10.1109/GCE.2008.4738443`

[128] Yusuf, Y.; Sarhadi, M.; Gunasekaran, A.: Agile manufacturing: The drivers, concepts and attributes. *International Journal of Production Economics*, ročník 62, č. 1-2, 1999: s. 33–43, ISSN 0925-5273, doi:10.1016/S0925-5273(98)00219-9.
URL `http://www.sciencedirect.com/science/article/pii/S0925527398002199`

[129] Zheng, Z.; Zhu, J.; Lyu, M. R.: Service-Generated Big Data and Big Data-as-a-Service: An Overview. In *2013 IEEE International Congress on Big Data*, Červen 2013, ISSN 2379-7703, s. 403–410, doi:10.1109/BigData.Congress.2013.60.
URL `http://dx.doi.org/10.1109/BigData.Congress.2013.60`

[130] Zima, M.; Larsson, M.; Korba, P.; aj.: Design Aspects for Wide-Area Monitoring and Control Systems. *Proceedings of the IEEE*, ročník 93, č. 5, Květen 2005: s. 980–996, ISSN 0018-9219, doi:10.1109/JPROC.2005.846336.
URL `https://doi.org/10.1109/JPROC.2005.846336`

Slovník

Advanced Message Queuing Protocol over TLS/SSL (AMQPS) Otevřený protokol pro předávání obchodních zpráv mezi různými IT aplikacemi nebo organizacemi zabezpečený pomocí Transport Layer Security (TLS)/Secure Sockets Layer (SSL). Protokol je popsaný ve standardu ISO/IEC 19464:2014 a definuje programové vybavení pro standardizovanou a spolehlivou výměnu obchodních zpráv mezi dvěma účastníky komunikace. Zprávy lze doručit různými způsoby včetně použití běžných zprostředkovatelů zasílání zpráv (účastníci komunikace mohou zprávy publikovat pod zvolenými kategoriemi a mohou se přihlásit k odběru publikovaných zpráv zvolených kategorií) a přímé výměny zpráv mezi dvěma účastníky (odesílatelé posílají zprávy jen vybraným adresátům). Protokol je vhodný pro těsnou integraci různých systémů, a to jak stávajících, tak nových aplikací, ale také databází a jiných sdílených zdrojů, včetně systémů a zdrojů technologie *cloud computing*. [83, 119]. 44, 79

aplikační programové rozhraní (anglicky „application programming interface“) (API) Počítačový kód, který umožňuje různým typům programového vybavení mezi sebou komunikovat a předávat si data. [90]. 15, 68, 79

architektura orientovaná na služby (anglicky „service-oriented architecture“) (SOA) Paradigma a disciplína návrhu programového vybavení pro soulad IT s obchodními potřebami. Jak si uvědomují některé organizace, přednostmi použití SOA jsou rychlejší uvedení produktu na trh, nižší náklady, lepší konzistence a flexibilita aplikací. SOA omezuje redundanci a zvyšuje použitelnost a hodnotu IT řešení. Díky SOA vznikají otevřené modulární systémy, které je snazší používat a udržovat. SOA také vytváří jednodušší a rychlejší systémy, které jsou pružnější a mají nižší náklady na údržbu. [45]. 82

big data Data, která lze charakterizovat pěti vlastnostmi: různorodost, rychlost, (velký) objem, věrohodnost a cena (v angličtině jsou tyto popisovány, jako pět V: variety, velocity, volume, veracity, value). Různorodost znamená různé typy dat, rychlost odkazuje na tempo vzniku a zpracování dat a (velký) objem upozorňuje na skutečnost, že se jedná o velmi obsáhlá data. Věrohodnost odkazuje na problematiku různé pravdivosti dat z různě důvěryhodných zdrojů, zatímco cena zdůrazňuje peněžní přínos správného zpracování big data pro společnosti. [9]. 15–17, 23, 28–30, 40–43, 45–47, 50, 54, 57, 59, 61, 63–65, 69, 71

Business Process Modelling Notation (BPMN) Grafické zobrazení posloupnosti dílčích kroků v podnikovém procesu od jeho začátku po jeho konec. Zobrazení bylo navrženo speciálně pro koordinaci sekvence procesů a zpráv zasílaných mezi různými účastníky procesů, kteří řeší příslušné aktivity procesů. Díky tomuto zobrazení mají podniky lepší schopnost porozumění svým vnitřním činnostem, možnost jejich grafického znázornění a standardizované dokumentace. Grafické znázornění procesů a jejich souvislostí podporuje také lepší porozumění spolupráce mezi podniky. Podniky pak porozumí nejen sami sobě, ale také účastníkům jejich procesů, což umožní rychlé přizpůsobení novým okolnostem uvnitř podniku i mezi podnikem a jeho partnery. [85]. 59, 79

cloud computing Styl uplatnění výpočetní techniky, kde jsou škálovatelná a elastická IT řešení poskytována uživatelům jako služba prostřednictvím technologií Internet. Je to distribuovaný koncept použití výpočetní techniky na vyžádání, který se snaží vyřešit časté problémy systémů IT, jako jsou vysoké náklady na údržbu a cena infrastruktury IT, nízká škálovatelnost a pružnost, problematický outsourcing a další. [45]. 1–5, 7–17, 19–21, 23, 25, 27–34, 36, 39–49, 51–61, 63–65, 67–72, 74, 76–78

Cloud Cube Model (CCM) Model navržený během Fóra Jericho, který definuje kritéria pro odlišení čtyř různých způsobů realizace a poskytování služeb technologie *cloud computing*. Cílem modelu je umožnit bezpečnou spolupráci poskytovatelů služeb a podniků dle jejich požadavků pomocí technologie *cloud computing*. Model odlišuje několik typů použití technologie *cloud computing* a popisuje rysy každého z těchto typů tak, aby byl srozumitelný a bylo možné se správně rozhodnout, je-li nejvhodnější dle skutečných potřeb podniku. U každého typu model zdůrazňuje jeho klíčové vlastnosti a radí klíčové otázky, které by měl případný uživatel služby technologie *cloud computing* daného typu položit svému poskytovateli této technologie, aby by se ujistil, že je řešení bezpečné a ve shodě s relevantními předpisy. Technologie *cloud computing* je zde popsána jako prostředí vně perimetru organizace uživatele, bez žádných hranic. Ačkoliv privátní nasazení technologie *cloud computing* mohou, v případě potřeby, omezit přístup ke svým aplikacím a jejich datům mimo organizaci uživatele, skutečná geografická poloha umístění těchto aplikací a dat je i zde většinou neznámá. Jedná se tedy skutečně o prostředí bez hranic vyžadující přísné zabezpečení informací dle kritérií stanovených přesněji v rámci Fóra Jericho. [88, 87]. 6, 40, 79

cloud manufacturing (CMfg) Model umožňující na vyžádání všudypřítomný a pohodlný přístup ke skupině sdílených výrobních zdrojů přes počítačovou síť (např. k počítačovému vybavení pro výrobu, výrobnímu vybavení a konkrétním strojům). Tyto sdílené výrobní zdroje pak mohou být rychle použity a poté uvolněny s minimálním úsilím a interakcí s poskytovatelem služeb. Sdílené a distribuované zdroje jsou zapouzdřeny do služeb technologie *cloud computing* a spravovány centrálně. Klienti pak používají jednotlivé služby podle svých potřeb. Uživatelé technologie *cloud computing* mohou takto používat různé služby pro návrh, výrobu, testování, správu a všechny další fáze životního cyklu výrobku. [126]. 19, 26, 39, 63, 65, 79

data-jako-služba (anglicky „Data as a Service“) (DaaS) Typ služby technologie *cloud computing* poskytující na vyžádání data. Taková služba typicky předává data zákazníkům přes aplikační programové rozhraní (anglicky „application programming interface“) (API), kde si tito mohou data stáhnout nebo se dotázat na data vyhovující různým kritériím. Díky těmto službám nemusí zákazníci stahovat a uchovávat velké datové sady a sami je prohledávat pro získání požadovaných informací, ale jednoduše vyhledají odpovídající službu, která požadovaná data nabízí, a zavolají příslušné API, pomocí kterého data získají. [122]. 15, 28, 40, 63, 80

dispečerské řízení a sběr dat (anglicky „Supervisory Control and Data Acquisition“) (SCADA) Systém používaný ve výrobě pro příjem měření procesních proměnných a stavů výrobních zařízení a pro výkon omezení nebo řízení těchto zařízení ve výrobě nebo její části. [45]. 13, 82

dohoda o úrovni služeb (anglicky „Service Level Agreement“) (SLA) Smlouva mezi poskytovatelem a spotřebitelem (uživatelem) služby, která popisuje IT službu, dokumentuje její cílové úrovně a určuje zodpovědnosti poskytovatele IT

služby a jejího spotřebitele. Jedna taková smlouva může pokrýt více IT služeb nebo být pro více spotřebitelů. [11]. 56, 82

eXtensible Access Control Markup Language (XACML) Jeden ze základních Extensible Markup Language (XML) standardů skupiny OASIS pro popis pravidel autentizace a řízení systému oprávnění, který slouží jako společný jazyk pro vyjádření bezpečnostních předpisů. Po implementaci v podniku tento společný jazyk umožní řídit prosazování všech prvků bezpečnostních předpisů ve všech komponentách jeho informačních systémů. Správa bezpečnostních předpisů může zahrnovat některé či všechny z následujících kroků: zápis, revize, testování, schválení, vydání, kombinace, analýza, modifikace, stažení, poskytnutí a vynucení předpisů. [81]. 59, 83

Extensible Markup Language (XML) Značkovací jazyk pro textové dokumenty s formátem snadno čitelným pro lidi i stroje. Jazyk, který byl původně navržen pro potřeby rozsáhlého elektronického publikování, hraje nyní důležitou roli při výměně různých dat přes web a jinde. XML dokumenty jsou tvořeny jednotkami uložení dat zvanými entity, které obsahují jak strukturovaná, tak nestrukturovaná data. Strukturovaná data se skládají ze znaků, které tvoří textová data a formátovací značky. Značky popisují strukturu dokumentu ve smyslu struktury jeho uložení i logické struktury. XML poskytuje, v případě potřeby, mechanismus pro omezení takové struktury dokumentu. [20]. 68, 83

fast data Jedná se o big data s důrazem na rychlost, např. vysokorychlostní datové proudy přitékající v reálném (či téměř reálném) čase. Typické příklady fast data jsou proudy senzorových dat, data akciových trhů v reálné čase a výstupy ze sociálních sítí. Fast data musí být často zpracovávána s minimálním zpožděním a velkou škálovatelností. [69]. 54, 58, 59, 63

File Transfer Protocol (FTP) Síťový aplikační protokol pro přenos souborů mezi klientem a serverem v počítačové síti. Cílem protokolu je podpořit sdílení souborů (počítačových programů či dat) a nepřímé nebo implicitní (prostřednictvím programů) použití vzdálených počítačů, a to tak, aby byl uživatel odstíněn od různých charakteristik souborových systémů jednotlivých poskytovatelů dat a byl mu umožněn spolehlivý a efektivní přenos dat. Přestože je protokol přímo použitelný z počítačového terminálu, je navržen hlavně pro využití v počítačových programech. [92]. 58, 80

grid computing Metoda použití velkého množství zdrojů, obvykle výpočetní kapacity, na jednotlivou (neinteraktivní) úlohu tím, že se použijí zdroje více než jednoho výpočetního systému. Grid je pak koordinovaná kolekce takových zdrojů uzpůsobená pro řešení běžných problémů. Výpočetní grid propojuje více počítačů různých vlastníků tak, aby na nich bylo možné řešit složité aplikační problémy. [45]. 2, 10

Hypertext Transfer Protocol (HTTP) Bezstavový síťový aplikační protokol typu dotaz-odpověď, který používá rozšiřitelnou sémantiku a samostatné datové rámce pro flexibilní interakci s hypertextovými informačními systémy přes počítačovou síť. Protokol je navržen obecně pro informační systémy, a to tak, aby skryl implementační detaily služeb za jednotné rozhraní poskytované jejich klientům nezávisle na typu zdrojů, ke kterým se přistupuje. Také server služby nemusí zajímat, proč klient chce daná data, a každý HTTP požadavek je obsloužen samostatně, bez spojení s konkrétním typem klienta nebo posloupností jeho předchozích aktivit.

Výsledný protokol je dobře použitelný v mnoha různých kontextech a jeho implementace se během času samostatně vyvíjely. HTTP je také navržen jako čistý přenosový protokol komunikace mezi ne-HTTP informačními systémy. HTTP proxy servery a brány mohou poskytovat přístup k alternativním informačním službám tím, že překládají různé protokoly na HTTP a umožňují tak klientům komunikovat se službami stejným způsobem, jako by to byly HTTP služby. [37]. 43, 69, 80

Hypertext Transfer Protocol over Transport Layer Security (HTTPS) Bezpečný bezstavový síťový aplikační protokol typu dotaz-odpověď, který používá rozšiřitelnou sémantiku a samostatné datové rámce pro flexibilní interakci s hypertextovými informačními systémy přes počítačovou síť. Protokol spočívá v komunikaci přes Hypertext Transfer Protocol (HTTP) se zabezpečením síťového spojení pomocí TLS. [96, 37]. 46, 80

identifikace na rádiové frekvenci (anglicky „Radio-frequency Identification“) (RFID) Bezdrátový systém skládající se ze dvou komponent: čteček a tzv. tagů. Čtečka je zařízení s jednou nebo více anténami, které vyzařují rádiové vlny a přijímají zpět signály z RFID tagů. Tyto tagy využívají zmiňované rádiové vlny pro zaslání informací o své identitě (a jiných) blízkým čtečkám. Tagy mohou být aktivní nebo pasivní. Pasivní tagy jsou napájeny rádiovými vlnami ze čteček a nemají vlastní baterie, na rozdíl od aktivních tagů, které jsou napájeny vlastními bateriemi. RFID tagy mohou uchovávat různé informace od jednoho sériového čísla pro identifikaci až po několik stran textu. Čtečky mohou být mobilní, takže je lze přenášet v ruce, nebo mohou být zabudované na určitých místech či nad nimi. Systémy čteček mohou být také zabudovány do nábytku, místnosti či stavby. [35]. 82

identita-jako-služba (anglicky „Identity as a Service“) (IdaaS) Služba technologie *cloud computing* poskytující funkce pro ověření (a správu) identit a oprávnění. Služba umožňuje ověřit oprávnění uživatele pro aplikaci (např. pro jinou službu technologie *cloud computing*) za běhu pomocí vlastní implementace řízení přístupu. Toto je založeno na dvou předpokladech. Nejprve musí být autentizační proces zahrnující předání přístupových údajů přenesen na službu, tedy uživatel zde komunikuje přímo s IdaaS službou, bez zapojení aplikace. Poté musí proběhnout proces ověření přístupových oprávnění, což je provedeno přímou komunikací aplikace s IdaaS službou, bez účasti uživatele. Funkcionalita obou částí (autentizace i ověření oprávnění) je, stejně jako správa identit, zapouzdřena do IdaaS služby a zpřístupněna aplikacím, uživatelů a ostatním službám technologie *cloud computing*. [34]. 5, 80

informační technologie (IT) Studium nebo použití elektronických procesů ke získání a uchování informací a jejich zpřístupnění pomocí počítačů. [90]. 43, 63, 65, 81

infrastruktura-jako-služba (anglicky „Infrastructure as a Service“) (IaaS) Doručení hardware (serverů, úložiště či sítě) a souvisejícího software (virtualizovaných operačních systémů, souborových systémů) jako služby. Vzniklo evolucí z tradičního hostování serverů bez žádných dlouhodobých závazků tak, že uživatelé mohou používat zdroje kdykoliv na vyžádání. Na rozdíl od služeb modelu platforma-jako-služba (anglicky „Platform as a Service“) (PaaS), poskytovatel IaaS služeb neprovádí prakticky žádné další činnosti nad rámec provozu svého datového centra. Uživatelé si pak musí sami nasadit a spravovat softwarové služby stejným způsobem, jako by byly provozovány v jejich vlastních datových centrech. [16]. 3, 5, 19, 39, 63, 71, 80

Internet Protocol (IP) Nízkoúrovňový komunikační protokol pro posílání datových

zpráv přes počítačovou síť (či sítě). Protokol přenáší bloky dat zvané datagramy mezi zdroji a cíli identifikovanými IP adresami pevné délky. Protokol také poskytuje prostředky pro rozdělení a opětovné sestavení dlouhých datagramů, pokud je to potřeba při přenosu sítěmi vyžadujícími menší dávky dat. [91]. 77, 81

internet věcí (anglicky „Internet of Things“) (IoT) Nově vznikající informační architektura pro výměnu zboží a služeb na síti Internet. Cílem je poskytovat infrastrukturu IT bezpečným a spolehlivým předáváním tzv. věcí, tj. překonat mezeru mezi objekty fyzického světa a jejich reprezentacemi v informačních systémech. Slouží také ke zvýšení transparentnosti a větší efektivnosti globálních sítí dodavatelů. [124]. 12, 23, 41, 63, 71, 80

IT Infrastructure Library (ITIL) Široce uznávaný přístup ke správě služeb IT, který je popsán souborem zavedených praktik, mezinárodně uznávaných soukromými i veřejnými organizacemi. ITIL prohlašuje, že služby IT odpovídají potřebám podniků a podporují jejich procesy. Poskytuje organizacím a jednotlivcům návod, jak používat IT jako nástroj k dosažení změny, transformaci nebo růstu podniků. ITIL odpovídá 11. části standardu ISO 20000, která popisuje způsob použití ITIL pro splnění požadavků certifikace ISO 20000 a jeho nezávislost. Zavedené praktiky ITIL jsou podpořeny certifikačním schématem, které umožňuje účastníkům prokázat jejich schopnosti při přijmutí a přizpůsobení IT rámců jejich specifickým potřebám. [12]. 81

JavaScript Object Notation (JSON) Jednoduchý textový formát pro výměnu dat, který je lehce čitelný i zapisovatelný pro lidi a lehce zpracovatelný i generovaný pro stroje. Formát vychází z podmnožiny programovacího jazyka JavaScript, avšak je nezávislý a používá zvyklosti známé programátorům jazyků příbuzných programovacímu jazyku C, vč. vlastního jazyka C a jazyků C++, C#, Java, JavaScript, Perl, Python a dalších. Díky tomuto je JSON ideální jazyk pro výměnu dat. JSON je postaven na dvou strukturách: na kolekci dvojic jméno/hodnota a na seřazeném seznamu hodnot. První z nich je v programovacích jazycích často realizován jako objekt, záznam, struktura, slovník, hash tabulka, klíčovaný seznam nebo asociativní pole. Druhý pak bývá realizován jako pole, vektor, seznam nebo sekvence. Jedná se o univerzální struktury, které podporují prakticky všechny programovací jazyky. Proto dává smysl, že univerzální formát pro výměnu dat, jako je JSON, je bude také podporovat. [64]. 59, 81

klíčový ukazatel výkonnosti (anglicky „key performance indicator“) (KPI) Vysokoúrovňová metrika výstupu systému, dopravy či jiných, která je zjednodušena pro týdenní, měsíční či čtvrtletní sběr a vyhodnocení. Typické příklady jsou kvalita síťového připojení, počet transakcí za sekundu, či počet hovorů na uživatele. KPI jsou často kombinovány s nákladovými metrikami (např. cena jedné transakce či uživatele) tak, aby vznikl klíčový systém operačních metrik. [45]. 14, 40, 81

kvalita služby (anglicky „quality of service“) (QoS) Uzavřená smlouva, jako je dohoda o úrovni služeb (anglicky „Service Level Agreement“) (SLA), mezi uživatelem a poskytovatelem služby, která zajišťuje určitý výkon poskytované služby (např. spolehlivě dostupnou kapacitu síťového připojení ve sdílené sítí, poskytovaného jako služba určitým poskytovatelem). [45]. 82

kyberfyzikální výrobní systém (anglicky „cyber-physical production system“) (CPPS) Systém spolupracujících výpočetních komponent, které jsou významně propojeny s okolním fyzickým světem v oblasti výroby a výrobních procesů a které souběžně používají výpočetní služby pro přístup k datům a jejich zpracování. Ta-

kové systémy se skládají z autonomních a spolupracujících prvků a subsystémů, které se propojují dle aktuálních potřeb na jednotlivých úrovních výroby i mezi nimi, od výrobních procesů, přes výrobní stroje, až po výrobní a logistické sítě. [79]. 13, 79

Lightweight Directory Access Protocol (LDAP) Jedná se o protokol pro přístup k adresářům pro distribuované adresářové služby. Adresář je zde tedy kolekce otevřených systémů spolupracujících za účelem poskytnutí adresářových služeb. Uživatel adresáře, což může být člověk nebo jiná entita, přistupuje k adresáři přes klientskou aplikaci, která provádí za uživatele dotazy na jeden či více serverů pomocí protokolu pro přístup k adresářům, jako je LDAP. [104]. 50, 81

MapReduce Programovací model a jeho implementace pro zpracování a generování big data, který je schopen pokrýt různé úlohy reálného světa. Uživatelé zadají výpočet pomocí funkcí map a reduce a běhový systém poté výpočet automaticky provede paralelně na rozsáhlých výpočetních clusterech, kde je systém schopen také ošetřit případné chybové stavy a rozvrhnout komunikaci mezi stroji tak, aby byly síť i disková úložiště jednotlivých strojů využity efektivně. [32]. 16

Message Queue Telemetry Transport (MQTT) Standard ISO/IEC PRF 20922 definující jednoduchý protokol komunikace stroje se strojem (anglicky „machine-to-machine“) (M2M), který implementuje komunikační model poskytovatel-odběratel (anglicky publisher-subscriber) a je postaven na TCP/IP protokolu. Protokol je jednoduchý, otevřený, nenáročný na zdroje a jednoduše implementovatelný. Díky těmto vlastnostem je protokol ideální pro mnoho případů užití, včetně použití v prostředích s určitými omezeními, např. pro komunikace v M2M a internet věcí (anglicky „Internet of Things“) (IoT), kde je nezbytné mít nízkou režii a přenos dat. Protokol běží nad sítí TCP/IP nebo libovolnou jinou, která umožňuje obousměrnou, bezeztrátovou komunikaci se zachováním pořadí zpráv. Mezi charakteristické vlastnosti standardu patří: použití vzoru komunikace publikuj/odebírej (angl. publish/subscribe) pro rozesílání zpráv z jednoho zdroje mnoha příjemcům a pro volnější provázanost komunikující stran; přenos zpráv nezávislý na jejich obsahu; přenos zpráv v různé (volitelné) kvalitě; malá režie a nízký objem dat přenášených na síti; mechanismus upozornění komunikující stran v případě náhlého nevysvětleného odpojení jedné z nich. [82]. 41, 81

Modbus Aplikační protokol pro zasílání zpráv, který poskytuje klient-server komunikaci zařízení připojených různými typy sběrnic či sítí. Jedná se o protokol typu dotaz-odpověď, který nabízí služby pod kódovým označením funkcí. Tyto kódy funkcí jsou části datových jednotek protokolu Modbus, které odesílá klient na server společně s dalšími informacemi. Tyto informace pak server použije k provedení příslušných akcí definovaných danými kódy funkcí. [78]. 44

model SPI (SPI) Tři základní rozdělení služeb technologie *cloud computing* jsou často označovány jako model SPI, kde SPI je zkratka pro software-jako-služba (anglicky „Software as a Service“) (SaaS), PaaS a infrastruktura-jako-služba (anglicky „Infrastructure as a Service“) (IaaS). [26]. 5, 82

Navrhni a vyrob kdekoliv (anglicky „Design Anywhere, Manufacture Anywhere“) (DAMA) Výrobní filosofie umožňující podnikům v případě potřeby rychle přesunout návrh výrobků a vlastní výrobu jinam, tak, aby reagovaly na změnu trhu a byly flexibilní v možnostech návrh či výrobu rozšířit nebo smluvně zajistit dle cyklu poptávky, či přidat nová návrhová střediska a továrny, které bude

lehké integrovat do celkového podnikového procesu. Tento přístup vyžaduje schopnost rychlého předávání informací o návrhu výrobků mezi pracovišti a také sladění návrhových nástrojů, komponent a výroby. [55]. 19, 80

OAuth Otevřený protokol pro bezpečnou autentizaci jednoduchou a standardizovanou metodou z webových, mobilních i desktopových aplikací. Protokol umožňuje aplikaci třetí strany získat omezený přístup k určité službě, a to jménem majitele zdroje (koncového uživatele) tím, že je zajištěno vyjednání přístupu mezi majitelem (uživatelem) a službou, nebo přímo jménem aplikace, která službu sama použije. [54]. 46, 47, 59

OPC Unified Architecture (OPC-UA) Platformě nezávislá servisně orientovaná architektura, která integruje všechnu funkcionalitu jednotlivých specifikací architektury OPC Classic do jednoho rozšiřitelného rámce. Narozdíl od OPC Classic, která byla založena na technologii Microsoft Windows s využitím modelu Distributed Component Object Model pro výměnu dat mezi komponentami programového vybavení, OPC UA je nezávislá na platformě a dostupná pro různý hardware a operační systémy (tradiční PC hardware, ale také servery technologie *cloud computing*, programovatelný logický automat (anglicky „programmable logic controller“) (PLC), mikrokontroléry a další, kde běží Microsoft Windows, Apple OSX, Android či libovolné distribuce systému Linux a jiné). OPC UA je funkčně shodná s OPC Classic, ale nabízí více možností. Architektura je kompatibilní se zabezpečením typu firewall a přidává zabezpečení řízením bezpečného přenosu, šifrování a podepisování zpráv, číslováním zpráv pro prevenci útoku přehráním zachycených zpráv, autentizace, správy uživatelů a auditu. [86]. 44, 81

Open MPI Otevřený standard rozhraní pro předávání zpráv mezi počítačovými programy (MPI znamená „message passing interface“, tedy rozhraní pro předávání zpráv), který je vyvíjen konsorciem akademických, výzkumných i průmyslových partnerů za účelem vysokorychlostního distribuovaného a paralelního počítání. Je to standardizované API typicky používané pro paralelní a distribuované výpočty. [110]. 2

platforma-jako-služba (anglicky „Platform as a Service“) (PaaS) Služba technologie *cloud computing* pro vrstvu prostředí programového vybavení (neboli softwarovou platformu). Uživatelé této vrstvy jsou vývojáři aplikací technologie *cloud computing*, kteří tyto aplikace vyvíjí a nasazují do prostředí technologie *cloud computing*. Poskytovatelé takových služeb nabízejí zmiňovaným vývojářům prostředí programovacího jazyka zahrnující dobře dokumentovaná API pro interakci aplikací s prostředím, snadnější vývoj a lepší škálovatelnost vyvíjených aplikací. [127]. 3, 5, 19, 39, 63, 70, 81

plánování podnikových zdrojů (anglicky „enterprise resource planning“) (ERP) Schopnost poskytovat integrovanou sadu podnikových aplikací. Nástroje plánování podnikových zdrojů sdílí společný procesní a datový model, který zahrnuje širokou škálu a hierarchii operační procesů pokrývajících na příklad finance, lidské zdroje, distribuci, výrobu, služby a dodávky. [45]. 13, 19, 80

plánování potřeby výrobních zdrojů (anglicky „manufacturing resource/requirements planning“) (MRP) Integrace informačních a výrobních technologií, plánů a zdrojů ke zlepšení efektivnosti výrobního podniku. Na rozdíl od předchozích přístupů ke plánování potřeby materiálu, zde se neplánuje jen materiál a části výroby, ale také postupy a rozvrhy výroby. Předpokládá se, že veškeré časové údaje jsou deterministické (např. časy výroby). Napojení

aktivit, jako je zpracování objednávek, řízení skladu a obchodování, je plánováno a rozvrhováno odděleně, jednoduchým získáváním, uchováváním a výměnou příslušných dat v systému dle potřeby. [24]. 19, 81

počítačové číslicové řízení (anglicky „computer numeric control“) (CNC) Počítačové řízení výrobních jednotek pomocí skupin mechanických pohonů, elektrických nebo elektro-hydraulických servomotorů, zesilovačů, senzorů polohy a rychlosti a dalších. Řízení je prováděno specializovaným počítačem s operačním systémem pro práci v reálném čase. [5]. 13, 79

prevence ztráty dat (anglicky „data loss prevention“) (DLP) Sada technologií pro zamezení ztráty citlivých dat vlastněných podniky. Řešení se zaměřuje na umístění, klasifikaci a monitorování dat při jejich uložení, použití i předávání a pomáhá podnikům spravovat jejich informace a zastavit každodenní únik dat. Prevence ztráty dat není jednoduše použitelné řešení, ale jeho úspěšná implementace vyžaduje náležitou přípravu a pečlivé průběžné provádění. Organizace, které chtějí implementovat prevenci ztráty dat, by měly být připraveny na usilovnou práci, která však významně omezí rizika, pokud bude provedena pořádně. Je nezbytné zvolit strategický přístup, který se zaměří na zmiňovaná rizika, jejich dopad a způsob prevence, společně se způsobem jejich řízení a měření. [80]. 35, 80

procesní řízení (anglicky „Business Process Management“) (BPM) Obor, kde se používají různé metody k odhalení, modelování, analýze, měření, zlepšování a obecně k optimalizaci podnikových procesů. Podnikové procesy zde koordinují chování lidí, systémů, informací a jiných prostředků k dožení podnikových cílů ve shodě s podnikovou strategií. Procesy mohou být strukturované a opakovatelné, nebo nestrukturované a nestálé. Přestože to není pravidlem, BPM bývá často podpořen pokročilými technologiemi. Je zde klíčové sladit investice do IT a výrobních technologií společně s podnikovou strategií. [45]. 19, 21, 63, 79

programovatelný logický automat (anglicky „programmable logic controller“) (PLC) Jedná se o základní stavební kámen průmyslové a procesní automatizace, kterým je speciální počítač se vstupními a výstupními zařízeními a komunikací po sériové lince, který provádí řídící programy, zejména řízení logicky provázaných posloupností operací. Programovatelný logický automat může být zabudován výrobcem ve stroji nebo procesním vybavení, může být samostatnou lokální jednotkou v řídícím prostředí, nebo připojen do systému po síti. [45]. 13, 39, 72, 81

předvídání a řízení provozního stavu zařízení (anglicky „prognostics and health management“) (PHM) Metoda umožňující určení aktuální spolehlivosti systému na základě jeho životních podmínek (zdraví atp.) a detekci blížícího se selhání, a tak snižující riziko. Problematika předvídání a řízení provozního stavu zařízení je již dobře známá v případě kritických mechanických systémů a struktur, včetně vědeckých postupů pro určení příznaků blížících se selhání (jako jsou např. změny vybrací ložisek a změny hluku v důsledku opotřebení) a algoritmů pro odvozování důsledků. V případě elektronických systémů, narozdíl od mechanických systémů a struktur, je však situace jiná, protože je težší detekovat a vyšetřit degradaci elektronických součástek a spojů. Důvodem je také menší měřítko elektroniky na úrovní mikro- a nano-metrů a složitá architektura většiny elektronických zařízení. [120]. 23, 24, 64, 81

Representational State Transfer (REST) Vrstvený architektonický styl typu klient-server pro webové zdroje, který je často používaný webovými službami pro přístup ke zdrojům pomocí jednotného rozhraní, bezstavových operací a s mezi-pamětí (cache). Styl REST je abstrakcí prvků architektury pro distribuované systémy

hypermédií, kde jsou všechna data zapouzdřena ve zdrojích a skryta ve zpracovávajících komponentách. Tyto REST komponenty komunikují přenosem reprezentace zdroje dat ve formátu odpovídajícím nějakému standardnímu datovému typu, vždy dle schopností a požadavků příjemce dat a povahy zdroje. Zdrojem může být jakákoliv informace, např. dokument nebo obrázek, dočasná služba, kolekce jiných zdrojů, nevirtuální objekt (např. osoba) atd. Skutečnost, je-li reprezentace zdroje ve stejném nebo jiném formátu než je zdroj, zůstává příjemci skryta za definovaným rozhraním. [38]. 43, 76, 82

robot-jako-služba (anglicky „Robot as a Service“) (RaaS) Služba technologie *cloud computing* poskytující na vyžádání přístup, sledování a řízení robotů, kteří jsou tímto způsobem zapojeni do této technologie a stávají se její součástí. Robot je mechanický nebo virtuální a umělý zástupce, který svou přítomností a pohyby jedná dle svých smyslů a záměrů. Podle RaaS by měl být robot schopen vystupovat jako poskytovatel služby. Klient může na robota umístit nové služby, které pak může robot využívat a které mohou být také sdíleny s ostatními roboty a zakomponovány do aplikací využívajících služby uvnitř i vně robota. Robot by měl být navíc schopen jednat jako distributor takových služeb i jako jejich spotřebitel. Takový spotřebitel, ať už robot nebo externí spotřebitel, pak může vyhledávat a používat služby a aplikace umístěné na jiných robotech. [23]. 14, 39, 63, 82

rozšířená realita (anglicky „augmented reality“) (AR) Případ, kdy jsou informace, obrázky a jiné počítačem generované výstupy slučovány s informacemi ze skutečného světa, jako jsou přímá zobrazení skutečných věcí. [90]. 48, 79

řídící jednotka robota (anglicky „robot controller“) (RC) Zdroje počítačového a programového vybavení podílející se na on-line řízení skupiny splupracujících zařízení (jako jsou roboti a senzory), které souvisejí s řídícími systémy. [107]. 14, 78, 82

řízení vztahů se zákazníky (anglicky „customer relationship management“) (CRM) Obchodní strategie pro optimalizaci příjmu a výnosu zvyšováním spokojenosti a loajálnosti zákazníka. CRM technologie podporují strategii a identifikují a spravují vztahy se zákazníky, osobní nebo virtuální. Programové vybavení pro CRM podporuje zejména čtyři oblasti podniku: obchod, marketing, zákaznickou podporu a elektronické obchodování. [45]. 19, 80

Secure Sockets Layer (SSL) Bezpečnostní protokol pro důvěrnou komunikaci přes Internet. Protokol umožňuje aplikacím typu klient-server komunikovat způsobem, který je odolný proti odposlechu, narušení a podvržení zpráv. Protokol se používá ke zapouzdření jiných protokolů vyšší úrovně. Jedním z takových zapouzdřených protokolů je SSL protokol pro seznámení komunikujících stran, který umožňuje stranám se navzájem autentizovat a domluvit se na kryptografickém algoritmu a klíčích šifrované komunikace ještě předtím, než začne aplikace posílat nějaká data. Jedna z výhod SSL je skutečnost, že je nezávislý na zapouzdřeném aplikačním protokolu a vysokoúrovňové protokoly mohou využívat SSL transparentně. Bezpečné spojení přes SSL má tři základní vlastnosti: spojení je soukromé (po počátečním seznámení je použito šifrování pro definici tajného klíče, kterým jsou pak symetricky zašifrována přenášená data), strana klienta se může autentizovat (použitím asymetrické kryptografie či veřejným klíčem) a spojení je spolehlivé (přenášení zprávy jsou opatřeny kontrolním součtem, který jsou schopny obě strany ověřit). Protokol je předchůdcem protokolu TLS. [1]. 59, 67, 82

Security Assertion Markup Language (SAML) Rámec založený na XML pro tvorbu a on-line výměnu bezpečnostních informací, např. pro autentizaci uživatelů, je-

jich oprávnění a dalších bezpečnostních atributů. SAML umožňuje obchodním entitám stanovit podmínky zabezpečení týkající se identit, vlastností a oprávnění subjektů (často lidských) jiných entit, jako jsou partnerské organizace či další podnikové aplikace. Před vznikem SAML zde nebyl žádný XML standard pro výměnu bezpečnostních informací mezi bezpečnostními systémy (jako je např. systém autentizační autority) a aplikacemi důvěřujícími těmto systémům. SAML poskytuje standardizovanou XML reprezentaci pro specifikaci takových informací a definuje cesty pro jejich výměnu a získání. [84]. 46, 82

simulace diskrétních událostí (anglicky „discrete event simulation“) (DES) Způsob počítačového modelování pro intuitivní a flexibilní reprezentaci komplexních systémů sekvencí výskytů časově navazujících událostí. Simulace diskrétních událostí vznikla v 60. letech 19. století ve inženýrském a operačním výzkumu pro analýzu a vylepšování průmyslových a podnikových procesů. Termín diskrétní značí skutečnost, že se simulace diskrétních událostí posouvá v čase v diskrétních úsecích (tedy, že model přechází z času jedné události do času události další) a že jsou události diskrétní (navzájem výlučné). Díky těmto skutečnostem je simulace diskrétních událostí flexibilní a dobře použitelná na celou řadu problémů. Klíčovými prvky simulace diskrétních událostí jsou entity, atributy, události, zdroje, fronty a čas. Entity jsou objekty, které během času mají atributy, zažívají události, konzumují zdroje a vstupují do front. Atributy jsou vlastnosti specifické pro každou z entit, které jí dovolují přenášet informace. Události jsou obecně definovány jako věci, které se mohou stát entitě či jejímu prostředí. Zdroje jsou objekty, které entitě poskytují služby. Pokud je zdroj obsazený a entita ho zrovna potřebuje, tato musí počkat a zařadí se do fronty. Vnější hodiny pak měří čas simulace od jejího počátku. [66]. 24, 80

sledování aktivit nad databází a soubory (anglicky „database and file activity monitoring“) (DAM/FAM) Sada nástrojů, které podporují schopnost zjistit a hlásit podvodné, ilegální či jinak nevhodné chování, a to při minimálním odpadu na činnost a produktivitu uživatelů. Tyto nástroje se vyvinuly z běžných analytických nástrojů uživatelských aktivit v relačních databázích (a souborových systémech), aby poskytly širší funkce, jako je odhalení a klasifikace incidentů, správu zranitelností, analýzu na úrovni aplikací, prevenci průniku, podporu pro zabezpečení nestrukturovaných dat, správu identit a řízení přístupu, či správu rizik. [45]. 35, 80

sledování podnikových aktivit (anglicky „business activity monitoring“) (BAM) Procesy a technologie, které pomáhají s porozuměním a umožňují analýzu kritických podnikových ukazatelů výkonnosti založených na reálných datech. Tyto procesy a technologie jsou používané ke zrychlení a zefektivnění podnikových aktivit, kdy umožňují sledovat průběh aktivit a detekovat případné nedostatky. Tento přístup může být podporován různými výpočetními nástroji, přičemž ty z nich, které jsou zaměřeny výhradně na BAM, se nazývají BAM platformy. [45]. 21, 79

smart city Město, které monitoruje a integruje stav všech svých kritických infrastruktur, včetně silnic, mostů, tunelů, železnic, metra, letišť, přístavů, komunikační infrastruktury, vodovodu, energetických sítí, ale také důležitých budov. Sledování a zpracování stavu se provádí za účelem optimalizace využití zdrojů, plánování aktivit preventivní údržby a sledování bezpečnostních aspektů během maximálního využití služeb občany města. [53, 28]. 12

smart grid Systém elektrické distribuční sítě, který řídí dodávku elektřiny trvale udržitelným, spolehlivým a ekonomicky výhodným způsobem. Systém je vystavěn na

pokročilé infrastruktuře a optimalizován pro integraci všech zúčastněných komponent sítě. Systém ovládá kapacitu přidělenou na základě poptávky a pomáhá vyvažovat spotřebu elektřiny a její dodávku. Navíc představuje systém potenciál pro integraci nových technologií, které umožňují zapojit zařízení pro uchovávání elektrické energie a automobily na elektrický pohon. [2]. 12, 36, 37

software-jako-služba (anglicky „Software as a Service“) (SaaS) Model služeb technologie *cloud computing*, kde jsou aplikace umístěné na výpočetní infrastruktuře poskytovatele (na rozdíl od umístění na počítačích zákazníka) a vývojáři aplikací jsou schopni aplikovat malé opravy a nasazovat nové funkce bez potřeby rušit uživatele žádostmi o instalaci aktualizací. Konfigurace a testování takových aplikací je snazší, jelikož je prostředí jejich provozu známé (jedná se o datové centrum poskytovatele). Model umožňuje poskytovateli nabízet službu s určitým ziskem a poskytuje mu stálý příjem, přičemž zisk může být při dlouhodobém pohledu poměrně vysoký. [127]. 3, 4, 19, 39, 63, 71, 82

softwarově definovaná síť (anglicky „software-defined network“) (SDN) Nově vznikající síťová architektura, která odděluje řídící a datovou vrstvu při použití síťových zařízení. Tímto může být řídící vrstva sítě centralizovaná a síťová infrastruktura pod datovou vrstvou může být abstrahována od aplikací (tzn. jedná se o virtuální síťovou infrastrukturu). [45]. 12, 82

správa digitálních práv (anglicky „digital rights management“) (DRM) Důvěrné předávání digitálních informací přes síť Internet, kde je uživatel oprávněn provést s informacemi pouze takové činnosti, které povolí jejich odesílatel. [45]. 35, 80

správa pracovních výkonů (anglicky „workforce performance management“) (WPM) Soubor praktik pro automatizaci a zlepšení procesů a výkonu zaměstnanců v organizaci, a tedy pro automatizaci a zvýšení efektivnosti pracovních procesů. Jeho cílem je optimalizovat výkonnostní úrovně a kompetence v organizaci tím, že jsou zaměstnanci lépe přiřazeni k pracovním procesům a je zvýšena jejich výkonnost a zisk. Správa pracovních výkonů vyžaduje nebo je vyžadována správou náboru zaměstnanců, správou kompenzací, pobídek, cílů, vzdělávání, kompetencí, měřením výkonnosti a dalšími. [109]. 21, 83

Storage Area Network (SAN) Dedikovaná počítačová síť skládající se ze dvou vrstev. První vrstva zajišťuje propojení uzlů úložišť v počítačové síti a přenos příkazů a stavových hlášení dle typů připojených zařízení. Do této vrstvy musí být připojeno alespoň jedno zařízení. Druhá je vrstva programového vybavení, která poskytuje užitečné služby pracující nad první vrstvou, jako je vzdálený nízkoúrovňový přístup k úložištím (na úrovni datových bloků). [45]. 82

System for Cross-domain Identity Management (SCIM) Standard IETF, vytvořený pro jednoduchou správu uživatelů v technologii *cloud computing*, definující schéma pro reprezentaci uživatelů a jejich skupin a API, které využívá architektonický styl Representational State Transfer (REST), pro příslušné operace jejich tvorby, změn a mazání. [60]. 59, 82

systém pro sledování rozsáhlých oblastí (anglicky „wide-area monitoring system“) (WAMS) Systém pro sledování zařízení v rozsáhlé oblasti, např. systém sledování stavu elektrické distribuční sítě, kde operátoři průběžně analyzují stav sítě v reálném čase. Jedná se o tzv. systém synchronního měření fázorů s vyhodnocením stability sítě a algoritmy pro její stabilizaci. Systém poskytuje časově synchronní informace o měření fázorů s údaji o napětí a proudu v elektrické síti a to každých 20 ms (při střídavém proudu frekvence 50 Hz). Každý datový vzorek je vybaven časovým razítkem a synchronizován s největší přesností. [130]. 36, 83

série velikosti jedna Výroba, kde každá část finálního výrobku prochází výrobním procesem samostatně, takže výroba může být rozdělena a je flexibilní v modifikacích jednotlivých svých částí (což je nezbytnou podmínkou pro „výrobu na vyžádání“, kde procesy musí být často překonfigurovány dle aktuálních požadavků). [102]. 13

síť pro doručování obsahu (anglicky „content distribution network“) (CDN) Počítačová síť v síti Internet, která poskytuje škálovatelný a nákladově úsporný způsob urychlení doručení webového obsahu uživatelům. Síť se skládá ze skupiny náhradních serverů v různých geografických lokacích, směrovačů a dalších síťových prvků. Náhradní servery jsou klíčovými prvky, které fungují jako proxy servery poskytující obsah klientům původních služeb přímo z vyrovnávací paměti serverů. Servery uschovávají ve vyrovnávací paměti identický obsah, jako původní služby, takže jsou lokálně schopni uspokojit požadavky klientů mířící na původní globální služby. Požadavek klienta na webový obsah ze serveru původní služby poskytovatele obsahu v CDN je zachycen a nasměrován na nejvhodnější náhradní server. Tím je zvýšena jak rychlost odezvy na požadavek klienta (protože je požadovaný obsah doručen ze serveru blízkého klientovi), tak celková prostupnost systému (protože je zátěž rozdělena mezi více serverů). [117]. 21, 79

síť-jako-služba (anglicky „Network as a Service“) (NaaS) Služba technologie *cloud computing* poskytující na vyžádání virtualizovanou síťovou infrastrukturu. Takovou službou může být flexibilní a rozšířená virtuální privátní síť (anglicky „virtual private network“) (VPN), síťové připojení na vyžádání, speciální směrování síťového provozu, připojení typu multicast, bezpečný firewall, detekce útoků a jejich prevence, rozsáhlá síť, monitorování a filtrování obsahu či antivirová ochrana. Přesná obecná definice obsahu NaaS služeb neexistuje a také implementace jsou různé. [15]. 5, 81

Transport Layer Security (TLS) Bezpečnostní protokol pro důvěrnost a integritu dat mezi dvěma komunikujícími aplikacemi. Protokol se skládá ze dvou vrstev: protokolu pro TLS záznam a protokolu pro TLS seznámení. Na nižší úrovni, nad nějakým transportním protokolem, je protokol pro TLS záznam, který zabezpečuje spojení tak, aby bylo soukromé a spolehlivé. Protokol pro TLS záznam je použit pro zapouzdření různých protokolů vyšší úrovně, jako je protokol pro TLS seznámení, který umožňuje komunikujícím stranám (klient a server) se navzájem autentizovat a domluvit se na kryptografickém algoritmu a klíčích šifrované komunikace ještě předtím, než začne aplikace posílat nějaká data. Protokol TLS se vivinul z protokolu SSL. [112]. 46, 67, 83

úložiště-jako-služba (anglicky „Storage as a Service“) (StaaS) Model služby, který umožňuje uživatelům uložit jejich data na vzdálených discích a mít tato data dostupná kdykoliv a kdekoliv. Systémy úložišť by měly splňovat několik vlastností pro správu uživatelských dat a informací, včetně vysoké dostupnosti, spolehlivosti, výkonnosti, replikace a datové konzistentnosti. Avšak vzhledem ke vzájemně konfliktní povaze těchto vlastností, žádný systém je neimplementuje všechny. [125]. 5, 22, 82

virtuální privátní síť (anglicky „virtual private network“) (VPN) Systém pro poskytování podnikově zaměřených komunikačních služeb na veřejné sdílené síťové infrastruktuře, který poskytuje podnikový síťový provoz jednotným a univerzálním způsobem v rámci celého podniku. Pojem VPN se používá obecně pro označení podnikových hlasových sítí, proto, aby se zabránilo nedorozumění, datové služby

založené na protokolu Internet Protocol (IP) jsou označovány jako datové VPN. Poskytovatelé VPN služeb definují tyto jako rozsáhlé sítě stálých virtuálních spojení, obecně používajících asynchronní přenos dat nebo přenos rámců pro protokol IP. Poskytovatelé VPN technologií pak definují VPN jako použití programového a počítačového vybavení pro šifrování za účelem soukromé komunikace přes veřejné nebo nedůvěryhodné datové sítě. [45]. 2, 77, 83

virtuální programovatelný logický automat (anglicky „virtual programmable logic controller“) (VPLC) Virtuální PLC, který řídí daný výrobní proces stejným způsobem, jako fyzický PLC. Takový virtualizovaný PLC může být na příklad implementován integrací několika softwarových PLC ve stroji schopném práce v reálném čase. [121]. 14, 83

virtuální továrna (anglicky „virtual factory“) (VF) Integrovaný simulační model hlavních systémů továrny, který zahrnuje celou továrnu a poskytuje podporu pro rozhodování v rámci továrny. Model umožňuje napodobovat skutečné operace v továrně a může sloužit pro testování postupů přetím, než se provádějí ve skutečné továrně. [61]. 23, 64, 83

virtuální řídící jednotka robota (anglicky „virtual robot controller“) (VRC) Virtuální řídící jednotka robota (anglicky „robot controller“) (RC), která monitoruje a řídí roboty stejným způsobem, jako fyzická RC. Virtualizovaný RC může být na příklad implementován integrací několika softwarových RC ve stroji schopném práce v reálném čase. VRC může být nasazen jako služba technologie *cloud computing*, přestože některé funkce RC je nezbytné ponechat mimo tuto technologii a blízko řízenému stroji tak, aby byla, díky kratším komunikačním spojením, zachována schopnost práce v reálné čase. [121]. 14, 39, 83

výroba-jako-služba (anglicky „Manufacturing as a Service“) (MaaS) Jedná se o paradigma služeb technologie *cloud computing* pro novou generaci konfigurovatelných výrobních systémů. Na rozdíl od jiných běžných přístupů ke přizpůsobení výroby (např. prostým přeprogramování jednotlivých strojů, aby produkovaly požadované výrobky), systémy tohoto paradigma jsou schopny se přizpůsobit pro výrobu technicky složitých výrobků tím, že se dynamicky překonfiguruje celý výrobní postup vč. napojení dodavatelů. Aby bylo možno vytvořit takové systémy, musí být zdroje (tedy výrobní prostředky) navrženy tak, aby podporovaly vzájemnou spolupráci přes výrobní síť, včetně schopnosti přizpůsobit se specifikům konkrétní výroby. Flexibilní kompozice výrobních služeb a zapojení příslušných IT služeb pro realizaci výrobních služeb probíhají podobně, jako v případě jiných modelů služeb technologie *cloud computing*. [95]. 25, 40, 81

výrobní informační systém (anglicky „manufacturing execution system“) (MES) Systém, který spravuje, monitoruje a synchronizuje v reálném čase spouštění fyzických procesů účastnících se transformace materiálů do polotovarů či hotových výrobků. Takové systémy koordinují provádění pracovních příkazů s plánováním výroby a jinými podnikovými informačními systémy. Nasazení výrobních informačních systémů zpřístupňuje informace o výkonu procesů, pohybu podpůrných komponent a materiálu, jejich návaznosti a souvislosti s procesní historií, je-li to potřeba. [45]. 13, 81

WebSocket Komunikační protokol navržený pro existující infrastrukturu webu. WebSocket spojení začínají vždy jako HTTP spojení a garantují tak plnou zpětnou kompatibilitu s komunikací účastníků, kteří dosud WebSocket nepodporují. Protokol umožňuje navázat plně duplexní a obousměrný komunikační kanál, který funguje na jediném přípojném místě (tzv. socket) přes Web mezi prohlížečem klienta

a vzdáleným strojem. Takto protokol umožňuje obousměrnou komunikaci mezi klientem, kde běží nedůvěryhodný kód v omezeném prostředí, a vzdáleným strojem, který je z takového kódu volán. Použitý bezpečnostní model vychází z běžného bezpečnostního modelu webových prohlížečů. Cílem je poskytnout mechanismus pro aplikace běžících na webových prohlížečích, které vyžadují rychlou a spolehlivou obousměrnou komunikaci se serverem. [65, 36]. 46

Zkratky

AEP Application Enablement Platform. 49

AMQPS Advanced Message Queuing Protocol over TLS/SSL. 44, *viz slovník:* Advanced Message Queuing Protocol over TLS/SSL (AMQPS)

API aplikační programové rozhraní (anglicky „application programming interface“). 13, 15, 43, 47, 68, 72, 76, *viz slovník:* aplikační programové rozhraní (anglicky „application programming interface“) (API)

AR rozšířená realita (anglicky „augmented reality“). 48–50, 52, *viz slovník:* rozšířená realita (anglicky „augmented reality“) (AR)

AWS Amazon Web Services. iii, 41–43, 48, 49, 64

BAM sledování podnikových aktivit (anglicky „business activity monitoring“). 21, 23, *viz slovník:* sledování podnikových aktivit (anglicky „business activity monitoring“) (BAM)

BLOB velký binární objekt (anglicky „binary large object“). 58, 59

BPM procesní řízení (anglicky „Business Process Management“). 19, 21, 23, 63, *viz slovník:* procesní řízení (anglicky „Business Process Management“) (BPM)

BPMN Business Process Modelling Notation. 59, *viz slovník:* Business Process Modelling Notation (BPMN)

CAD počítačem podporované projektování (anglicky „computer-aided design“). 52

CCM Cloud Cube Model. 6–8, 40, 41, 43–47, 49, 54, 58, 60, *viz slovník:* Cloud Cube Model (CCM)

CDN síť pro doručování obsahu (anglicky „content distribution network“). 21, 22, *viz slovník:* síť pro doručování obsahu (anglicky „content distribution network“) (CDN)

CMfg cloud manufacturing. 19, 20, 25–27, 29, 36, 37, 39–41, 43, 54, 56, 57, 60, 61, 63–65, *viz slovník:* cloud manufacturing (CMfg)

CNC počítačové číslicové řízení (anglicky „computer numeric control“). 13, *viz slovník:* počítačové číslicové řízení (anglicky „computer numeric control“) (CNC)

CPPS kyberfyzikální výrobní systém (anglicky „cyber-physical production system“). 13, *viz slovník:* kyberfyzikální výrobní systém (anglicky „cyber-physical production system“) (CPPS)

CPU centrální procesorová jednotka (anglicky „central processing unit“). 22, 31, 45

CRM řízení vztahů se zákazníky (anglicky „customer relationship management“). 19, 21, 29, *viz slovník:* řízení vztahů se zákazníky (anglicky „customer relationship management“) (CRM)

CSA Cloud Security Alliance. iii, 33, 35, 65

DaaS data-jako-služba (anglicky „Data as a Service“). 15, 28, 29, 40, 63, *viz slovník:* data-jako-služba (anglicky „Data as a Service“) (DaaS)

DAM/FAM sledování aktivit nad databází a soubory (anglicky „database and file activity monitoring“). 35, *viz slovník:* sledování aktivit nad databází a soubory (anglicky „database and file activity monitoring“) (DAM/FAM)

DAMA Navrhni a vyrob kdekoliv (anglicky „Design Anywhere, Manufacture Anywhere“). 19, 20, *viz slovník:* Navrhni a vyrob kdekoliv (anglicky „Design Anywhere, Manufacture Anywhere“) (DAMA)

DES simulace diskrétních událostí (anglicky „discrete event simulation“). 24, *viz slovník:* simulace diskrétních událostí (anglicky „discrete event simulation“) (DES)

DLP prevence ztráty dat (anglicky „data loss prevention“). 35, *viz slovník:* prevence ztráty dat (anglicky „data loss prevention“) (DLP)

DRM správa digitálních práv (anglicky „digital rights management“). 35, *viz slovník:* správa digitálních práv (anglicky „digital rights management“) (DRM)

ERP plánování podnikových zdrojů (anglicky „enterprise resource planning“). 13, 19, 21, 27, 28, *viz slovník:* plánování podnikových zdrojů (anglicky „enterprise resource planning“) (ERP)

FTP File Transfer Protocol. 58, *viz slovník:* File Transfer Protocol (FTP)

GE General Electric. iii, 42, 48, 57, 58, 61, 64, 65

HIPAA Health Insurance Portability and Accountability Act. 35

HTTP Hypertext Transfer Protocol. 23, 43, 46, 58, 69, 78, *viz slovník:* Hypertext Transfer Protocol (HTTP)

HTTPS Hypertext Transfer Protocol over Transport Layer Security. 46, 47, 50, 55, *viz slovník:* Hypertext Transfer Protocol over Transport Layer Security (HTTPS)

HW hardware. 1, 29, 31, 45, 46, 54–56, 59, 63

IaaS infrastruktura-jako-služba (anglicky „Infrastructure as a Service“). 3, 5, 8, 16, 17, 19–23, 31, 32, 34, 35, 39, 55, 57–60, 63, 71, *viz slovník:* infrastruktura-jako-služba (anglicky „Infrastructure as a Service“) (IaaS)

IdaaS identita-jako-služba (anglicky „Identity as a Service“). 5, *viz slovník:* identita-jako-služba (anglicky „Identity as a Service“) (IdaaS)

IoT internet věcí (anglicky „Internet of Things“). iii, 12, 13, 17, 23, 41–52, 54, 58, 61, 63–65, 71, *viz slovník:* internet věcí (anglicky „Internet of Things“) (IoT)

IP Internet Protocol. 7, 21, 31, 77, *viz slovník:* Internet Protocol (IP)

IT informační technologie. 1, 2, 7, 10, 17, 19, 27–32, 43, 50, 51, 55, 58, 60, 63, 65, 67, 68, 70, 73, 78, *viz slovník:* informační technologie (IT)

ITIL IT Infrastructure Library. 28, *viz slovník:* IT Infrastructure Library (ITIL)

JSON JavaScript Object Notation. 59, *viz slovník:* JavaScript Object Notation (JSON)

KPI klíčový ukazatel výkonnosti (anglicky „key performance indicator“). 14, 30, 40, *viz slovník:* klíčový ukazatel výkonnosti (anglicky „key performance indicator“) (KPI)

LDAP Lightweight Directory Access Protocol. 50, *viz slovník:* Lightweight Directory Access Protocol (LDAP)

M2M komunikace stroje se strojem (anglicky „machine-to-machine“). 46, 48, 71

MaaS výroba-jako-služba (anglicky „Manufacturing as a Service“). 25, 40, *viz slovník:* výroba-jako-služba (anglicky „Manufacturing as a Service“) (MaaS)

MES výrobní informační systém (anglicky „manufacturing execution system“). 13, *viz slovník:* výrobní informační systém (anglicky „manufacturing execution system“) (MES)

MQTT Message Queue Telemetry Transport. 41, 43, 44, 46, *viz slovník:* Message Queue Telemetry Transport (MQTT)

MRP plánování potřeby výrobních zdrojů (anglicky „manufacturing resource/requirements planning“). 19, *viz slovník:* plánování potřeby výrobních zdrojů (anglicky „manufacturing resource/requirements planning“) (MRP)

NaaS síť-jako-služba (anglicky „Network as a Service“). 5, *viz slovník:* síť-jako-služba (anglicky „Network as a Service“) (NaaS)

NIST National Institute of Standards and Technology. 2–5, 19

OPC-UA OPC Unified Architecture. 44, 53, *viz slovník:* OPC Unified Architecture (OPC-UA)

PaaS platforma-jako-služba (anglicky „Platform as a Service“). 3, 5, 8, 17, 19–23, 32, 34, 35, 39, 41–49, 52–54, 57–60, 63, 70, 71, *viz slovník:* platforma-jako-služba (anglicky „Platform as a Service“) (PaaS)

PCI Payment Card Industry. 34

PHM předvídání a řízení provozního stavu zařízení (anglicky „prognostics and health management“). 23, 24, 64, *viz slovník:* předvídání a řízení provozního stavu zařízení (anglicky „prognostics and health management“) (PHM)

PK porovnávací kritéria (anglicky „comparison criteria, CC“). 25, 39, 40, 42

PLC programovatelný logický automat (anglicky „programmable logic controller“). 13, 14, 39, 53, 55, 57, 60, 72, 77, *viz slovník:* programovatelný logický automat (anglicky „programmable logic controller“) (PLC)

QoS kvalita služby (anglicky „quality of service“). 11, *viz slovník:* kvalita služby (anglicky „quality of service“) (QoS)

RaaS robot-jako-služba (anglicky „Robot as a Service“). 14, 39, 63, *viz slovník:* robot-jako-služba (anglicky „Robot as a Service“) (RaaS)

RC řídící jednotka robota (anglicky „robot controller“). 14, 78, *viz slovník:* řídící jednotka robota (anglicky „robot controller“) (RC)

REST Representational State Transfer. 43, 44, 47, 76, *viz slovník:* Representational State Transfer (REST)

RFID identifikace na rádiové frekvenci (anglicky „Radio-frequency Identification“). 13, *viz slovník:* identifikace na rádiové frekvenci (anglicky „Radio-frequency Identification“) (RFID)

SaaS software-jako-služba (anglicky „Software as a Service“). 3–5, 8, 17, 19–21, 23, 27, 28, 31, 32, 34, 35, 39, 42, 47, 48, 52, 53, 57, 63, 71, *viz slovník:* software-jako-služba (anglicky „Software as a Service“) (SaaS)

SAML Security Assertion Markup Language. 46, 50, 59, *viz slovník:* Security Assertion Markup Language (SAML)

SAN Storage Area Network. *viz slovník:* Storage Area Network (SAN)

SCADA dispečerské řízení a sběr dat (anglicky „Supervisory Control and Data Acquisition“). 13, *viz slovník:* dispečerské řízení a sběr dat (anglicky „Supervisory Control and Data Acquisition“) (SCADA)

SCIM System for Cross-domain Identity Management. 59, *viz slovník:* System for Cross-domain Identity Management (SCIM)

SDK soubor nástrojů pro vývoj software (anglicky „software development kit“). 49

SDN softwarově definovaná síť (anglicky „software-defined network“). 12, 13, 22, *viz slovník:* softwarově definovaná síť (anglicky „software-defined network“) (SDN)

SLA dohoda o úrovni služeb (anglicky „Service Level Agreement“). 31, 56, *viz slovník:* dohoda o úrovni služeb (anglicky „Service Level Agreement“) (SLA)

SOA architektura orientovaná na služby (anglicky „service-oriented architecture“). 14, *viz slovník:* architektura orientovaná na služby (anglicky „service-oriented architecture“) (SOA)

SOX Sarbanes-Oxley Act. 35

SPI model SPI. 5, *viz slovník:* model SPI (SPI)

SSL Secure Sockets Layer. 35, 59, 67, 77, *viz slovník:* Secure Sockets Layer (SSL)

StaaS úložiště-jako-služba (anglicky „Storage as a Service“). 5, 22, 30, *viz slovník:* úložiště-jako-služba (anglicky „Storage as a Service“) (StaaS)

SU strojové učení (anglicky „machine learning, ML“). 47, 59

SW software. 1, 25, 28, 30, 32, 44, 45, 49, 51, 52, 57, 58, 61, 63–65

TLS Transport Layer Security. 46, 67, 69, 74, *viz slovník:* Transport Layer Security (TLS)

UAA uživatelský účet a autentizace (anglicky „user account and authentication“). 59

UI umělá inteligence (anglicky „artificial intelligence, AI“). 47

USA Spojené státy americké. 31

V/V vstup/výstup (anglicky „input/output, I/O“). 22, 31

VF virtuální továrna (anglicky „virtual factory“). 23, 64, *viz slovník:* virtuální továrna (anglicky „virtual factory“) (VF)

VPLC virtuální programovatelný logický automat (anglicky „virtual programmable logic controller“). 14, *viz slovník:* virtuální programovatelný logický automat (anglicky „virtual programmable logic controller“) (VPLC)

VPN virtuální privátní síť (anglicky „virtual private network“). 2, 7, 22, 35, 77, *viz slovník:* virtuální privátní síť (anglicky „virtual private network“) (VPN)

VRC virtuální řídící jednotka robota (anglicky „virtual robot controller“). 14, 15, 39, 57, 60, *viz slovník:* virtuální řídící jednotka robota (anglicky „virtual robot controller“) (VRC)

WAMS systém pro sledování rozsáhlých oblastí (anglicky „wide-area monitoring system“). 36, 37, *viz slovník:* systém pro sledování rozsáhlých oblastí (anglicky „wide-area monitoring system“) (WAMS)

WPM správa pracovních výkonů (anglicky „workforce performance management“). 21, *viz slovník:* správa pracovních výkonů (anglicky „workforce performance management“) (WPM)

XACML eXtensible Access Control Markup Language. 59, *viz slovník:* eXtensible Access Control Markup Language (XACML)

XML Extensible Markup Language. 68, 74, 75, *viz slovník:* Extensible Markup Language (XML)