



**FAKULTA
INFORMAČNÍCH
TECHNOLÓGIÍ
ČVUT V PRAZE**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název: Metodika pre realizáciu legálne metrologického SW v prostredí Cloud Computing
Student: Vladimír Pozdeev
Vedoucí: Ing. Martin Koval, Ph.D.
Studijní program: Informatika
Studijní obor: Informační systémy a management
Katedra: Katedra softwarového inženýrství
Platnost zadání: Do konce letního semestru 2020/21

Pokyny pro vypracování

Cílem práce je analyzovat možnosti realizace legálně metrologického SW v prostředí Cloud Computing (CC). Výstupem práce bude metodika a její obchodní model sloužící pro implementaci metrologického SW v souladu s WG7.2 (příručkou WELMEC Guide) v prostředí CC.

Pro realizaci bakalářské práce postupujte dle následných kroků:

- 1 Specifikujte vlastnosti měřícího zařízení dle WG7.2.
- 2 Zvolte poskytovatele CC pro realizaci bakalářské práce.
- 3 Vypracujte přehled metodik, které jsou zaměřeny na validaci SW v CC.
- 4 Navrhněte architekturu pro aplikaci (SW) reprezentující měřící zařízení.
- 5 Analyzujte možnosti zabezpečení a ukládání dat pro metrologický SW v CC v souladu s WG7.2.
- 6 Vypracujte metodiku pro realizaci legálně metrologického SW pro měřící zařízení v CC v souladu s WG7.2.
- 7 Analyzujte jak metodika pro validaci metrologického SW pro měřící zařízení v CC koresponduje s jinými metodikami pro validaci SW v CC a navrhněte ekonomický (obchodní) model uplatnění metodiky na trhu.

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 23. ledna 2020



**FAKULTA
INFORMAČNÍCH
TECHNologiÍ
ČVUT V PRAZE**

Bakalářská práce

Metodika pro realizaci legálně metrologického SW v prostředí Cloud Computing

Vladimir Pozdeev

Katedra softwarového inženýrství

Vedoucí práce: Ing. Martin Koval, Ph.D.

21. prosince 2020

Poděkování

Tímto bych chtěl poděkovat především p. Ing. Martinu Kovalovi, Ph.D. za pomoc při tvorbě bakalářské práce. A také bych chtěl poděkovat p. Ing. Zuzaně Pospíšilové za pomoc při korektuře gramatické části práce.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 21. prosince 2020

.....

České vysoké učení technické v Praze
Fakulta informačních technologií

© 2020 Vladimír Pozdeev. Všechna práva vyhrazena.

Tato práce vznikla jako školní dílo na Českém vysokém učení technickém v Praze, Fakultě informačních technologií. Práce je chráněna právními předpisy a mezinárodními úmluvami o právu autorském a právech souvisejících s právem autorským. K jejímu užití, s výjimkou bezúplatných zákonných licencí a nad rámec oprávnění uvedených v Prohlášení na předchozí straně, je nezbytný souhlas autora.

Odkaz na tuto práci

Pozdeev, Vladimír. *Metodika pro realizaci legálně metrologického SW v prostředí Cloud Computing*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2020.

Abstrakt

Tato bakalářská práce se zabývá problematikou metrologických SW v kategoriích, jako: dlouhodobé ukládání dat, komunikace, download SW. Problém bude řešen s využitím technologií Cloud Computing a podle metodiky Welmec Guide 7.2.

Práce bude rozdělena na dvě části: teoretická část a praktická část.

Cílem teoretické části práce je specifikovat vlastnosti měřicího zařízení podle Welmec Guide 7.2, vypracovat stručný přehled platform CC a zvolit vhodného poskytovatele pro realizaci bakalářské práce. Do teoretické části také bude patřit přehled struktury Welmec Guide 7.2, požadavků na typy přístrojů a možnosti rozšíření.

Cílem praktické části práce je analyzovat a popsat možnosti zabezpečení a ukládání dat pro metrologický SW v CC v souladu s Welmec Guide 7.2. Cílem také je navrhnout vhodnou architekturu pro aplikaci (SW) reprezentující měřicí zařízení na základě Welmec Guide 7.2.

Klíčová slova Metrologie, Cloud computing, Welmec Guide 7.2, Software, Bezpečnost, Amazon Web Services.

Abstract

This bachelor thesis deals with problems of metrological SW in categories such as: long-term data storage, communication, download SW. The problem will be solved using Cloud Computing and Welmec Guide 7.2 methodology.

Bachelor thesis will be divided into two parts: the theoretical part and the practical part.

The aim of the theoretical part of the thesis is to specify properties of the measuring equipment of Welmec Guide 7.2, to develop a brief overview of the CC platforms and to choose the appropriate provider for the bachelor thesis. The theoretical part will also include an overview of the Welmec Guide 7.2, device type requirements and expandability.

The aim of the practical part is to analyze and describe the possibilities of data security and storage for metrological SW in CC in accordance with Welmec Guide 7.2. Also the aim is to design a suitable architecture for application (SW) representing the measuring equipment based on Welmec Guide 7.2.

Keywords Metrology, Cloud computing, Welmec Guide 7.2, Software, Safety, Amazon Web Services.

Obsah

Úvod	1
1 Cíl práce	3
2 Cloud Computing	5
2.1 Popis a vyvoj Cloud Computing	5
2.2 Nevýhody Cloud computing	7
2.3 Výhody Cloud Computing	7
2.4 Bezpečnost	8
2.5 Aktuální stav	8
3 Výběr platformy Cloud computing	9
3.1 Platformy	9
3.2 Srovnání Azure a AWS	9
3.3 Amazon Web Services	9
4 Metrologie	15
4.1 Definice	15
4.2 Historie metrologie	15
4.3 Legální metrologie	16
4.4 Měřicí zařízení	16
5 Welmec Guide 7.2: Softwarová příručka	19
5.1 Welmec Guide 7.2	19
5.2 Požadavky	19
5.3 Rozšíření	20
6 Řešení Cloud computing pro legální metrologii	23
6.1 IaaS	23
6.2 PaaS	24

6.3	SaaS	24
7	Aplikace měřicích zařízení do cloudu	27
7.1	Systém	27
7.2	Funkcionalita uživatelského rozhraní	35
7.3	Databáze	40
7.4	Bezpečné připojení k AWS službám	43
8	Trh a Cloud	47
8.1	Cloud v průmyslové výrobě	47
8.2	Role metrologie pro digitalizaci a ekonomiku	48
8.3	Statistika Cloud Computing na trhu	49
9	Přínosy	51
9.1	Aktuální stav	51
9.2	Perspektivy	51
9.3	AWS	52
9.4	Bezpečnost	52
	Závěr	53
	Literatura	55
A	Seznam použitých zkratk	61
B	Obsah příloženého SD	63

Seznam obrázků

2.1	Cloud Computing [1].	6
3.1	Podíl na trhu [2].	10
3.2	Bezpečnostní služby AWS [3]	13
3.3	Sdílená odpovědnost [4]	14
4.1	Bloková schéma: měřící zařízení.	16
5.1	Struktura Welmec Guide 7.2	20
6.1	Infrastructure as a Service v cloudu [5].	24
6.2	Software as a Service v cloudu [5].	25
7.1	Use case diagram: Konzument.	36
7.2	Use case diagram: Kontrolní orgán.	37
7.3	Use case diagram: Výrobce.	38
7.4	Use case diagram: Poskytovatel energií.	39
7.5	Databázový model.	41
7.6	AWS IoT [4]	44
7.7	AWS Security Token Service [4]	45

Seznam tabulek

3.1	Srovnání Azure a AWS	11
5.1	Požadavky na přístroje typu P a U	21
5.2	Možnosti rozšíření podle Welmec Guide 7.2	22
7.1	Splnění podle typu rozšíření Welmec Guide 7.2	30
9.1	S3 Standard Storage [6].	52

Úvod

V současné době není možné si představit náš život bez Cloudových technologií a v budoucnu se očekává mnohem efektivnější využití. Aktuálně technologie Cloud Computing jsou ve stavu rychlého rozvoje a používají se skoro ve všech oborech života a tam, kde ještě se nepoužívají, už za pár let určitě budou.

Technologie CC bude samozřejmě i v legální metrologii. To přinese velké množství výhod, zejména teď, když se vyvíjejí environmentální řešení problémů lidstva. Jedno z populárních a rychle se rozvíjejících řešení je Smart City.

Smart city - je to město, které bude využívat digitální a informační technologie pro zlepšení života ve všech typech moderních měst. Zaměřuje se především na efektivní využívání zdrojů, jako: snižování spotřeby energií, sdílení dat pro veřejné účely a optimalizaci dopravy. Jedním z hlavních bodů Smart city je zlepšení životního prostředí. V Smart city bude možné: měřit kvalitu vody, vzduchu, řešit efektivní svoz odpadu, využívat obnovitelné zdroje a snížit emise CO₂ [7].

Toto je pouze malá část výhod, který přinese technologie CC v metrologii v našem moderním světě.

Cíl práce

Cílem bakalářské práce je analyzovat možnosti realizace legálního metrologického SW v prostředí Cloud Computing. Práce také pomůže vyřešit problémy implementace metrologického SW v CC v kategoriích, jako: dlouhodobé ukládání dat, komunikace, download SW. Cíle práce budou řešeny s využitím technologií Cloud Computing a podle pravidel WelmeC Guide 7.2.

Cloud Computing

2.1 Popis a vyvoj Cloud Computing

Cloud Computing je model vývoje a dodávání výpočetních služeb přes Cloud, jako jsou servery, databáze, síť, software a další. Společnosti, který nabízejí tyto služby se nazývají poskytovatelé Cloudu. Mezi hlavní pozitiva Cloud Computingu v současnosti patří nízké náklady, škálovatelnost a pružnost.

Myšlenka Cloud Computingu pochází z 20. století. Vedoucí vývojové skupiny, která vytvořila ARPANET - Joseph Carl Robnett Licklider měl myšlenku, že všechno po celém světě bude propojené pomocí počítačů a kdokoli, kdykoli a odkudkoli bude mít možnost přistupovat k datům. První projekt na Cloud Computingu byl Salesforce.com v roce 1999. V roce 2002 Amazon spustila projekt Amazon Mechanical Turk, součástí kterého byl CC [8]. Samotnou Cloud Computing službu Amazon spustil v roce 2006 a dodnes zůstává vůdcem v této oblasti.

Model nasazení

Cloudy se odlišují metodou nasazení prostředků. Existují čtyři modely: veřejný cloud, komunitní cloud, soukromý cloud a hybridní cloud.

- Veřejný cloud

Cloudy jsou provozované jinými poskytovateli cloudu, kteří dodávají své servery a úložiště přes internet.

- Soukromý cloud

Cloudy jsou provozované pouze pro organizaci, kde se infrastruktura spravuje v privátní síti.

- Komunitní cloud

Cloudy, kde infrastruktura je sdílena mezi několika organizacemi.

- Hybridní cloud



Obrázek 2.1: Cloud Computing [1].

Je kombinací veřejného a soukromého cloudu. Cloudy jsou propojené tak, aby mezi nimi bylo možné sdílet aplikace a data [9].

Typy služeb

Existují tři modely služeb Cloud computingu: Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS), Software-as-a-service (SaaS).

- IaaS

Služba, kde spotřebitel používá výpočetní prostředky dodavatele (server, síťová infrastruktura, úložiště).

- PaaS

Služba, kde dodavatel poskytuje spotřebiteli přístup k softwarové platformě.

- SaaS

Služba, kde spotřebitel může používat hotovou aplikaci dodavatele [10].

2.2 Nevýhody Cloud computing

Navzdory obrovskému množství výhod existují i nevýhody použití CC:

- S výjimkou pro soukromý cloud, pro práce je nutné mít neustálé připojení k Internetu
- Uživatel nemůže vždy přizpůsobit software pro sebe
- Bezpečnost dat může být pod hrozbou
- Firmy jsou vázané na nové náklady

2.3 Výhody Cloud Computing

Mezi hlavní důvody, proč společnosti přecházejí ke službám CC jsou:

- Náklady
S Cloud Computing není nutné kupovat hardware a software, vytvářet místní datová centra.
- Rychlost
Množství výpočetních prostředků lze zjistit během několika minut, což přináší flexibilitu.
- Škálovatelnost
Znamená to, že lze dodat vhodné množství IT prostředků, například více nebo méně výpočetních sil.
- Spolehlivost
Zálohování dat, kontinuita podnikových procesů bude mnohem méně nákladná.
- Produktivita
Cloud computing odstraňuje potřebu nastavení hardwaru a softwaru a také další náročné úkoly na správu IT [10].

Stále více společností se stěhuje do CC a dodavatelé vyvíjejí bezpečnostní nástroje a používají časté zálohování.

2.4 Bezpečnost

Pro zajištění bezpečnosti je nutné vždy mít nové metody a technologie ochrany. Úkolem poskytovatele je zajistit fyzickou i programovou nedotknutelnost údajů proti napadení třetími stranami. Spotřebitel by měl zavést příslušné politiky a postupy, které vylučují převod přístupových práv třetím stranám. Jak ukazuje praxe, použití Cloud computingu může i výrazně zlepšit úroveň zabezpečení dat. Jedním z důvodů je neustálá práce na vysoké úrovni bezpečnosti ze strany společností poskytujících přístup k službám Cloud Computingu, protože oni vědí o obavách svých zákazníků a jsou nuceni investovat značné prostředky na vytváření nových bezpečnostních servisů a udržování spolehlivého systému ochrany. Někteří poskytovatelé služeb v oblasti Cloud computing zaměřují své marketingové akce přesně na záruku vysoké úrovně bezpečnosti.

Pro zajištění spolehlivého bezpečnostního systému musí být dodržena řada podmínek pro ochranu, kde hlavními jsou:

- Měly by být použity kryptografické prostředky zabezpečení dat. Všechna data, s kterými klient pracuje v rámci služby, musí být bezpečně zašifrovány.
- Samotný proces přenosu informací z klienta na server a zpět by měl být také bezpečný, to znamená, že pro přístup na server je třeba použít zabezpečené protokoly přenosu dat.

Každý poskytovatel nabízí řadu bezpečnostních služeb.

2.5 Aktuální stav

Cloud computing je stále se rozvíjející obor. V posledních letech vidíme velký růst nasazení různými firmami. Předpokládá se, že příjmy globálního cloudového IT trhu se zvýší z 180 miliard dolarů v roce 2015 na 390 miliard dolarů v roce 2020 a dosáhnou roční průměrný růst (CAGR) 17% [11].

Výběr platformy Cloud computing

3.1 Platformy

Ve spolupráci s vedoucím práce jsme vybrali variantu vypracovat stručný přehled platform CC a zvolit jednoho vhodného poskytovatele pro realizaci projektu. Platform, které využívají technologie Cloud computing v různých oborech je velké množství a zvolit jednu variantu nebylo jednoduché, protože každá má své výhody a nevýhody.

V současné době existují čtyři nejznámější platformy: Amazon Web Services, Google Cloud, Azure a IBM Cloud. Cloud od Google a od IBM mají mnohem menší podíl na trhu, než Azure a AWS (obrázek 3.1 [2]). Proto vybíráme pouze mezi Azure od Microsoft a AWS od Amazon.

3.2 Srovnání Azure a AWS

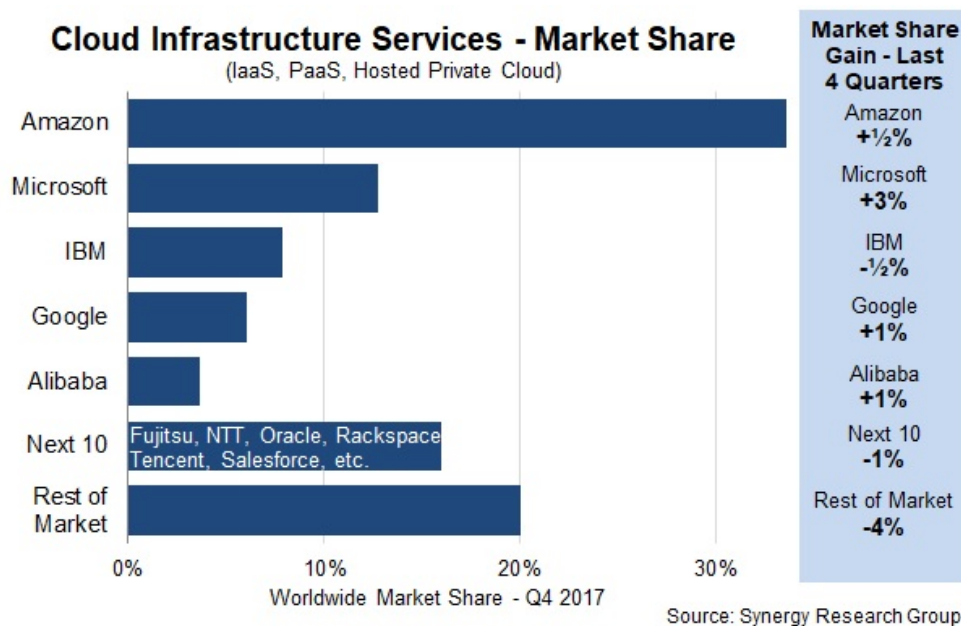
V tabulce lze vidět srovnání platform Azure a Amazon Web Services podle základních parametrů (tabulka 3.1).

Zvolili jsme platformu pro realizaci našeho projektu - AWS. Platforma má velké množství uživatelů, vysokou úroveň bezpečnosti a vysokou rychlost přenosu dat.

3.3 Amazon Web Services

Amazon postupně změnil ekonomický aspekt zahájení nových IT společností. AWS nabízí své služby od roku 2006. Málokdo ví, jak mnoho firem používá Amazon EC2 ve své infrastruktuře a pokud dojde k nějakému selhání, dojde k výpadku mnoha internetových stránek. To znamená, že Amazon má velmi dobrý a kvalitní produkt. Lidé vybírají tuto službu, protože zjednodušuje

3. VÝBĚR PLATFORMY CLOUD COMPUTING



Obrázek 3.1: Podíl na trhu [2].

spuštění aplikací a služeb, čímž snižuje množství potřebných znalostí, šetří peníze, které jsou potřebné k zahájení spouštění.

Mezi zákazníky AWS je mnoho známých světových značek, jako jsou: SAP, Vodafone, Siemens, Adobe, Expedia, Atlassian, AirAsia, Avianca, D-Link, Airbnb, Unilever, Spotify a stovky dalších zákazníků [17].

Amazon poskytuje skvělou infrastrukturu, která velmi zjednodušuje rozvoj škálovatelných a odolných aplikací proti chybám.

3.3.1 Základní služby

Amazon EC2

První a nejdůležitější věc, kterou musíme vědět o AWS je to - EC2.

Amazon Elastic Compute Cloud (Amazon EC2) - je to webová služba, která poskytuje bezpečné a výpočetní prostředky v cloudu. EC2 pomáhá vývojářům zlepšit rozsáhlých výpočtů v cloudu [18].

Hlavní výhodou EC2 je flexibilita. Je možné pustit nový server velmi rychle a za několik minut se už přihlásit.

Amazon S3

Amazon Simple Storage Service (Amazon S3) - je úložiště objektů určené pro ukládání a načítání libovolných dat z libovolných zdrojů. Podle oficiálního webu služba zaručuje spolehlivost ukládání na úrovni 99,999999999%. Amazon S3 je nejvíce podporovaná platforma cloud storage [19].

Prvek	Microsoft Azure	AWS
Vlastnosti	Má velký rozsah funkcí pro selektivní kategorie - například PaaS a IaaS [12].	AWS má nejširší spektrum funkcí. Ale vyžadují více řízení než ostatní [12].
Cena	Za služby Azure můžeme platit pouze za jejich použití a nejsou žádné předběžné náklady [13].	Za AWS můžeme platit pouze za konkrétní služby, které potřebujeme, a pouze za jejich použití [14].
Přístupový zóny	Azure obsahuje 50 přístupových zón a je k dispozici ve 140 zemích [15].	Cloud AWS obsahuje 54 přístupových zón, které jsou umístěny v 18 geografických regionech po celém světě. Aktuálně vytvářejí ještě 12 přístupových zón [16].
Podíl na trhu	Azure je na druhém místě na trhu [2].	AWS je lídrem na trhu [2].
Dodržování	Prohlašuje, že má více certifikací, než každý z jiných poskytovatelů [12].	Má silný vztah s globálními agenturami [12].

Tabulka 3.1: Srovnání Azure a AWS

Amazon RDS

Amazon Relational Database Service (Amazon RDS) umožňuje konfigurovat, měnit relační databáze a používat v cloudu. Amazon RDS umožňuje používat šest databázových strojů podle výběru, mezi něž patří: Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle a Microsoft SQL Server [20].

Amazon ElastiCache

Amazon ElastiCache - je webová služba, která zjednodušuje nasazení a škálování v cloudu nebo cache v paměti. ElastiCache podporuje dvě služby s otevřeným zdrojovým kódem: Redis a Memcached [21].

Amazon DynamoDB

Amazon DynamoDB - je databáze NoSQL od společnosti Amazon. Cloud databáze podporuje práci založenou jak na dokumentech, tak i repositář key-value [22].

Elastic Load Balancing

Elastic Load Balancing - je balancer zatížení, který distribuuje požadavky uživatele podle různých EC2 Instances v různých zónách dostupnosti nebo podle IP-adres. Elastic Load Balancing nabízí tři produkty pro vyvažování zátěže: Application Load Balancer (nejvhodnější pro vyvažování zátěže přenosů

HTTP a HTTPS), Network Load Balancer (nejvhodnější pro vyvažování zátěže přenosů TCP), Classic Load Balancer (poskytuje základní vyvažování zátěže mezi Amazon EC2 Instances) [23].

Amazon Route 53

Amazon Route 53 - je vysoce dostupná a škálovatelná webová služba založená na cloudu pro systém DNS (Domain Name System). Prostřednictvím Route 53 lze registrovat domény přímo v Amazonu a služba je plně kompatibilní s protokolem IPv6 [24].

Amazon CloudFront

Amazon CloudFront - je služba doručování obsahu (CDN), která zajišťuje zabezpečené doručení dat s vysokou přenosovou rychlostí. CloudFront spolupracuje s dalšími službami: Amazon S3, Elastic Load Balancing, Amazon EC2 a AWS Shield pro neutralizaci útoků DDoS [25].

Amazon CloudWatch

Amazon CloudWatch je služba pro sledování zdrojů cloudu AWS a může být použita k shromažďování a sledování metrik, analýze souborů protokolu, vytváření výstrah a automatickému reagování na změny zdrojů AWS [26].

Amazon CloudSearch

Amazon CloudSearch - je služba v cloudu AWS, která umožňuje konfigurovat vyhledávací řešení pro webové stránky nebo aplikace. CloudSearch nyní podporuje 34 jazyků a mnoho vyhledávacích funkcí [27].

AWS Identity and Access Management (IAM)

Služba IAM poskytuje možnost bezpečně spravovat přístup k službám a zdrojům AWS. Pomocí služby IAM lze vytvářet uživatele nebo skupiny uživatelů AWS, spravovat a používat oprávnění k udělení nebo odepření přístupu [28].

Existuje mnoho dalších služeb, například Config (poskytuje přístup k konfiguraci zdrojů AWS), SQS (fronta zpráv), SES (služba pro posílání pošty), EMR (Hadoop v cloudu) a desítky dalších služeb.

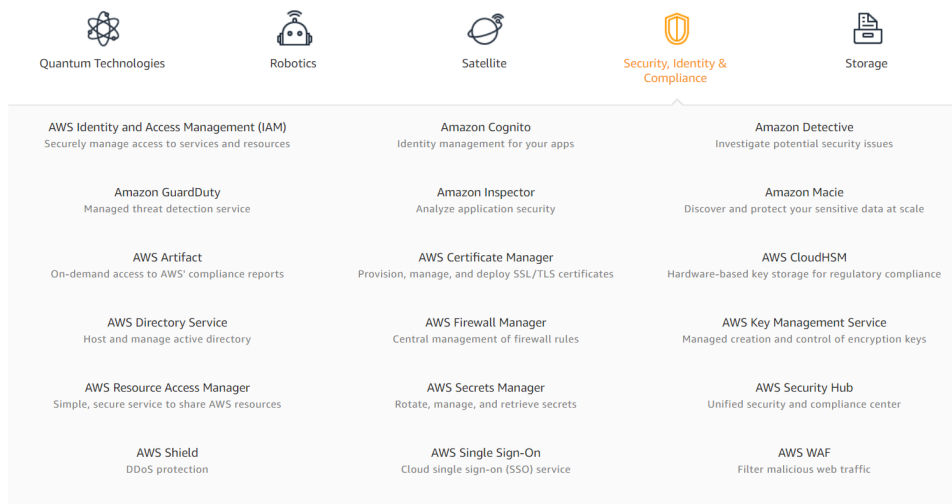
3.3.2 Bezpečnost AWS

AWS poskytuje několik funkcí zabezpečení a služeb:

- Síťové firewally v Amazon VPC.
- AWS WAF, umožňující vytvářet soukromé sítě a spravovat přístup.
- Šifrování dat přes protokol TLS.
- Možnost implementovat strategii vrstvené ochrany proti útokům DDoS.
- Flexibilní možnosti správy klíčů, kde zákazník si může vybrat zachovat plnou kontrolu nad šifrovacími klíči, nebo předat správu klíčů AWS.

- Služby které automaticky vyhodnocují aplikace pro zranitelnosti.
- Nástroje pro správu účetnictví a konfigurace.
- Monitorování a protokolování.
- Možnosti definovat a prosazovat politiky přístupu uživatelů
- Inspekce zranitelnosti a proniknutí

Existuje i mnoho dalších služeb pro maximální bezpečnost. Pouze na hlavní stránce AWS je vidět jak mnoho bezpečnostních prvků jsou v nabídce (obrázek 3.2 [3]).

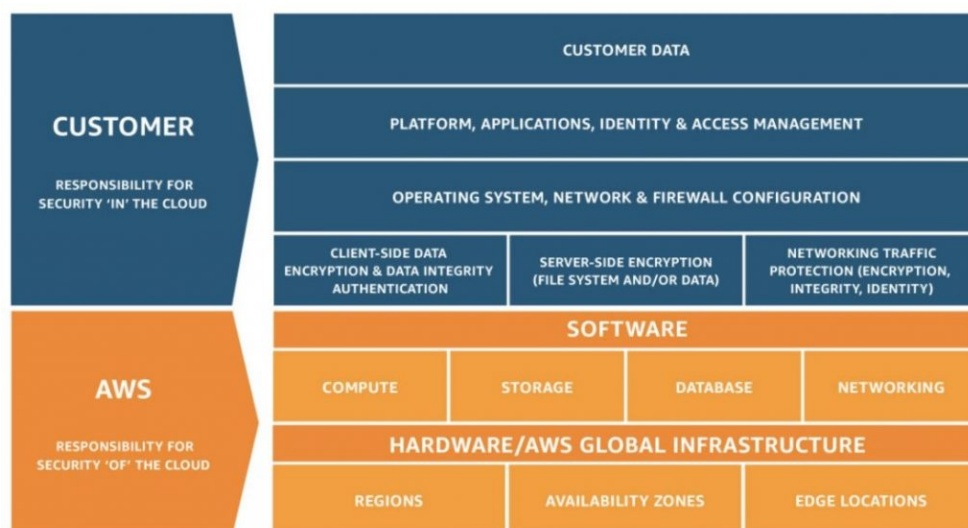


Obrázek 3.2: Bezpečnostní služby AWS [3]

3.3.2.1 Odpovědnost za bezpečnost

Amazon poskytují sadu efektivních metod pro zvýšení zabezpečení, ale nemůžeme očekávat, že tyto metody budou nést plnou odpovědnost za konkrétní aplikace. AWS proto mají řadu dokumentů o sdílené odpovědnosti, které popisují roli poskytovatele a roli uživatele. Na základě studia dokumentů můžeme říct, že poskytovatelé CC mají odpovědnost za bezpečnost Cloudu a zákazníci jsou odpovědní za aplikace a používané data. (obrázek 3.3 [4]).

3. VÝBĚR PLATFORMY CLOUD COMPUTING



Obrázek 3.3: Sdílená odpovědnost [4]

Metrologie

4.1 Definice

Metrologie - věda zabývající se měřením. Metrologie má v technické praxi důležité místo. Je nezbytná zvláště při kontrole a řízení jakosti [29].

V praktickém životě se člověk všude zabývá rozměry. Každý den se člověk setkává s měřením různých veličin, jako je délka, objem, hmotnost, čas a další. Metody a prostředky měření těchto veličin ve starověku byly primitivní a nedokonalé, nicméně byli potřebné pro evoluci civilizací.

Metrologie má velký význam pro pokrok přírodních a technických věd, protože zvýšení přesnosti měření je jedním ze základních způsobů, jak zlepšit způsoby poznávání přírody člověkem, objevy a praktické uplatnění znalostí.

4.2 Historie metrologie

Potřeba měření vznikla už v prvních činnostech lidstva. K tomu se používaly především improvizované prostředky. Například, jednotkou hmotnosti drahých kamenů je karát, který v překladu z jazyků starého jihovýchodu znamená - fazole. Babylonci založili rok, měsíc, hodinu. Následně bylo $1/86400$ části průměrné doby otáčení Země kolem její osy nazváno sekundami.

Nový význam metrologie získala v době průmyslové revoluce. Historicky významné fáze ve vývoji metrologie jsou:

- rok 1832 - vytvoření absolutních systémů jednotek Karlem Gaussem
- rok 1875 - podpis Metrické konvence
- rok 1960 - vývoj a zavedení Mezinárodního systému jednotek (SI) [30]

Světový den metrologie se slaví každoročně 20. května. V roce 1875 byla v Paříži podepsána mezinárodní smlouva o metrické soustavě, Metrická konvence [31].

4.3 Legální metrologie

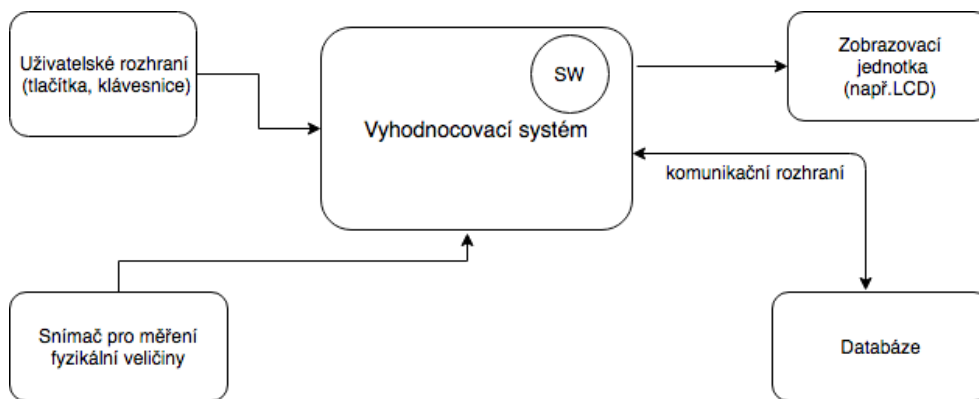
Legální metrologie se primárně zabývá měřidly, která podléhají metrologické kontrole, a hlavním cílem legální metrologie pak je zabezpečit občanům správné výsledky měření. Vedle legální metrologie existuje dále mnoho dalších oblastí legislativy, kde je měření nezbytné k posouzení shody s předpisy nebo zákony. Měřidla podléhající metrologické kontrole by měla garantovat správné výsledky měření:

- v průběhu celého období používání
- v provozním režimu
- v mezích stanovených povolených chyb

Národní a regionální legislativa stanoví v oblasti legální metrologie požadavky na měřidla, metody měření a zkoušení [32].

4.4 Měřicí zařízení

Měřicí přístroj je zařízení používané k měření, samostatně nebo ve spojení s jedním nebo více doplňkovými zařízeními [33] (obrázek 4.1).



Obrázek 4.1: Blokové schéma: měřicí zařízení.

Uživatelské rozhraní - je rozhraní, které poskytuje přenos informací mezi uživatelem a komponentami zařízení.

Snímač pro měření fyzikální veličiny - je zařízení, které je určeno pro snímání a detekci fyzikálních veličin.

LCD displej - je zobrazovací jednotka s malou hustotou informací a kapalnými krystaly [34].

Databáze - je systém pro ukládání dat a jejich následné zpracování. Data jsou uložena na paměťovém médiu a mají mezi sebou určité vztahy [35].

Vyhodnocovací systém tvoří soubor ústrojí, který zpracovává výstupní signál z převodníku [36].

V současné době měřidla, která jsou předmětem pro legální metrologii, často obsahují SW, který musí být kontrolován a v současné době je nejlépe zpracován dokument Welmec Guide 7.2, který slouží pro validaci SW v zemích Evropské unie.

Měřicí přístroje mají řadu parametrů, hlavní z nich jsou:

- Rozsah měření

Rozsah hodnot naměřené hodnoty, pro které je zařízení určeno.

- Přesnost

Schopnost přístroje označovat skutečnou hodnotu měřeného indikátoru.

- Prah citlivosti

Představuje určitou minimální hodnotu naměřené hodnoty, kterou může zařízení rozlišit.

- Citlivost

Spojuje hodnotu měřeného parametru s odpovídající změnou naměřených hodnot přístroje.

- Stabilita

Schopnost přístroje udržovat stanovenou přesnost měření po určitou dobu [36].

Welmec Guide 7.2: Softwarová příručka

5.1 Welmec Guide 7.2

Welmec je organizace zajišťující spolupráci v oblasti legální metrologie mezi členskými státy Evropské unie a členy EFTA. Příručky organizace Welmec mají pouze doporučující charakter, nepředstavují žádná omezení a nepředepisují žádné technické požadavky nad rámec požadavků stanovených příslušnými normami Evropské unie [37].

Welmec Guide 7.2 je technická příručka, která se zabývá aplikací směrnice MID, a to zejména na měřicí přístroje vybavené softwarem (obrázek 5.1). Její míra podrobnosti je zaměřena na potřeby výrobců měřicí techniky a požadavky notifikovaných osob zabývajících se posouzením shody měřicích přístrojů [37].

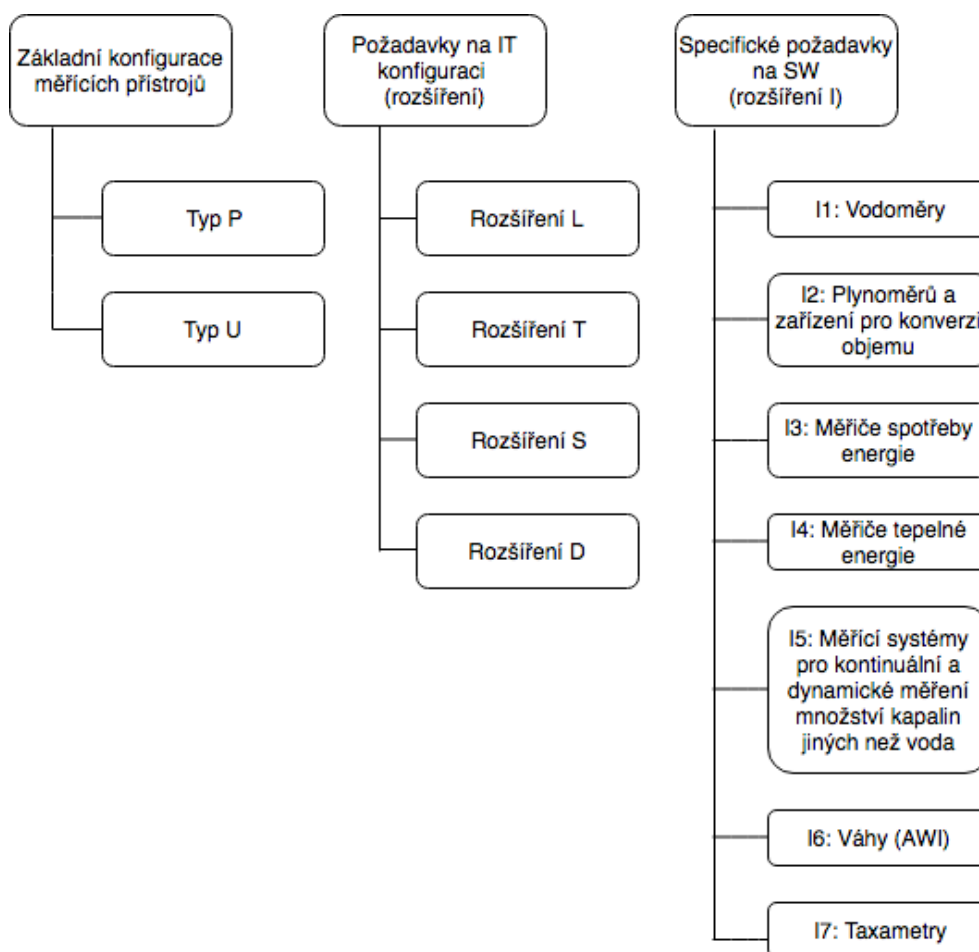
5.2 Požadavky

5.2.1 Měřicí přístroje typu P a U

Požadavky typu P - jsou požadavky na vestavěný software v jednoúčelových měřicích přístrojích. Přístroj typu P je měřicí přístroj s vestavěným IT systémem. Požadavky typu U - jsou požadavky na přístroje využívající univerzální počítač [37].

5.2.1.1 Požadavky na přístroje typu P a U

Požadavky jsou rozděleny do několika kategorií a vypadají následovně podle tabulky (tabulka 5.1).



Obrázek 5.1: Struktura Welmec Guide 7.2

5.3 Rozšíření

5.3.1 Typy rozšíření L, T, S, D, I

Rozšíření L

Požadavky rozšíření L se týkají dlouhodobého ukládání naměřených dat. Termín „dlouhodobé ukládání“ označuje úsek od chvíle, kdy je měření fyzicky dokončeno, až do okamžiku ukončení všech procesů [37].

Rozšíření T

Požadavky rozšíření T se aplikují, když jsou naměřená data přenášena přes komunikační síť do vzdáleného zařízení, kde jsou data dále zpracována a nebo použita k legálně relevantním účelům [37]. Síť může být otevřená a uzavřená.

Rozšíření S

Typ P	Typ U
P1: Dokumentace	U1: Dokumentace
P2: Označení softwaru	U2: Označení softwaru
P3: Vliv uživatelského rozhraní	U3: Vliv uživatelského rozhraní
P4: Vliv komunikačního rozhraní	U4: Vliv komunikačního rozhraní
P5: Ochrana proti náhodným či neúmyslným změnám	U5: Ochrana proti náhodným či neúmyslným změnám
P6: Ochrana proti záměrným změnám	U6: Ochrana proti záměrným změnám
P7: Ochrana parametrů	U7: Ochrana parametrů
P8: Prezentace naměřených dat	U8: Prezentace naměřených dat
	U9: Vliv jiného softwaru

Tabulka 5.1: Požadavky na přístroje typu P a U

Požadavky rozšíření S umožňují rozlišit legálně relevantní software od legálně nerelevantního softwaru [37]. Oddělení softwaru je realizováno nezávisle na operačním systému na nízké úrovni (na úrovni programovacího jazyka) a softwarové moduly jsou realizovány na vysoké úrovni.

Rozšíření D

Rozšíření D se aplikují pouze na přístroje vybavené nástroji na stahování a nahrávání legálně relevantního SW bez porušení plomby.

Rozšíření I

Požadavky rozšíření I se týkají přístrojů konkrétního typu, což znamená, že pouze doplňuje požadavky ostatních rozšíření a typů, a to pouze v případě, když jsou k tomu doplňující požadavky v MID (Measuring Instruments Directive). V této sekci může být uvedena informace o nejčastějších technických konfiguracích, jak jsou použity požadavky a rozšíření, užitečné kontrolní seznamy.

Rozšíření jsou rozdělena do několika kategorií a vypadají následovně podle tabulky (tabulka 5.2).

Rozšíření L	Rozšíření T	Rozšíření S	Rozšíření D
L1: Úplnost uložených naměřených dat	T1: Úplnost přenesených dat	S1: Realizace oddělení softwaru	D1: Mechanismus stahování
L2: Ochrana proti náhodným či neúmyslným změnám	T2: Ochrana proti náhodným či neúmyslným změnám	S2: Smíšená indikace	D2: Prokázání věrohodnosti přeneseného softwaru
L3: Integrita dat	T3: Integrita dat	S3: Ochranné rozhraní softwaru	D3: Integrita stahovaného softwaru
L4: Sledovatelnost uložených naměřených dat	T4: Sledovatelnost přenášených naměřených dat		D4: Ná vaznost stahovaného legálně relevantního softwaru
L5: Utajení klíčů	T5: Utajení klíčů		
L6: Načtení, ověření a označení uložených dat	T6: Příjem, ověření a zpracování přenášených naměřených dat		
L7: Automatické ukládání	T7: Zpoždění při přenosu		
L8: Kapacita paměti a kontinuita	T8: Dostupnost přenosových služeb		

Tabulka 5.2: Možnosti rozšíření podle Welmec Guide 7.2

Řešení Cloud computing pro legální metrologii

Celý cloud systém se skládá ze zařízení, síťové části včetně firewallu, fyzického serveru, virtuálních počítačů, použitého operačního systému, paměťového zařízení a webového serveru [5]. Je důležité se podívat na vztahy mezi modely Cloud computing. Tři důležité konfigurace CC: IaaS, PaaS na SaaS.

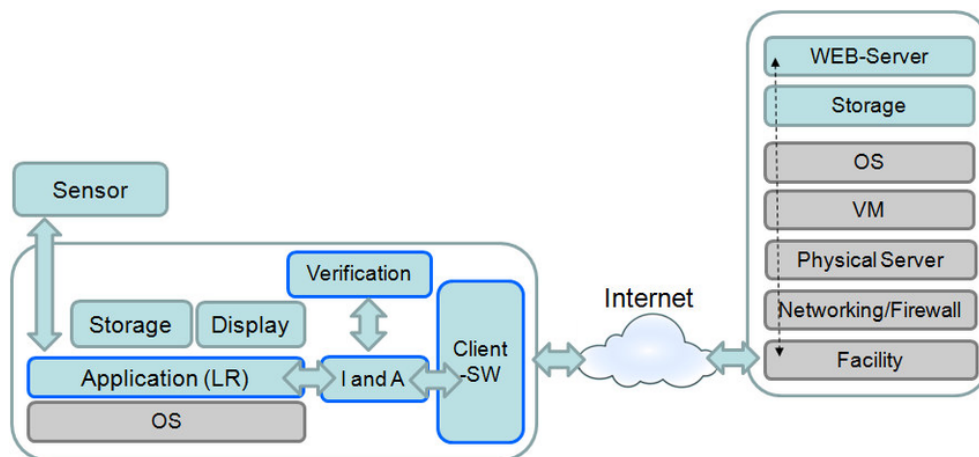
6.1 IaaS

Obecně model IaaS poskytuje rozšiřitelnost s několika funkcemi, které jsou podobné aplikacím. To znamená, že model vyžaduje, aby operační systémy, aplikace a obsah byly spravovány a zabezpečeny cloudovým spotřebitelem. Nejjednodušší IaaS model je právě ten, který používá externí hardware k uložení měřených dat (obrázek 6.1 [5]).

Předpokládáme, že je zajištěna celistvost a autenticita dat a proto není třeba vyhodnocovat celý systém. Použití moderních podpisových algoritmů poskytuje tyto požadavky. Data posílaná do cloudu musí být zašifrována nebo alespoň podepsána měřicím nástrojem pomocí jeho soukromého klíče. V tomto případě může být cloudový systém považován za „black box“, protože nemůže měnit data bez detekce.

Orgány dozoru mohou kontrolovat a provádět testy prostřednictvím internetu. V takovém případě musí být klíče získány z infrastruktury veřejných klíčů (PKI), aby se zajistila správnost veřejného klíče. Každý měřicí přístroj a jeho data bude možné ověřit jedinečnou sadou veřejných a soukromých klíčů.

Dostupnost nelze zaručit. Je-li fakturační akce zpochybněna a data nelze extrahovat z cloudu, odpovědnost nese uživatel zařízení. Data v cloudu jsou obvykle lépe chráněna než na jednom měřicím přístroji [5].



Obrázek 6.1: Infrastructure as a Service v cloudu [5].

6.2 PaaS

PaaS model, ve kterém poskytovatel cloudu dodává výpočetní platformu, která obvykle obsahuje: operační systém, databázi a webový server. PaaS leží nad IaaS a přidává SW, který poskytuje aplikacím služby nad rámec poskytovaných operačním systémem (middleware). Zde ale samozřejmě se vyskytují stejné výzvy týkající se dostupnosti [5].

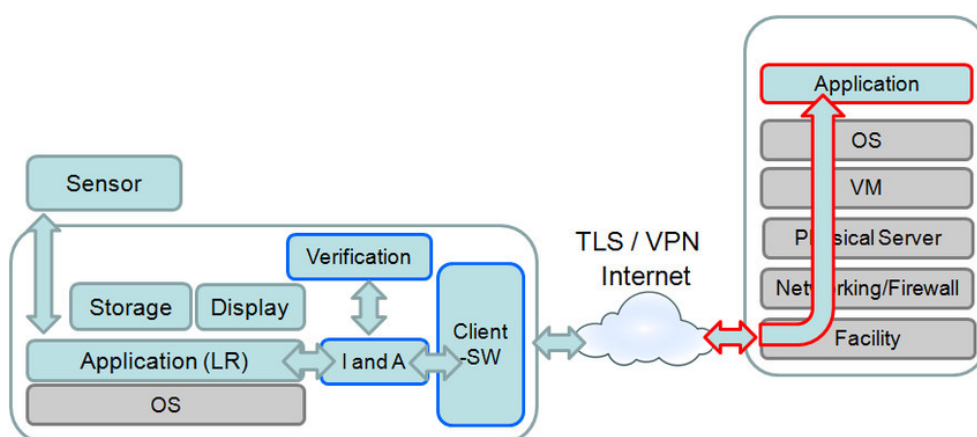
6.3 SaaS

SaaS model funguje jako přenos softwaru pro zpracování z přístroje do cloudu (obrázek 6.2 [5]). To znamená, že model umožňuje uživatelům připojit se ke cloudovým aplikacím a používat je přes internet. Veškerá podpůrná infrastruktura, middleware, software a data aplikace jsou umístěné v datovém centru poskytovatele služeb [38].

Připojení k aplikaci v cloudu by mělo probíhat přes internetový tunel. Například, vytvořit VPN pomocí protokolu TLS.

Nevýhodou SaaS v oblasti legální metrologie je, že se nedá důvěřovat jen cloudové infrastruktuře (viz 3.3.2.1). Proto klíčová ochrana je velmi důležitá.

Služby vzdáleného posuzování jsou rozhodující pro implementaci bezpečnostních řešení v cloudu. Všechny metriky spojené s VM (Virtual Machine) a jejich stavem jsou zachovány a porovnány s dřívějšími stavy úspěšného nasazení služby prostřednictvím samostatného serveru aterace, který stahuje očekávané programy pouze s předpokládanými konfiguračními soubory v očekávaném VM [5].



Obrázek 6.2: Software as a Service v cloudu [5].

Aplikace měřicích zařízení do cloudu

7.1 Systém

Návrh řešení pro metrologický SW je navrhován pro prostředí CC. Mezi funkce metrologické SW patří také ukládání, zobrazování, přenos a aktualizace dat. Z toho důvodu je nutné se zabývat i návrhem struktury databáze.

7.1.1 Splnění požadavek na SW dle Welmec Guide 7.2 pro měřicí zařízení typu U

Podle Welmec Guide 7.2 náš SW spadá do kategorie typu U a musí splňovat požadavky daného typu (viz 5.2.1.1):

- U1: Dokumentace

Dokumentace musí obsahovat:

- a. Popis funkcí softwaru: co to je za systém, jaký má význam, jaké má funkce.
- b. Popis přesnosti výpočetních algoritmů: principy výpočtu naměřených dat a principy výpočtu cen.
- c. Popis uživatelského rozhraní (viz 7.2).
- d. Označení softwaru: označení verze SW.
- e. Přehledné informace o hardwaru systému: jaký je výkon, načítání impulsu, zálohování dat.
- f. Přehled konfigurace použitého operačního systému, uplatněná pravidla bezpečnosti daného operačního systému: uživatelské účty, jejich práva.

– g. Operační manuál.

Dokumentace musí být přístupná a dohledatelná. Dokumenty mohou být umístěné na webových stránkách.

- U2: Označení softwaru

Legálně relevantní software musí být jasně označen. Označení musí být zobrazeno: trvale, na příkazu nebo během používání [37].

Označení může být ve tvaru řetězce čísel, písmen, jiných znaků. Řetězec může být doplněn číslem verze.

Označení určitého SW a verze může být uvedena jak na webu, tak i v samotném přístroji, když je k dispozici zobrazovací jednotka (například, LCD). V případě instalaci nového SW, které má nově funkce nebo mění se původní - musí být označena příslušná verze SW a musí být k dispozici dokumentace, popisující změny. V případě malého zásahu, například bug fixes, nemusí se měnit označení verze.

- U3: Vliv uživatelského rozhraní

Příkazy zadané přes uživatelské rozhraní nesmí nepřipustně ovlivňovat legálně relevantní software, specifické parametry přístroje ani naměřená data [37].

Data z uživatelského rozhraní může přijímat modul a filtrovat, falešné vstupy budou blokovány.

V našem případě uživatelské rozhraní nebude dovolovat manipulace s parametry a ani nebude umožněné měnit data. Uživatelé budou mít pouze "read only"(pouze čtení, bez možnosti zápisu/editace) přístup.

- U4: Vliv komunikačního rozhraní

Příkazy zadané přes komunikační rozhraní přístroje nesmí nepřipustně ovlivňovat legálně relevantní software, specifické parametry přístroje ani naměřená data [37].

Data z komunikačního rozhraní může přijímat modul, který ale jiným modulům bude předávat pouze povolené příkazy. Všechny jiné příkazy budou odmítnuty.

Stejně, jako u požadavku U3, pro uživatelé nebude umožněné měnit data, ale pouze číst.

- U5: Ochrana proti náhodným či neúmyslným změnám

Legálně relevantní software a specifické parametry přístroje musí být zabezpečeny proti náhodným či neúmyslným změnám [37].

Měl by být bezpečný přístup k SW: používat hesla a mechanismy pouze pro čtení; prostředků ochrany a práv na soukromí, které poskytuje operační systém nebo programovací jazyk.

Skoro každý moderní programovací jazyk umožňuje implementovat vysokou úroveň bezpečnosti a AWS taky umí řídit přístupy a má vysoké mechanismy zabezpečení. V rámci programu může být úplně zakázané mít jakákoliv jiná práva, než na čtení.

- U6: Ochrana proti záměrným změnám

Legálně relevantní software a naměřená data musí být zabezpečeny proti záměrným, nepřípustným modifikacím nebo nahrazení [37].

Kód programu může být zabezpečen uložením SW na jednoúčelovou přídatnou jednotku, která bude zajištěna plombou. Tato jednotka bude tvořena mikroprocesorem a pamětí chráněnou proti zápisu.

Pro případ manipulace s plombou nebo pokusu změnit data (včetně neúspěchu), SW může okamžitě odesílat upozornění na správce systému a zapisovat případ do logu.

- U7: Ochrana parametrů

Specifické parametry přístroje musí být po svém nastavení zabezpečeny proti nepovoleným změnám [37].

Specifické parametry budou uloženy přímo v jednotce snímače. Přepsání bude blokováno hardwarovým zaplombovaným prepínačem.

Stejně, jako u požadavku U6, pro pokus o přepsání může být vygenerované upozornění pro správce a proveden zápis do logu.

- U8: Prezentace naměřených dat

Musí být zaručena autentičnost prezentovaných naměřených dat [37].

Nerelevantním programům nebude umožněn přístup k naměřeným datům. Okno by se mělo aktualizovat a uživatel by neměl být schopen jej zavřít, dokud nebude dokončeno měření. Pokud bude okno během měření uzavřeno, zpracování bude zastaveno. Snímač bude šifrovat naměřené hodnoty klíčem známým SW na univerzálním počítači a pouze tento SW bude mít možnost hodnoty dešifrovat. Klíč bude hash kódem programu v univerzálním počítači a při každé změně bude vložen nový klíč, který nebude možné změnit bez porušení plomby.

- U9: Vliv jiného softwaru

Legálně relevantní software musí být navržen tak, aby ho nebylo možné nepřípustně ovlivnit jiným softwarem [37].

SW bude realizován nezávisle na operačním systému v aplikační doméně nebo SW moduly budou realizovány jako nezávislé objekty.

7.1.2 Splnění požadavků na SW dle Welmec Guide 7.2 pro rozšíření L, T, S a D

Podle Welmec Guide 7.2 náš metrologický SW musí splňovat požadavky na rozšíření L, T, D a S (tabulka 5.1).

Rozšíření L	Rozšíření T	Rozšíření S	Rozšíření D
Musí splňovat	Musí splňovat	Musí splňovat	Musí splňovat

Tabulka 7.1: Splnění podle typu rozšíření Welmec Guide 7.2

7.1.2.1 Dlouhodobé ukládání dat (rozšíření L, viz 5.3.1)

- L1: Úplnost uložených naměřených dat

Uložená naměřená data musí být doplněna všemi náležitými informacemi potřebnými pro legální účely [37].

Blok dat se musí skládat z naměřených hodnot, jednotek měření, ceny za jednotku, času měření, označení přístroje; místa měření. Data budou ukládána ve stejných hodnotách, jako bude indikováno při měření.

Data budou uložena na serveru AWS, což zaručuje dostatek místa.

- L2: Ochrana proti náhodným či neúmyslným změnám

Uložená naměřená data musí být chráněna proti náhodným a neúmyslným změnám [37].

Uložená data musí být doplněna informacemi, umožňujícími softwaru data načíst, vyhodnotit a zobrazit.

Data nebude možné mazat (s výjimkou starých dat, která musí být vymazána po několika letech). Přepsat naměřená data bude možné pouze když záznamy budou zabezpečené. Přepsaná data budou zálohována s vazbou na nová data.

Data budou vždy přístupná pro případ ověření.

- L3: Integrita dat

Uložená naměřená data musí být chráněna proti záměrným změnám [37].

Bude generován podpis přes hašovací a šifrovací algoritmus.

Přístupy a práva mazat a přepisovat mohou být realizována stejným způsobem, jako u L2.

- L4: Autentičnost uložených naměřených dat

Musí být možné věrohodně dohledat měření, při němž uložena naměřená data vznikla [37].

V bloku dat by měly být následující data: unikátní identifikační číslo; čas, kdy bylo měření provedeno; označení měřicího přístroje; podpis.

Náhled na data bude umožněn přes DB, která bude umístěna na serverech AWS. Vysoký výkon AWS může navíc zaručit hledání požadovaných údajů v obrovském objemu dat s dobrou rychlostí.

- L5: Utajení klíčů

S klíči a s informacemi s nimi souvisejícími musí být nakládáno jako s naměřenými daty. Musí zůstat v tajnosti a musí být chráněny proti odhalení [37].

Tajný klíč bude uložen v binární podobě a přes SW nebude možné ani zobrazit ani editovat tyto údaje.

- L6: Načtení, ověření a označení uložených dat

Zobrazovat nebo tisknout uložená naměřená data může pouze legálně relevantní software [37].

SW bude číst data a vypočítávat podpis celého datového bloku, který bude porovnán s nominální hodnotou. Když se data nebudou shodovat, systém je označí za poškozená.

Když systém označí data za poškozená bude možné zkontrolovat data a podívat se do datové historie a chybového logu, který může zaznamenávat nestandardní chování.

- L7: Automatické ukládání

Naměřená data musí být po skončení měření ukládána automaticky [37].

Naměřené hodnoty budou uloženy automaticky ihned po měření do datového bloku. Po skončení měření data budou předána a uložena na serveru AWS.

- L8: Kapacita paměti a kontinuita

Kapacita paměti pro dlouhodobé ukládání dat musí být pro zamýšlené účely dostatečná [37].

Měření by mělo být možné dokončit i tehdy, když bude paměť nedostupná díky dostatečně velké dočasné paměti. Hodnoty budou v dočasné paměti do chvíle, než mohou být přeneseny a do té doby nelze začít další měření. U měření, která nejde přerušit, není vyžadována dočasná paměť kvůli kumulativnosti údajů, které mohou být přeneseny do paměti, když bude k dispozici.

Když dojde k naplnění dočasné paměti, uživatel bude upozorněn zprávou na obrazovce zařízení. V případě, že zpráva bude ignorována, měření bude zastaveno a na displeji bude trvale zobrazené hlášení o chybě včetně kódového označení problémů.

Kapacita paměti cloudu AWS je obrovská, proto ten požadavek je již splněn od začátku.

7.1.2.2 Přenos naměřených dat komunikačními sítěmi (rozšíření T, viz 5.3.1)

- T1: Úplnost přenesených dat

Přenesená data musí obsahovat všechny odpovídající informace nutné k zobrazení či k dalšímu zpracování naměřených hodnot v přijímací jednotce [37].

Blok dat se musí skládat z naměřených hodnot; jednotky míry; jednotkové ceny; času měření; označení přístroje; místa měření.

Nejpopulárnější řešení je přenos velkého objemu dat na denní bázi pomocí dávek s zaarchivované soubory. Tato metoda běžně se používá v praxi.

- T2: Ochrana proti náhodným či neúmyslným změnám

Data musí být při přenosu chráněna proti náhodným a neúmyslným změnám [37].

SW by měl detekovat náhodné chyby během přenosu na základě kontrolních informací dat. Před použitím dat přijímač vypočte hodnotu kontrolního součtu a porovná ji s nominální hodnotou. Když se data nebudou shodovat, systém je označí za poškozená.

Když data budou označena za poškozená, musí být realizován přenos celého balíčku dat, který byl takto označen, nikoliv jen části.

- T3: Integrita dat

Naměřená data musí být při přenosu chráněna proti záměrným změnám [37].

Bude generován podpis a ochranu budou zajišťovat protokoly HTTPS a TLS.

- T4: Autentičnost přenesených dat

Musí být zajištěna autentičnost přenesených dat měření [37].

V bloku dat by měly být následující data: unikátní identifikační číslo; čas, kdy bylo měření provedeno; informace o původu naměřených dat. Datový blok bude opatřen podpisem a při příjmu bude kontrolována věrohodnost dat.

- T5: Utajení klíčů

Viz „L5: Utajení klíčů“ v 7.1.2.1

- T6: Zacházení s poškozenými daty

Data, u nichž bylo zjištěno poškození, musí být označena, aby je software, který je bude dále zpracovávat, rozpoznal a mohl náležitě zareagovat [37].

Pokud bude nesoulad mezi zaslanými daty a kontrolní hodnotou, program se pokusí obnovit původní hodnotu. V případě neúspěchu program vygeneruje upozornění a blok bude označen jako neplatný.

Neplatný blok musí být celý zaslán ještě jednou.

- T7: Zpoždění při přenosu

Měření nesmí být nepřípustně ovlivněno zpožděním při přenosu [37].

Přenos bude prováděn po skončení měření. V případě zpoždění přenosu se vytvoří o tom záznam. V případě delšího zpoždění budou data ignorována, vytvořen záznam a naměřená data budou přijata jako validní s následujícím balíčkem dat, kde zpoždění přenosu bude v povoleném časovém limitu.

- T8: Dostupnost přenosových služeb

V případě nedostupnosti služeb sítě nesmí dojít ke ztrátě naměřených dat [37].

Viz „L8: Kapacita paměti a kontinuita“ v 7.1.2.1

7.1.2.3 Oddělení softwaru (rozšíření S, viz 5.3.1)

- S1: Realizace oddělení softwaru

Část softwaru obsahující legálně relevantní software a parametry musí být jednoznačně oddělená od ostatních částí softwaru [37].

To je možné realizovat na úrovni programního kódu. Část programu může být realizována pomocí privátních a chráněných metod.

- S2: Smíšená indikace

Informace generované legálně nerelevantním softwarem musí být na displeji nebo tištěném výstupu zobrazeny či uvedeny tak, aby nemohlo dojít k jejich záměně s informacemi generovanými legálně relevantním softwarem [37].

Legálně relevantní informace musí procházet filtrem pro ověření, zda informace ze vstupu byly extrahovány a filtr musí detekovat nepřípustné informace.

- S3: Ochranné rozhraní softwaru

Výměna dat mezi legálně relevantním softwarem a legálně nerelevantním softwarem musí probíhat výhradně přes ochranné rozhraní [37].

V programu datové domény legálně relevantní části SW budou deklarované lokálními proměnné. Rozhraní bude podprogram a data budou přenášena jako parametry podprogramu. SW bude filtrovat nepřipustné příkazy rozhraní.

Když legálně relevantní SW bude muset zobrazit data z legálně nerelevantního SW, pak taková data budou mít automaticky přiřazen příznak, se kterým se pak zobrazí uživateli.

7.1.2.4 Stahování legálně relevantního softwaru (rozšíření D, viz 5.3.1)

- D1: Mechanismus stahování

Obě etapy stahování softwaru, přenos i následná instalace softwaru, musí probíhat automaticky a bez vlivu na zabezpečení legálně relevantního softwaru [37].

Pokud chce být SW aktualizován, musí být nejprve schválen oznámeným subjektem. Pak může dojít ke stahování softwaru.

Celý proces stahování a instalace může být popsán v pěti krocích:

- Kontrola na úrovni SW, když balík pro instalaci je od výrobce.
- Přenos dat a následující kontrola, když balík pro instalaci nebyl porušen během přenosu a že přenos proběhl úspěšně a bez chyb.
- Instalace.
- Kontrola instalace. Když instalace spadne, pak SW nebude aktualizován.
- Inicializace nového SW a aktualizace verze.

- D2: Prokázání věrohodnosti přeneseného softwaru

Je třeba implementovat prostředky zaručující autentičnost přeneseného softwaru [37].

Bude generován elektronický podpis části SW, která má být stažena. Klíč musí potvrdit vytvoření podpisu autorizovaným orgánem.

Typ přístroje bude automaticky porovnán s označeným typem v seznamu přístrojů SW.

- D3: Integrita stahovaného softwaru

Je třeba použít prostředky zabráňující změně softwaru při přenosu [37].

Integritu bude možné ověřit přepočtem kontrolního součtu a porovnáním výsledku s kontrolním součtem skrytým v SW. Když součty nebudou shodovat, SW bude označen za poškozený a nebude možné ho instalovat.

- D4: Návaznost stahovaného legálně relevantního softwaru

Za účelem následných kontrol musí být v přístroji zajištěna odpovídajícími technickými prostředky zpětná návaznost a dohledatelnost stahovaných legálně relevantních softwarů [37].

Přístroj bude automaticky zaznamenávat minimálně datum a čas stahování. Záznam o stahování bude vytvořen při každém pokusu. Po dosažení limitu kapacity bude zabráněno dalšímu stahování SW.

Data o stahování budou uložena ne jen v samotném přístroji, ale i v DB. Příslušná stahování budou přidávána i do logu.

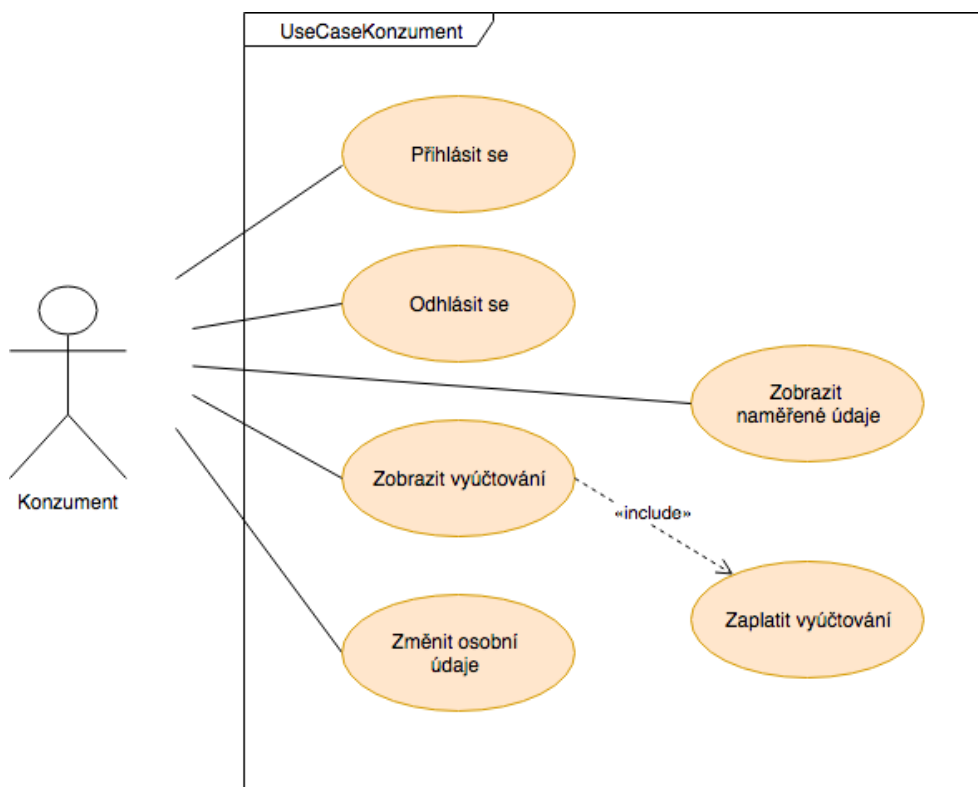
7.2 Funkcionalita uživatelského rozhraní

Systém bude mít uživatelské rozhraní pro zobrazení dat, ve kterém bude pro spotřebitele, kontrolní orgán, poskytovatele energií a výrobce k dispozici několik funkcí. Funkcionalitu systému popíšeme pomocí use case diagramu.

7.2.1 Spotřebitel (konzument)

Konzument bude mít následující funkcionalitu (obrázek 7.1):

- Přihlásit se
Pokud přihlašovací údaje jsou správné, proběhne přihlášení uživatele.
Pokud přihlašovací údaje nejsou správné, bude zobrazena hláška o chybných údajích a bude možné zadat údaje ještě jednou.
- Odhlásit se
Systém odhlásí uživatele.
- Zobrazit naměřené údaje
Zobrazí naměřené údaje u daného uživatele.
- Zobrazit vyúčtování
Zobrazí dokumenty typu vyúčtování.
- Zaplatit vyúčtování
Bude možné zaplatit vyúčtování.
- Změnit osobní údaje
Bude možné změnit osobní údaje.



Obrázek 7.1: Use case diagram: Konzument.

7.2.2 Kontrolní orgán

Kontrolní orgán bude mít k dispozici všechny informace o měřicím přístroji: certifikáty, event loggery, změny v přístroji a bude mít možnost vydávat povolení k aktualizaci SW. Kontrolní orgán bude mít následující funkcionalitu (obrázek 7.2):

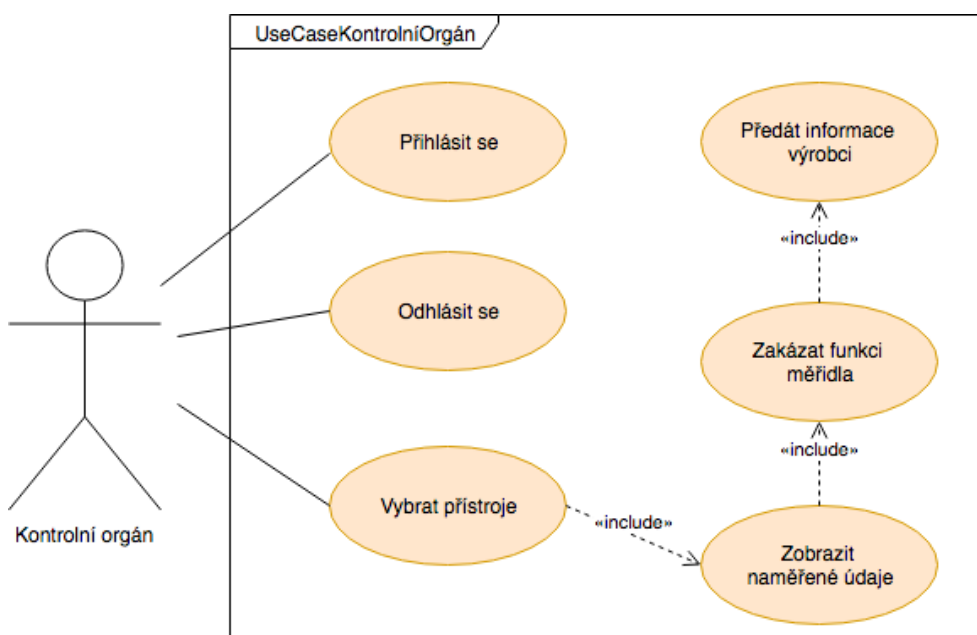
- Přihlásit se
Viz „Přihlásit se“ v 7.2.1.
- Odhlásit se
Viz „Odhlásit se“ v 7.2.1.
- Vybrat přístroje
Bude možné vybrat přístroje, jejichž data kontrolní orgán bude chtít zkontrolovat.
- Zobrazit naměřené údaje
Viz „Zobrazit naměřené údaje“ v 7.2.1.

- Zakázat funkci měřidla

Když kontrolní orgán zjistí, že měřicí zařízení měří špatně, může zakázat funkci měřidla.

- Předat informace výrobci

Bude možné předat výrobci informace, že musí udělat opravu.



Obrázek 7.2: Use case diagram: Kontrolní orgán.

7.2.3 Výrobce

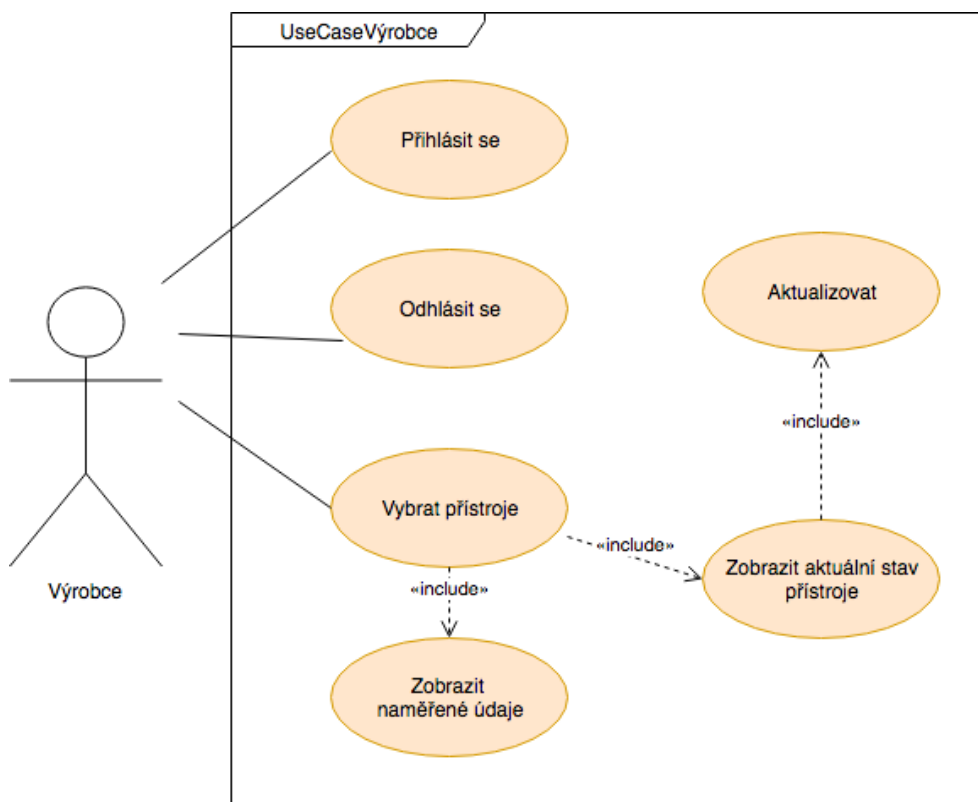
Výrobce bude zodpovědný za celou funkčnost měřidla a měl by mít přístup ke komunikaci a přenosu údajů. Výrobce nesmí ovlivnit kalibrační procesy, nesmí mazat naměřené údaje. Pokud dostane svolení od kontrolního orgánu, může provést aktualizaci SW. Výrobce bude mít následující funkcionalitu (obrázek 7.3):

- Přihlásit se

Viz „Přihlásit se“ v 7.2.1.

- Odhlásit se

Viz „Odhlásit se“ v 7.2.1.

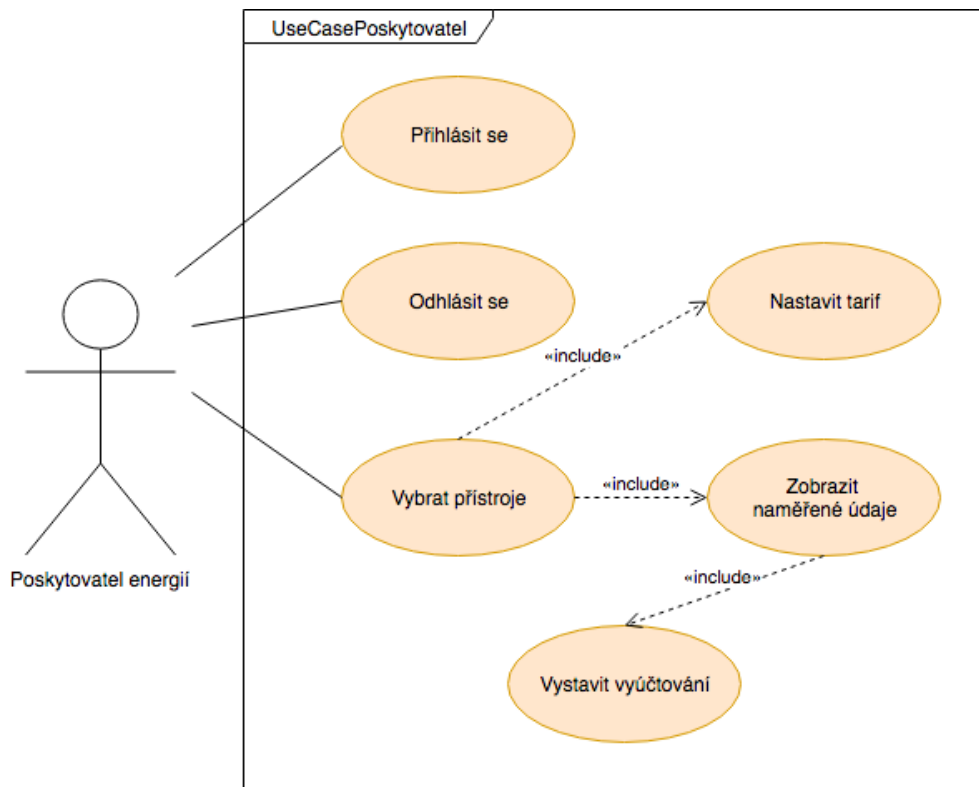


Obrázek 7.3: Use case diagram: Výrobce.

- **Vybrat přístroje**
Bude možné vybrat přístroje, jejichž data bude chtít výrobce zkontrolovat.
- **Zobrazit naměřené údaje**
Viz „Zobrazit naměřené údaje“ v 7.2.1.
- **Zobrazit aktuální stav přístroje**
Zobrazí aktuální stav přístroje.
- **Aktualizovat**
Bude možné aktualizovat moduly SW na základě žádosti od kontrolního orgánu.

7.2.4 Poskytovatel energií

Poskytovatel energií bude provádět montáž na odběrní místo, nastavovat tarify a databáze měřicích zařízení. Poskytovatel bude zodpovědný za vyúčtování a bude mít následující funkcionalitu (obrázek 7.4):



Obrázek 7.4: Use case diagram: Poskytovatel energií.

- Přihlásit se
Viz „Přihlásit se“ v 7.2.1.
- Odhlásit se
Viz „Odhlásit se“ v 7.2.1.
- Vybrat přístroje
Viz „Vybrat přístroje“ v 7.2.3.
- Nastavit tarif
Bude možné nastavit tarify.
- Zobrazit naměřené údaje
Viz „Zobrazit naměřené údaje“ v 7.2.1.
- Vystavit vyúčtování
Bude možné vystavit vyúčtování.

7.3 Databáze

Základní databázový model bude obsahovat: informace o osobách; role; měřicí zařízení; naměřené údaje, za které spotřebitel zaplatí; vyúčtování; logy. Příklad ER (Entity-Relationship) modelů s popisem jednotlivých prvků je na obrázku 7.5.

- Informace o osobách

Databáze by měla obsahovat data o osobách. Osobu reprezentuje entita User (obrázek 7.5). Každá osoba má:

- UsedId: Unikátní identifikátor uživatele.
- Name: Jméno uživatele.
- Surname: Příjmení uživatele.
- BirthNumber: Rodné číslo uživatele.
- Adress: Adresa uživatele.
- Email: E-mail uživatele.
- Phone: Telefonní číslo uživatele.

- Role

Každá osoba má přidělenou roli (obrázek 7.5). Role mají různá oprávnění pro práce v systému.

- RoleId: Unikátní identifikátor uživatelské role.
- Name: Název role.
- Authorization: Oprávnění role.

- UserRole

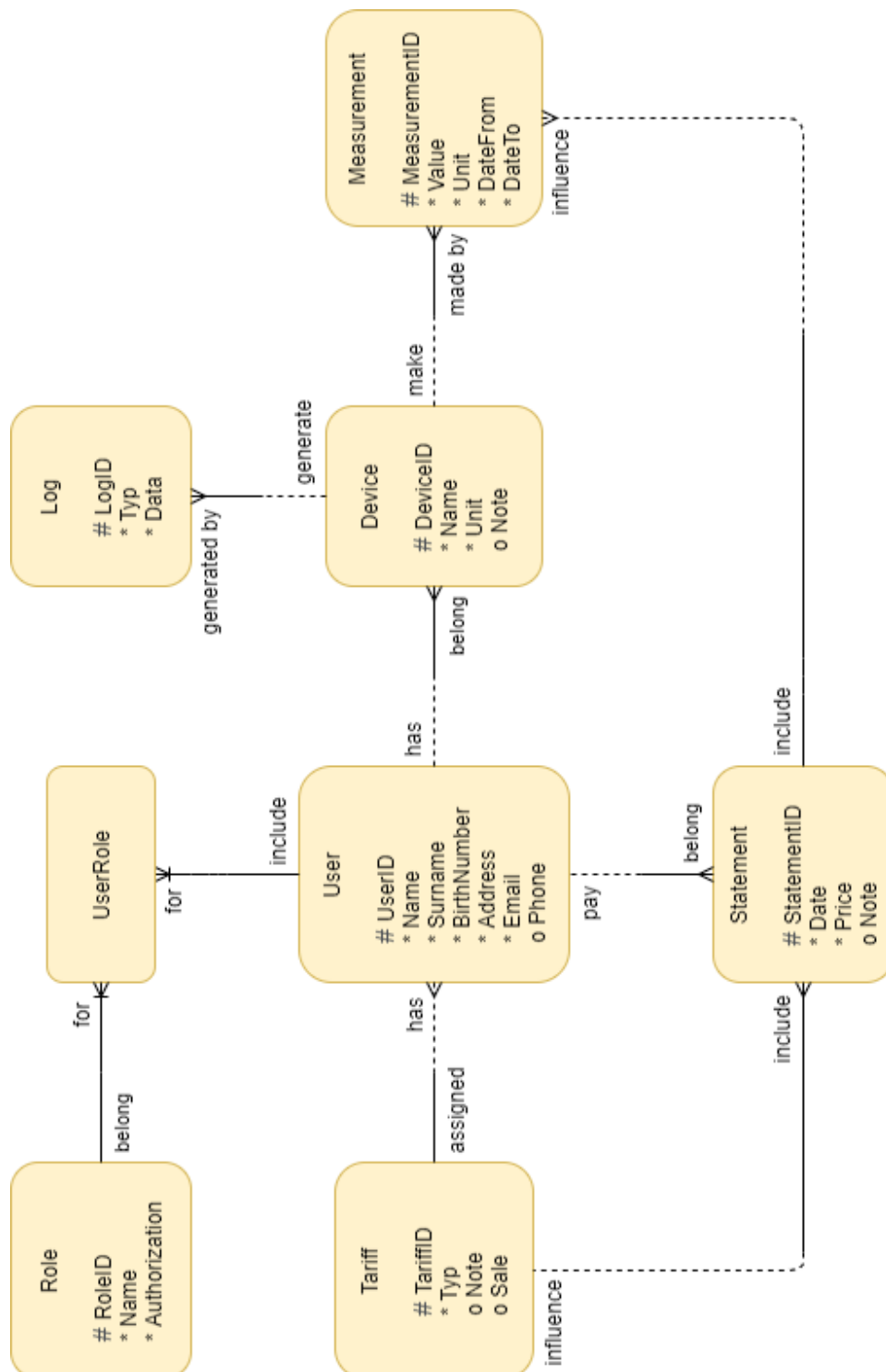
UserRole je entita, která řeší vazbu M:N a má:

- UserId: Unikátní identifikátor uživatele.
- RoleId: Unikátní identifikátor uživatelské role.

- Měřicí zařízení

Databáze bude obsahovat informace o měřicích zařízeních. Přístroj reprezentuje entita Device (obrázek 7.5). Každý přístroj má:

- DeviceId: Unikátní identifikátor měřicího přístroje.
- Name: Název přístroje.
- Unit: Měřicí jednotka.
- Note: Doplnující informace o zařízení. Například, verze SW.



Obrázek 7.5: Databázový model.

- Vyúčtování

Vyúčtování reprezentuje entita Statement (obrázek 7.5). Každé vyúčtování má:

- StatementId: Unikátní identifikátor vyúčtování.
- Date: Datum vyúčtování.
- Price: Cena vyúčtování.
- Note: Doplnující informace.

- Měření

Naměřené údaje reprezentuje entita Measurement (obrázek 7.5) a entita má:

- MeasurementId: Unikátní identifikátor naměřených údajů.
- Value: Hodnota naměřených údajů.
- Unit: Měřicí jednotka.
- DateFrom: Datum.
- DateTo: Datum.

- Tarif

Tarif reprezentuje entita Tariff (obrázek 7.5):

- TariffId: Unikátní identifikátor tarifů.
- Type: Typ tarifů.
- Note: Doplnující informace.
- Sale: Možná hodnota slevy.

- Log

Databáze bude obsahovat logy (obrázek 7.5). Logy obsahují následující informace:

- LogId: Unikátní identifikátor logu.
- Type: Request nebo response.
- Data: Data reprezentující req. nebo resp., případně error zprávy.

7.3.1 Vytvoření databáze v AWS

Vytvoření databáze v AWS je jednoduchý proces pomocí Amazon RDS (viz 3.3.1). Celý proces lze popsat v několika krocích:

- Vytvoření instance databáze MySQL

- Stahování SQL klienta
- Připojení k databázi MySQL

Pokud instance již není potřeba, lze ji snadno odstranit. Amazon doporučuje odstraňovat nepoužívané instance, aby nebyly účtovány [39].

7.3.2 Migrace databází na platformu AWS

Pomocí AWS Database Migration Service lze snadno a bezpečně přenést databáze na platformu AWS. Zdrojová databáze zůstává plně funkční během procesu migrace, což minimalizuje prostoje aplikací, které ji používají. Služba podporuje přímou migraci a migraci mezi různými databázovými platformami s konverzí. Existuje možnost kombinace a pohodlné analýzy dat, jejichž objem může být měřen petabyty. Pro migrace není třeba instalovat žádné ovladače nebo aplikace a není třeba provádět změny původní databáze.

Migrace databáze má dobrou cenu. Například, migrace jednoho terabajtu stojí 3 USD (cena je platná pro květen roku 2018) [40].

7.4 Bezpečné připojení k AWS službám

Interní průmyslové sítě jsou dobře zabezpečeny. Problém ale je s rozšířením sítě o přístroje, které nemají vysoký výkon pro složité bezpečnostní algoritmy. Proto připojená zařízení mají velký počet hrozeb a je nezbytné zavést další bezpečnostní opatření.

7.4.1 Internet of Things a AWS

Internet of Things (IoT) - síť fyzických zařízení a spotřebičů, která jsou vybavena elektronikou, senzory, SW a síťovou konektivitou. Potom zařízení jsou navzájem propojena a mohou vyměňovat si data [41].

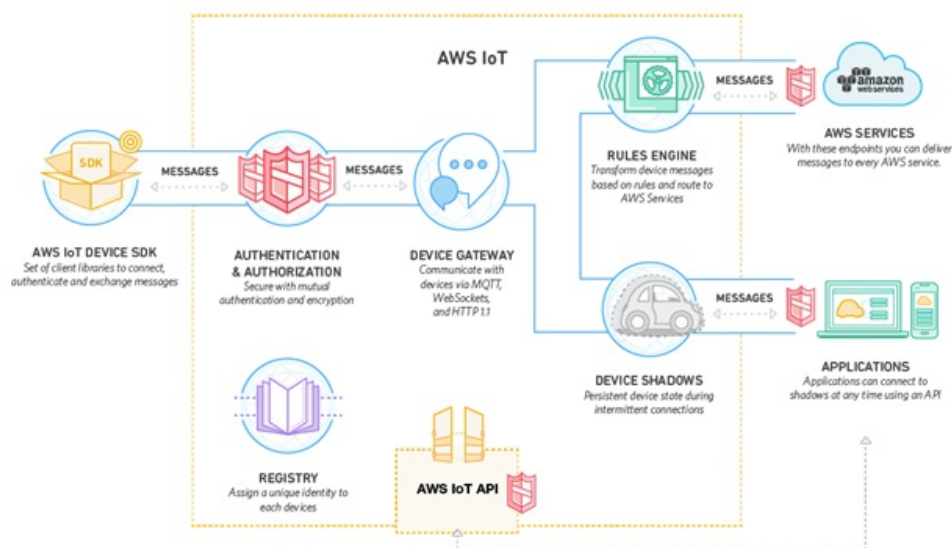
Vestavěné zařízení a Cloud se používají specifické bezpečnostní protokoly, které provádí vzájemnou autentizaci a autorizaci pro přístup k CC službám. Protokoly jsou většinou součástí služby, která je poskytnuta IoT portálem.

AWS poskytuje speciální portál, který vestavěné zařízení musí použít pro připojení. Vestavěné zařízení připojují se pomocí vzájemného ověřování s bránou zařízení a pak brána propojuje přístroj s dalšími službami IoT. Zařízení má unikátní identifikátor. AWS IoT poskytuje službu, která udržuje data o stavu v virtuálním zařízení spojeném s fyzickým zařízením IoT. Amazon tomu říká - poskytování stínů (obrázek 7.6 [4]).

7.4.2 Připojení k IoT portálu

Vestavěné zařízení musí mít soukromý klíč a certifikát. Doklady o totožnosti přístrojů jsou poskytované IoT portálu pomocí tokenů nebo klíčů s certi-

7. APLIKACE MĚŘICÍCH ZAŘÍZENÍ DO CLOUDU

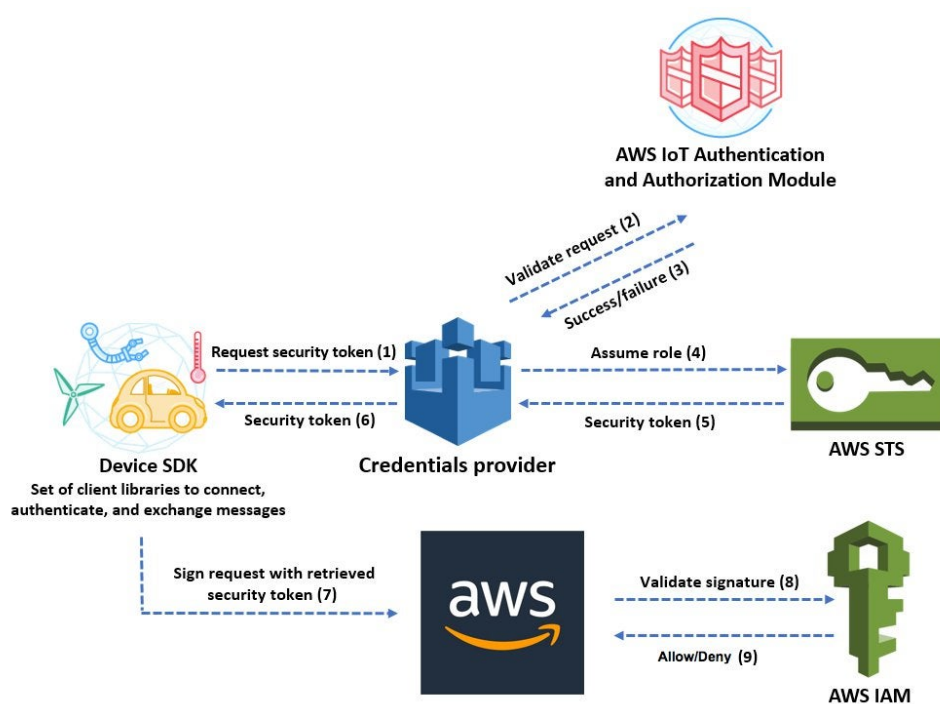


Obrázek 7.6: AWS IoT [4]

fikátem. IoT portál navíc potřebuje definici přístupových práv pro komunikace. Služby AWS podporují ne jen ověřování pomocí certifikátů, ale ještě autentizační metody pomocí tokenů na základě JWT (JSON Web Token). Registry používají se k ukládání metadat pro každé připojené zařízení a přístupových práv pro entity a komunikační kanály [4].

AWS má služby, které podporují dynamické poskytování autentizačních tokenů pomocí funkce AWS Lambda. Modul AWS pro autentizaci a autorizaci IoT schvaluje žádost o token a služba STS (Security Token Service) generuje token, pomocí kterého systémy mají možnost přistupovat ke službám AWS. (obrázek 7.7). Podobná služba je pro dynamické přidělování přístupových práv.

AWS IoT nabízí funkce zajištění bezpečnosti pro celé flotily zařízení [4].



Obrázek 7.7: AWS Security Token Service [4]

Trh a Cloud

8.1 Cloud v průmyslové výrobě

Průmyslové společnosti využívají Cloud s každým rokem více a více. Cloud je jednou z technologických inovací, společně s Big Data a Machine Learning, které jsou základem nové generace. Dále se podíváme na existující nejpopulárnější způsoby využití Cloudu ve výrobě na trhu [42].

Industrial Internet of Things

Jedním ze způsobů využití CC je IIoT (Industrial Internet of Things). Senzory jsou nasazené na výrobní prostředky s telemetrií, která slouží pro přenos dat do Cloudu pro ukládání, aplikace a analytiků. Jedná se o velmi populární pojem ve výrobě. IIoT propojuje stroji s lidí, ukládá a předává velké množství dat. IIoT umožňuje implementovat autonomnější a chytřejší zařízení a dává možnost těmto zařízením spolu komunikovat. Výhody IIoT:

- Monitorování výroby v reálném čase
- Vzdálená správa strojů
- Údržba
- Lepší rozhodování
- Autonomní manipulace s materiálem
- Zvýšení efektivity na základě analýzy dat [43].

Přesun datových skladů

Dalším způsobem využití CC jsou virtuální stroje. Jeden fyzický server může hostit mnoho virtuálních strojů, které provozují mnoho aplikací. Díky tomu se zlepšuje využití hardwaru.

Základní motivace k přesunu je úspora. Náklady na server mohou být 50 krát vyšší než cena samotného serveru. Amazon doporučuje společností se

zaměřit na „datové centrum o rozloze nula metrů čtverečních“, což znamená mít datové centrum se všemi aplikacemi běžícími v Cloudu.

Datová jezera

Datové jezero znamená uplatnění různých typů dat v jednom systému. Tento přístup umožňuje nalezení nových znalostí pro zlepšení výroby a obchodních procesů. Nevýhodou je vysoké náklady (jak časové tak i finanční) na implementaci.

Cloud přehledové systémy

Systémy umožňují přístup k různým datům pro účely analytiky a statistiky. Data mohou odpovídat na definované dotazy pro odborníky mimo výrobu.

Rychlá analytika

Týká se to aplikačního modelu SaaS. Uživatelé mají možnost přistupovat k analytice lokálně nebo přes cloudu bez žádného zásahu IT. Je možné tohle všechno dělat vůbec bez nutnosti přesunutí, kopírování a ukládání záznamů. Nevýhodou často je nutnost platit za SW licence [42].

8.2 Role metrologie pro digitalizaci a ekonomiku

Hlavním pilířem efektivní kvalitní infrastruktury je schopnost získat platná data založená na vysoce přesných měřeních - což je součástí metrologie. Ekonomika a společnosti 21. století je v procesu komplexní digitální transformace. Digitalizace je proces zavádění využívání digitálních technologií v nejrůznějších oblastech výroby i života společnosti [44]. Rozvoj výpočetních a úložných kapacit, rychlost výměny dat, dostupnost univerzálních senzorů otevírají zcela nové možnosti.

Kvalitní infrastruktura skládající se z metrologie, standardizace, akreditace a legální metrologie měla by se posílit, protože je předpokladem úspěšné digitální transformace do vzájemně propojené ekonomiky, průmyslu a společnosti. Německý národní metrologický institut Physikalisch-Technische Bundesanstalt (PTB) je jedním z největších hráčů, který se aktivně zabývá implementací digitalizačních technologií. PTB hlavně se zabývá:

- Vývojem a ověřováním postupů měření zajišťujících nejvyšší přesnost
- Implementaci algoritmů a metod datové analýzy
- Validaci naměřených dat a jejich převodem do mezinárodního systému jednotek (SI) [45].

Několik velkých skupin po celém světě, společně s veřejnými institucemi a soukromými ekonomickými partnery se vyvíjí regulační a administrativní základy pro oblasti Cloud Computingu, Big Data, bezpečnosti IT, Machine Learning a dlouhodobě budují metrologický základ pro vývoj vysoce výkonných komunikačních kanálů 5G. UK se také silně rozvíjí oblast 5G sítě a výzkum

související s digitalizací. PTB samozřejmě bude odpovídajícím způsobem rozvíjet své kapacity, aby být jedním z předních světových metrologických institutů a vést digitální transformaci a rozšíření metrologie [45].

Covid-19

COVID-19 má taky dopad na růst Cloud Computingu. Na základě průzkum společnosti Flexera s cílem odpovědět na otázku, jak pandemie ovlivnila růst CC bylo zjištěno, že z 187 respondentů více než polovina uvedla, že využití Cloudu je výrazně větší, než se očekávalo. Zejména díky dalším požadavkům na IT potřebné k uspokojení poptávky zákazníků [46].

8.3 Statistika Cloud Computing na trhu

Statistika CC ukazují stále exponenciální růst průmyslu. V roce 2010 byla překročena hranici 100 miliard dolarů a do konce roku 2020 měla by být dosázená hranice 150 miliard dolarů. Budoucnost CC je jasná. Očekává se, že příjmy z tohoto sektoru do roku 2022 vzrostou na 331 miliard dolarů. Podle výzkumu sledujícího 600 mezinárodních podniků je vidět rychlý růst v přijímání CC velkými společnostmi. Hlavně proto, že podniky postupně zavádějí provoz mimo kancelář a je nezbytným řešením propojení zaměstnanců a sdílení informací prostřednictvím sítě [46].

Statistika a čísla (data jsou platná pro rok 2020)

- Lídrem na trhu v roce 2020 je stále AWS s podílem 32%
- Nejrychlejší rostoucí segment cloudových platforem je model PaaS (Platform-as-a-service)
- Podle IDC (International Data Corporation) jsou tři sektory, které plánují utratit nejvíce za služby Cloud Computingu: výrobní průmysl (19,7 miliard dolarů), profesionální služby (18,1 miliardy dolarů) a bankovníctví (16,7 miliardy dolarů)
- 84% podniků popisuje svoji IT infrastrukturu jako „více Cloudů“
- 80% společností hlásí zlepšení provozu během prvních několika měsíců od přijetí této technologie
- AWS přineslo Amazonu obrovské výnosy ve výši 25,66 miliard dolarů a to je pouze v roce 2018
- Na konce roku 2020 bude 67% IT infrastruktury a softwaru založeno na Cloudů
- Každý nový Cloudový server má kapacitu hostovat 600 smartphonů a 120 tabletů

8. TRH A CLOUD

- Cloud bude do konce roku 2020 obsahovat více než 40 zettabytů informací
- Nejoblíbenější CC službou je úložiště iCloud a taky Dropbox. Pouze tyto bezplatné platformy mají kolem 300 miliony uživatelů [46]

Přínosy

9.1 Aktuální stav

Přechod metrologie do Cloud computingu samozřejmě má smysl a přináší řadu výhod. Zatím CC je ještě stále rozvíjející se obor. Většina velkých společností, včetně státních, začínají využívat služby CC.

Aktuálně firmy, zabývající se měřením, jsou nuceny kupovat tisíce měřících zařízení za velké peníze. Cloud computing může zbavit firmy od takových už zbytečných ztrát.

V posledních letech ceny za služby AWS rychle klesají. Snížení cen za poslední tři roky bylo v průměru o 58% ročně. Celkově zde existuje tendence nejen k výraznému poklesu cen, ale také ke značnému zvýšení kapacity (vyšší ECU a více RAM), což je ještě lepší pro zákazníka [47]. Taková tendence je pravděpodobně díky příchodu mnoha nových poskytovatelů služeb CC.

Je ale nezbytné uvést, že i když technologie CC je už využívána, některé legislativní zákony v oblasti legální metrologií ji nemusejí povolit.

9.2 Perspektivy

Cloud computing ještě není úplně zaveden v legální metrologii a proto máme více perspektiv a možností (viz 8.3). Realizace modelu IaaS pomůže přenést metrologické SW do cloudu. Spotřebitel CC bude mít všechno pod kontrolou, protože v daném typu modelu pouze používáme externí hardware. Operační systém, obsah a SW bude mít na starosti spotřebitel CC.

Hotový model IaaS bude možné rozšířit a vytvořit ještě modely PaaS a SaaS. Samozřejmě to přinese několik dobrých možností, hlavní z nich je možnost prodávat hotový SW. V tom případě kupující bude mít hotový produkt, ale starat se o správu a bezpečnost bude prodávající. Tohle ovšem nabízí nové produkty a služby na trhu, jako jsou například prodej licence na SW, podpora a údržba SW.

9.3 AWS

Amazon je největší poskytovatel cloudu s dobrou pověstí. Aktuálně AWS má největší spektrum funkcí a největší množství uživatelů [12].

Ceny na objektové úložiště (viz Amazon S3 3.3.1) jsou závislé na regionu a na použitém objemu dat. Například, ceny pro region Frankfurt (tabulka 9.1 [6]).

Úložiště	Cena
První 50 TB v měsíci	0.0245\$ za GB
Další 450 TB v měsíci	0.0235\$ za GB
Více než 500 TB v měsíci	0.0225\$ za GB

Tabulka 9.1: S3 Standard Storage [6].

Ceny jsou platné pro listopad roku 2020.

9.4 Bezpečnost

Poskytovatel cloudu AWS nabízí mnoho služeb zabezpečení (viz 3.3.2). Samozřejmě ale je nutné starat se o bezpečnost (viz 2.4 a 7.4).

Důležité je pravidelně zálohovat data, aby v nějakém neočekávaném případě ztráty dat (i když je to málo pravděpodobné) byla nejaktuálnější záložní verzi. Na základě toho, že zákazníků a jejich naměřených dat bude velmi mnoho, bude ideální provádět zálohování každých 12 hodin.

Když budou splněna všechna doporučení podle Welmec Guide 7.2, použity služby zabezpečení od AWS, budou šifrovaná data a pravidelně prováděná zálohování - bezpečnost bude na velmi vysoké úrovni.

Závěr

Cílem bakalářské práce bylo analyzovat problémy implementace metrologického SW v CC v kategoriích, jako: komunikace, dlouhodobé ukládání dat, download SW podle pravidel Welmec Guide 7.2.

V teoretické části byl vypracován stručný přehled platforem CC a byl zvolen vhodný poskytovatel pro realizaci bakalářské práce. Také byly specifikovány vlastnosti měřicího zařízení podle Welmec Guide 7.2.

V praktické části byla provedena analýza a popis možností zabezpečení a ukládání dat pro metrologický SW v CC v souladu s Welmec Guide 7.2. Také byla navrhována vhodná architektura pro aplikaci (SW) reprezentující měřicí zařízení na základě Welmec Guide 7.2. V kapitole 7.2 je návrh pro funkcionalitu uživatelského rozhraní s use case diagramy a příkladem základních vlastností databáze s ER modelem. Byla provedena analýza trhu a možnosti využití CC v průmyslové výrobě a role metrologii pro ekonomiku.

Osobním přínosem bylo rozšíření teoretických znalostí v oblasti Cloud computing, metrologie a oboznámení se s pravidly Welmec Guide 7.2 zabývající se postupem pro validaci SW pro legální metrologii. Přínosem praktické části byla možnost využít znalosti získané během studia a zlepšit si analytické schopnosti na reálném projektu.

Přechod legální metrologie do CC bude mít smysl a přinese celou řadu výhod jak pro spotřebitele tak i pro poskytovatele (viz 9).

Literatura

- [1] Deepak Sharma: Cloud Computing : Everything You Need To Know About Cloud. In: *Cloudmyinfo.com* [online]. December 2017, [citováno 21. 04. 2018]. Dostupné z: <https://cloudmyinfo.com/cloud-computing/>
- [2] Synergy Research Group: Cloud Growth Rate Increases; Amazon, Microsoft & Google all Gain Market Share. In: *Srgresearch.com* [online]. February 2018, [citováno 11. 04. 2018]. Dostupné z: <https://www.srgresearch.com/articles/cloud-growth-rate-increases-amazon-microsoft-google-all-gain-market-share>
- [3] Amazon Web Services: Security, Identity & Compliance. In: *Aws.amazon.com* [online]. [citováno 17. 09. 2020]. Dostupné z: <https://aws.amazon.com>
- [4] Stephen Evanczuk, Digi-Key: Bezpečnost IoT - část 5: Bezpečné připojení ke cloudovým službám In: *vyvoj.hw.cz* [online]. September 2020, [citováno 14. 10. 2020]. Dostupné z: <https://vyvoj.hw.cz//bezpecnost-iot-cast-5-bezpecne-pripojeni-ke-cloudovym-sluzbam.html>
- [5] F. Thiel, M. Esche, D. Peters, U. Grottker: Cloud Computing in Legal Metrology. In: *Cfmetrologie.edpsciences.org* [online]. [citováno 25. 04. 2018]. Dostupné z: https://cfmetrologie.edpsciences.org/articles/metrology/pdf/2015/01/metrology_metr2015_16001.pdf
- [6] Amazon Web Services: Amazon S3 Pricing. In: *Aws.amazon.com* [online]. [citováno 10. 11. 2020]. Dostupné z: <https://aws.amazon.com/s3/pricing/>
- [7] Ing. Jakub Slavík, MBA: Co to je a jak funguje inteligentní město – smart city. In: *Novinky – elektrotechnika elektronika energetika průmyslová automatizace* [online]. 27.1.2015. [citováno 10. 04. 2018]. Dostupné z: <http://www.proelektrotechniky.cz/vzdelavani/38.php>

- [8] Arif Mohamed: A history of cloud computing. In: *Computerweekly.com* [online]. [citováno 21. 03. 2018]. Dostupné z: <https://www.computerweekly.com/feature/A-history-of-cloud-computing>
- [9] Kolektiv autorů Abacusnext.com: What's the Difference between Public, Private, Hybrid, and Community Clouds? In: *Abacusnext.com* [online]. January 2017, [citováno 28. 03. 2018]. Dostupné z: <https://www.abacusnext.com/blog/whats-difference-between-public-private-hybrid-and-community-clouds>
- [10] Microsoft: What is cloud computing? In: *Azure.microsoft.com* [online]. [citováno 27. 03. 2018]. Dostupné z: <https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/>
- [11] Mark Brinda, Michael Heric: The Changing Faces of the Cloud. In: *Bain.com* [online]. [citováno 14. 04. 2018]. Dostupné z: http://www.bain.com/Images/BAIN_BRIEF_The_Changing_Faces_of_the_Cloud.pdf
- [12] Jake, Marketing: Microsoft Azure vs AWS: Cloud Comparison Guide [2018 Update]. In: *Redpixie.com* [online]. March 2018, [citováno 10. 04. 2018]. Dostupné z: <https://www.redpixie.com/blog/microsoft-azure-aws-guide>
- [13] Microsoft: Azure pricing. In: *Azure.microsoft.com* [online]. [citováno 20. 04. 2018]. Dostupné z: <https://azure.microsoft.com/en-us/pricing/>
- [14] Amazon Web Services: AWS Pricing. In: *Aws.amazon.com* [online]. [citováno 20. 04. 2018]. Dostupné z: https://aws.amazon.com/pricing/?nc1=h_ls
- [15] Microsoft: Azure pricing. In: *Azure.microsoft.com* [online]. [citováno 20. 04. 2018]. Dostupné z: <https://azure.microsoft.com/en-us/global-infrastructure/regions/>
- [16] Amazon Web Services: AWS Global Infrastructure. In: *Aws.amazon.com* [online]. [citováno 20. 04. 2018]. Dostupné z: https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h_ls
- [17] Amazon Web Services: AWS Customer Success. In: *Aws.amazon.com* [online]. [citováno 25.03. 2018]. Dostupné z: https://aws.amazon.com/solutions/case-studies/?nc1=h_ls
- [18] Amazon Web Services: Amazon EC2. In: *Aws.amazon.com* [online]. [citováno 15. 04. 2018]. Dostupné z: https://aws.amazon.com/ec2/?nc2=h_m1

-
- [19] Amazon Web Services: Amazon S3. In: *Aws.amazon.com* [online]. [citováno 15. 04. 2018]. Dostupné z: https://aws.amazon.com/s3/?nc2=h_m1
- [20] Amazon Web Services: Amazon Relational Database Service (RDS). In: *Aws.amazon.com* [online]. [citováno 18. 04. 2018]. Dostupné z: https://aws.amazon.com/rds/?nc2=h_m1
- [21] Amazon Web Services: Amazon ElastiCache. In: *Aws.amazon.com* [online]. [citováno 16. 04. 2018]. Dostupné z: https://aws.amazon.com/elasticache/?nc2=h_m1
- [22] Amazon Web Services: Amazon DynamoDB. In: *Aws.amazon.com* [online]. [citováno 16. 04. 2018]. Dostupné z: https://aws.amazon.com/dynamodb/?nc2=h_m1
- [23] Amazon Web Services: Elastic Load Balancing. In: *Aws.amazon.com* [online]. [citováno 17. 04. 2018]. Dostupné z: https://aws.amazon.com/elasticloadbalancing/?nc2=h_m1
- [24] Amazon Web Services: Amazon Route 53. In: *Aws.amazon.com* [online]. [citováno 16. 04. 2018]. Dostupné z: https://aws.amazon.com/route53/?nc2=h_m1
- [25] Amazon Web Services: Amazon CloudFront. In: *Aws.amazon.com* [online]. [citováno 10. 04. 2018]. Dostupné z: https://aws.amazon.com/cloudfront/?nc2=h_m1
- [26] Amazon Web Services: Amazon CloudWatch. In: *Aws.amazon.com* [online]. [citováno 16. 04. 2018]. Dostupné z: https://aws.amazon.com/cloudwatch/?nc2=h_m1
- [27] Amazon Web Services: Amazon CloudSearch. In: *Aws.amazon.com* [online]. [citováno 16. 04. 2018]. Dostupné z: https://aws.amazon.com/cloudsearch/?nc2=h_m1
- [28] Amazon Web Services: AWS Identity and Access Management (IAM). In: *Aws.amazon.com* [online]. [citováno 17. 04. 2018]. Dostupné z: https://aws.amazon.com/iam/?nc2=h_m1
- [29] ČSN 01 0115: *Mezinárodní slovník základních a všeobecných termínů v metrologii*. Praha: Český normalizační institut, 1996.
- [30] French National Metrology Network: History of measurement. In: *French metrology network: studies and research in metrology* [online]. [citováno 30. 03. 2018]. Dostupné z: <http://www.french-metrology.com/en/history/history-mesurement.asp>

- [31] ÚNMZ: World Metrology Day - Světový den metrologie. In: *Unmz.cz* [online]. [citováno 29. 04. 2018]. Dostupné z: <http://www.unmz.cz/urad/world-metrology-day-svetovy-den-metrologie>
- [32] Úřad pro technickou normalizaci: Metrologie v kostce. Třetí upravené a doplněné vydání. In: *Cmi.cz* [online]. [citováno 20. 04. 2018]. Dostupné z: <https://bit.ly/2IADKew>
- [33] Working Group 2 of the Joint Committee for Guides in Metrology: International vocabulary of metrology - Basic and general concepts and associated terms (VIM). In: <https://jcgmbipm.org/vim/en/index.html> [online]. 2012, [citováno 06. 11. 2020]. Dostupné z: <https://jcgmbipm.org/vim/en/3.1.html>
- [34] ELUC: Displeje LCD. In: *Eluc.kr-olomoucky.cz* [online]. [citováno 13. 04. 2018]. Dostupné z: <https://eluc.kr-olomoucky.cz/verejne/lekce/627>
- [35] Adaptic – tvorba webu, webdesign: Databáze. In: *Adaptic.cz* [online]. [citováno 22. 04. 2018]. Dostupné z: <http://www.adaptic.cz/znalosti/slovnicek/database/>
- [36] Doc. Ing. Karel Kadlec, CSc., Doc. Ing. Miloš Kmínek, CSc.: Základní vlastnosti měřicích přístrojů. In: *Ústav počítačové a řídicí techniky* [online]. [citováno 19. 04. 2018]. Dostupné z: <http://uprt.vscht.cz/kminekm/mrt/F4/F4k41-zvmp.htm>
- [37] Working Group 7: *WELMEC 7.2, 2019: Software Guide*. 2019. Dostupné z: https://www.welmec.org/fileadmin/user_files/publications/WG_07/Guides/WELMEC_Guide_7.2-Software_Guide_2019.pdf
- [38] Microsoft: Co je SaaS? In: <https://azure.microsoft.com/cs-cz/> [online]. [citováno 11. 11. 2020]. Dostupné z: <https://azure.microsoft.com/cs-cz/overview/what-is-saas/>
- [39] Amazon Web Services: Create and Connect to a MySQL Database. In: *Aws.amazon.com* [online]. [citováno 28. 04. 2018]. Dostupné z: https://aws.amazon.com/getting-started/tutorials/create-mysql-db/?nc1=h_ls
- [40] Amazon Web Services: AWS Database Migration Service. In: *Aws.amazon.com* [online]. [citováno 28. 04. 2018]. Dostupné z: https://aws.amazon.com/dms/?nc1=h_ls
- [41] IoTport: Co to je IoT? In: *iotport.cz* [online]. January 2020, [citováno 11. 10. 2020]. Dostupné z: <https://www.iotport.cz/iot-novinky/ostatni-clanky-o-iot/co-to-je-iot>

-
- [42] Control Engineering Česko: Způsoby využití cloudu průmyslovými výrobci In: *vseoprmyslu.cz* [online]. July 2020, [citováno 16. 08. 2020]. Dostupné z: <https://www.vseoprmyslu.cz/automatizace/site-a-komunikace/zpusoby-vyuziti-cloudu-prumyslovymi-vyrobci.html>
- [43] redakce *iot-portal.cz*: Co dokáže IIoT? In: *iot-portal.cz* [online]. December 2018, [citováno 29. 09. 2020]. Dostupné z: <https://www.iiot-portal.cz/2018/12/15/co-dokaze-iiot/>
- [44] PortálDigi: Digitalizace In: *portaldigi.cz* [online]. [citováno 21. 09. 2020]. Dostupné z: <https://portaldigi.cz/digislovník/digitalizace/>
- [45] BIPM: METROLOGY FOR THE DIGITALIZATION OF THE ECONOMY AND SOCIETY In: *bipm.org* [online]. October 2017, [citováno 03. 09. 2020]. Dostupné z: https://www.bipm.org/cc/PARTNERS/Allowed/2017_October/2017-Metrology-for-the-Digitalisation-of-Economy-and-Society.pdf
- [46] Radoslav Ch.: 33 Heavenly Cloud Computing Statistics for 2020 In: *techjury.net* [online]. June 2020, [citováno 10. 10. 2020]. Dostupné z: <https://techjury.net/blog/cloud-computing-statistics>
- [47] App Developer Magazine: Why the cost of cloud computing is dropping dramatically. In: *Appdeveloper magazine.com* [online]. January 2018, [citováno 29. 04. 2018]. Dostupné z: <https://appdeveloper magazine.com/5820/2018/1/25/why-the-cost-of-cloud-computing-is-dropping-dramatically/>

Seznam použitých zkratek

CC Cloud Computing

SW Software

IaaS Infrastructure as a Service

PaaS Platform as a Service

SaaS Software as a Service

PKI Public Key Infrastructure

TLS Transport Layer Security

VPN Virtual Private Network

VM Virtual machine

ECU Electronic Control Unit

RAM Random Access Memory

VPC Virtual Private Cloud

DDoS Distributed Denial of Service

WAF Web Application Firewall

HTTPS HyperText Transfer Protocol Secure

EFTA European Free Trade Association

JWT JSON Web Token

IoT Internet of Things

STS Security Token Service

A. SEZNAM POUŽITÝCH ZKRATEK

IIoT Industrial Internet of Things

PTB Physikalisch-Technische Bundesanstalt

IDC International Data Corporation

MID Measuring Instruments Directive

ER model Entity-Relationship model

Obsah přiloženého SD

readme.txt.....	stručný popis obsahu SD
└─ src	
└─ thesis	zdrojová forma práce ve formátu \LaTeX
└─ text	text práce
└─ thesis.pdf	text práce ve formátu PDF