ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

Cloudová řešení pro služby IoT a E-health

Cloud Solutions for IoT and E-health Services

květen 2019

Diplomant: Lukáš Krupka

Vedoucí práce: Ing. Lukáš Vojtěch, Ph.D.

Čestné prohlášení

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

Datum: 24. 5. 2019

……

podpis diplomanta

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Krupka** Jméno: **Lukáš** Osobní číslo: **420370**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra telekomunikační techniky**

Studijní program: **Elektronika a komunikace**

Studijní obor: **Komunikační systémy a sítě**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Cloudová řešení pro služby IoT a E-health

Název diplomové práce anglicky:

Cloud Solutions for IoT and E-health Services

Pokyny pro vypracování:

Prozkoumejte dostupná řešení a realizujte ukázkovou experimentální cloudovou službu pro zpracování a vizualizaci dat z IoT senzoru detekce pomalých pohybů kosterního svalstva. Zaměřte se na cenově efektivní řešení, možnosti open source řešení a zejména na problematiku provozní a datové bezpečnosti v prostřední služeb E-health. Speciální pozornost věnujte standardu „Health Level 7 - FHIR“.

Seznam doporučené literatury:

[1] HIMSS Interoperability & Standards Committee, Technology Information Exchange Work Group, „Foundations for Healthcare Interoperability,“ Healthcare Information and Management Systems Society (HIMSS), 2014
[2] National Institute of Standards and Technology, „Healthcare - Standards & Testing,“ 1. 3. 2017. Dostupné na: https://www.nist.gov/itl/ssd/systems-interoperability-group/healthcare-standards-testing. [on-line]
[3] HL7 Standards, http://www.hl7.org/
[4] MZČR, Národní strategie elektronického zdravotnictví, http://www.nsez.cz/

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Lukáš Vojtěch, Ph.D., katedra telekomunikační techniky FEL

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

Datum zadání diplomové práce: **11.02.2019** Termín odevzdání diplomové práce: _____

Platnost zadání diplomové práce: **20.09.2020**

Ing. Lukáš Vojtěch, Ph.D.	podpis vedoucí(ho) ústavu/katedry	prof. Ing. Pavel Ripka, CSc.
podpis vedoucí(ho) práce		podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

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

. _____
Datum převzetí zadání Podpis studenta

Anotace:

Tato diplomová práce se zabývá návrhem a implementací možných cloudových řešeních pro zdravotnické služby v rámci IoT a eHealth. Cílem je porovnání možností technologií a poskytovatelů cloudových služeb v těchto oblastech za účelem nalezení vhodného řešení pro implementaci malé zdravotnické služby. Práce mapuje právní rámec a definuje základní zdravotnické pojmy jako PHI a HIE. Rozebírá aspekty přenosových technologií vhodných pro implementaci zdravotnické služby. Práce popisuje a porovnává experimentální zdravotnickou služba pro detekci pohybů kosterního svalstva z pohledu IoT a eHealth. Služba z pohledu IoT je implementována na serverech společnosti IBM pomocí technologie MQTT. Ze zdravotnického pohledu byl vytvořen model služby s technologií FHIR, u kterého byla ověřena funkčnost testem na platformě společnosti Cerner a byl doplněn o doporučený způsob reálné implementace FHIR technologie do praxe.

Klíčová slova:

zdravotnická služba, Internet věcí, IoT, eHealth, MQTT, HL7, FHIR

Summary:

This thesis deals with design and implementation of possible cloud solutions for health services within IoT and eHealth. The goal is to compare the capabilities of technology and cloud service providers in these areas to find the right solution for implementing a small health service. The work maps the legal framework and defines basic medical terms such as PHI and HIE. It analyzes aspects of transmission technologies suitable for health service implementation. The work describes and compares experimental medical service for detection of skeletal muscle movements from the perspective of IoT and eHealth. IoT service is implemented on IBM servers using MQTT technology. From the medical point of view, a model of experimental service with FHIR technology was created, where the functionality was tested on the Cerner platform. It was supplemented by the recommended method of real implementation of FHIR technology into practice.

Index Terms:

medical service, HIE, Internet of Things, IoT, eHealth, MQTT, HL7, FHIR

Poděkování

Děkuji vedoucímu práce Ing. Lukáši Vojtěchovi, Ph.D. za velmi užitečnou metodickou pomoc a cenné rady při zpracování této diplomové práce.

V Praze dne 24. 5. 2019

…….…….

podpis diplomanta

Obsah

Úvod

Tato diplomová práce se zabývá návrhem a implementací možných cloudových řešeních pro zdravotnické služby v rámci IoT a eHealth. Cloudová úložiště jsou v nynější době velmi rozvinutá a nabízí celou škálu různých služeb, ovšem do oblasti zdravotnictví zasahují jen zřídka. Důvodem jsou specifické podmínky, ve kterých se zdravotnické služby provozují a jsou na ně tudíž i kladeny odlišné nároky. Zdravotnické služby také pokrývají velké množství různých aplikací, které vyžadují různé přístupy. Všechny tyto aplikace mají společné prvky. Mezi hlavními je především důraz na bezpečnost řešení a soukromí pacientů, jelikož se zde pracuje s citlivými zdravotnickými a osobními informacemi. S těmi je nutno zacházet jiným způsobem než s běžnými daty, a jsou i proto speciálně definované v zákonech. Tímto se práce zabývá v následujících kapitolách.

Obecně problematika zdravotnických informačních systémů a navazujících služeb většího či menšího rozsahu je nyní velice aktuální a jejich rozvoj probíhá již několik let. Zejména v posledních letech se v oboru zdravotnictví začalo zaměřovat na jejich zvýšenou elektronizaci a systematizaci zaváděním sofistikovaných informačních systémů a databází. Je mnoho tendencí k zavádění ucelených systémů zdravotní péče s databází pacientů, kde bude mít každý pacient a lékař veškeré zdravotnické informace pacienta k dispozici. Zároveň je zde i možnost při anonymizaci dat pro rozsáhlé výzkumné aktivity napříč populací.

Stejně tak jako v politice, kde se každá instituce zabývá vlastním informačním systémem, děje se tak i ve zdravotnictví. Každá poskytovatel zdravotnické služby potřebuje vlastní systém ke poskytování kvalitní zdravotnické péče, který tak zpravidla sám vyvíjí či formou out-sourcingu získá od externích společností. Každá instituce takto funguje pak na odlišných systémech, které jsou zpravidla vzájemně nekompatibilní. Ucelený a jednotný systém služeb mezi vícero institucemi je díky tomu během na dlouhou trať či spíše nemožný. Existence tohoto problému dala tak vzniknout novým technologiím, které se tuto problematiku snaží řešit a zajistit komptabilitu mezi nimi. Jedním z nich je například od instituce Health Level 7 přenosová technologie FHIR, která byla rozebrána a otestována v této práci.

Tato práce se věnuje především cloudové zdravotnické službě navázané na malé zařízení pro detekci mikro pohybů svalů kosterního svalstva. Tato celá zdravotnická aplikace má široký dosah u pacientů po úrazech, kterým může napomoci správně rehabilitovat a cvičit. Sloužila by k detekci mikro pohybů svalů, zdali pacient procvičuje a zatíná správná svalová ústrojí. Z pohledu cloudové služby lze přistupovat k této aplikaci ze dvou pohledů, kdy každá má svá specifika a úskalí. Liší se také použitými technologiemi, protože odvětví Internetu věcí (IoT) zaměřující se na drobná chytrá zařízení používá odlišné postupy a upřednostňuje jiné standardy. Z druhé strany je pohled téměř výhradně zdravotnický, který je zpravidla komplikovanější kvůli větší obavě o zabezpečení informací.

Oba zmíněné pohledy budou v této práci ukázány. Popsány budou modely fungování i způsoby implementace včetně použitých technologií, topologií a dalších specifikací. Varianta z pohledu IoT bude ověřena praktickou implementací a u zdravotnické varianty bude definován model fungování takové aplikace podpořený testovací ukázkou funkčnosti a doplněn o doporučený způsob reálné implementace FHIR technologie do praxe.

1. Osobní a zdravotní informace

Definice osobních a zdravotních informací je vysoce důležitá pro problematiku získávání, ukládání a přenosu takovýchto informací. Je nutné provést jejich klasifikaci a rozřadit je do kategorií. Po jejich nadefinování je již možné stanovovat konkrétní pravidla pro dané kategorie dat. Zmiňuje se o tomto již americký zákon HIPAA (Health Insurance Portability and Accountability Act) z roku 1996, který byl jedním z prvních svého druhu a mnoho dalších z něj dále vycházelo. Tento zákon je komplexní a zahrnuje mnoho další pravidel, které byly časem doplněny či upraveny. Tento zákon bude podrobněji rozebrán v samostatné kapitole.

Osobně identifikovatelné informace (Personally identifiable information – PII) jsou první základní kategorií dat, která by mohla potenciálně identifikovat konkrétní jednotlivce. Veškeré informace, které lze použít k odlišení jedné osoby od jiného či je použít pro odhalení anonymních dat lze považovat za PII. PII mohou být citlivé nebo necitlivé. Necitlivé PII jsou informace, které mohou být přenášeny v nezašifrované podobě, aniž by to vedlo k poškození jednotlivce. Necitlivé PII mohou být snadno shromažďovány z veřejných záznamů, telefonních seznamů, firemních adresářů a webových stránek. Citlivé PII jsou informace, které, pokud jsou zveřejněny, mohou vést k poškození jednotlivce, jehož soukromí bylo narušeno. Citlivé PII by proto měly být vždy šifrovány při přenosu a ukládání. Tyto informace zahrnují biometrické informace, lékařské informace, informace o majetku, osobně identifikovatelné finanční informace (PIFI) a jedinečné identifikátory, jako jsou čísla pasu nebo sociálního zabezpečení. Dále se do PII zahrnují také technické údaje jako například MAC a IP adresy, e-mailové adresy, poštovní adresy a telefonní čísla pro firmy jakož i další statické identifikátory, které by mohly konzistentně propojit určitou osobu. [1]

Další kategorie informací se nazývá chráněné zdravotní informace (Protected health information – PHI), označované také jako osobní zdravotní informace. PHI je často považována za jakékoli zdravotní informace, které jsou individuálně identifikovatelné a vytvořil či obdržel je poskytovatel zdravotní péče. Mezi příklady poskytovatelů zdravotní péče patří lékaři, zdravotní sestry, zubaři, lékárníci, vědci ve zdravotnictví i organizace, které je zaměstnávají (nemocnice, kliniky, lékařské laboratoře, instituty lékařského výzkumu atd.).

Obecně se toto týká demografických informací, anamnéz, testů a laboratorních výsledků, informace o duševním zdraví a pojištění, a další údaje, které zdravotnické organizace shromažďují k identifikaci jednotlivce a určení vhodné péče. Informace mohou souviset s aktuálním, minulým nebo budoucím zdravotním stavem jednotlivce, a to buď ve fyzickém, nebo mentálním smyslu stejně jako aktuální stav osoby. PHI lze obecně použít k identifikaci konkrétní osoby a odkazuje na data, která jsou buď udržována nebo přenášena v jakémkoli formuláři včetně řeči, papíru nebo elektronicky.

Na tyto informace se vztahují přísnější pravidla než na obecné PII. Pravidla ochrany osobních údajů a bezpečnostní předpisy zákona HIPAA poskytují zvýšenou ochranu pro PHI a dává pacientům řadu práv týkající se těchto informací. Zároveň je pravidlo ochrany osobních údajů vyrovnané, aby umožňovalo zveřejňování osobních zdravotních informací potřebných pro péči o pacienty a další důležité účely.

PHI nezahrnuje vzdělávací záznamy ani neodkazuje na žádné záznamy o zaměstnancích, které jsou spravovány zaměstnavatelem osoby. Předpisy obvykle odkazují na řadu různých oborů, které by mohly být využity k identifikaci osoby, včetně:

- Jména
- Všechna data přímo spojená s jednotlivcem, včetně data narození, úmrtí, propuštění z práce a administrativy

- Telefonní a faxová čísla
- E-mailové adresy a geografické členění, jako jsou adresy ulic, PSČ a okres
- Zdravotní záznamy entity a zdravotní plány
- Čísla certifikátů nebo čísla účtů
- Čísla sociálního pojištění nebo identifikátory vozidel
- Biometrické identifikátory, včetně hlasových nebo otisků prstů
- Fotografické snímky celé tváře nebo rozpoznatelné znaky

PHI je také komodita. Kromě jejich použití pro pacienty a zdravotnické pracovníky, jsou také velmi cenné v anonymizované podobě pro klinické a vědecké pracovníky. Pro hackery a zloděje je PHI pokladnicí osobních informací o spotřebiteli, které při odcizení mohou být prodávány jinde. Mohou být také zneužity k vydírání za účelem peněžního zisku pomocí ransomware útoků. [2]

1.1.1. Využití PHI

Zdravotní péče je ze své podstaty věnována citlivým údajům o pacientovi, včetně data narození, zdravotních stavů a nároků na zdravotní pojištění. Ať už v papírových záznamech nebo v systému elektronického zdravotního záznamu (Electronic health record – EHR). PHI vysvětluje anamnézu pacienta, včetně nemocí, různých léčebných postupů a výsledků.

Od prvních okamžiků po narození, dítě dnes pravděpodobně bude mít PHI záznamy zahrnuty do EHR, včetně hmotnosti, délky, tělesné teploty a jakékoli komplikace při porodu. Sledování těchto lékařských informací v průběhu života pacienta nabízí lékaři širší povědomí o zdraví člověka, který může pomoci při rozhodování o léčbě. Při širším rozhledu může být PHI zbaven identifikačních prvků a anonymně přidán do rozsáhlých databází informací o pacientech. Tyto de-identifikovatelné údaje mohou globálně přispět ke snaze zajistit vyšší úroveň zdraví obyvatelstva i díky vytváření specifických zdravotních postupů či plánů.

1.1.2. Pravidla a regulace

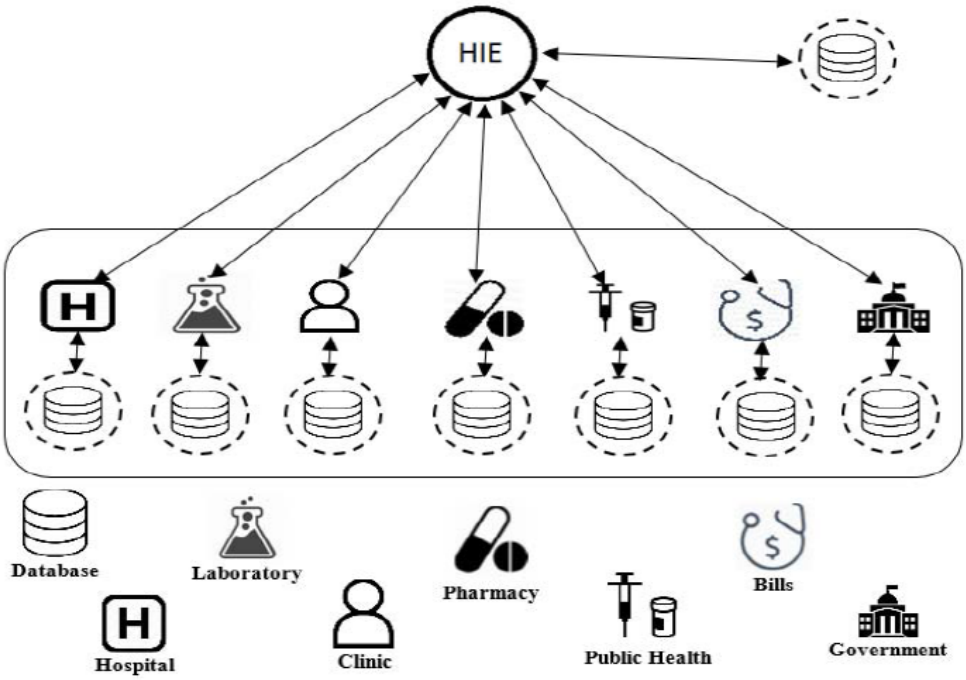
Pravidla a regulace o využívání PHI jsou specifikovány rozdílně v každé zemi v závislosti na jejich vlastní legislativě. V zemích jako USA je například tato problematika upravena už zákonem HIPAA a jeho dodatky. Tento zákon rozděluje specifikace PHI mezi pravidla ochrany osobních údajů a jejich zabezpečení. Pravidla ochrany osobních údajů upravují nastavení, jak nemocnice, ambulantní centra, zařízení pro dlouhodobou péči a další zdravotnická zařízení mohou používat a sdílet PHI. Bezpečnostní ustanovení se mezitím vztahují na opatření včetně softwaru, která omezují neoprávněný přístup k PHI. [3] [4]

Zákon HIPAA a jeho důležité části budou rozebrány v samostatné kapitole níže. Tato práce se bude zabývat tímto zákonem, ačkoliv je americký, jelikož se jedná o jeden z prvních a hlavních komplexních zákonů na světě věnující se problematice osobních informací a eHealth. Zároveň v České republice zatím neexistuje takto postavený a komplexní zákon, ačkoliv zákon o ochraně osobních údajů i GDPR se některými věcmi zaobírá a řeší je velmi podobně. Proto se bude práce věnovat i Národní strategii elektronického zdravotnictví a programu Evropské komise eHealth European Interoperability Framework (eHealth EIF).

1.2. Health information exchange

Stejně jako v mnoha jiných odvětvích využívající technologie (např. finance, obchodování, letectví) se stávají informační systémy pohonem inovace a udržitelnosti. Tyto informační systémy jsou postaveny na výměně dat a interoperabilitě. Mechanismy a nástroje pro výměnu dat se neliší pro zdravotní péči od jakéhokoli jiného odvětví. Rozdíl spočívá v důsledcích rizika. Ty jsou výrazně vyšší, pokud se jedná o naše osobní informace a zdraví. Následkem toho jsou procesy potřebné ke komunikaci podstatně více složitější.

Informace o zdravotní péči jsou ukládány u jednoho či více poskytovatelů zdravotní péče, kteří spolupracují na poskytování technologií, správy a podpory takzvané výměny zdravotnických informací (Health information exchange – HIE). Výměna informací o zdravotním stavu (HIE) umožňuje spolupracujícím poskytovatelům zdravotní péče a pacientům přistupovat k elektronickým údajům a bezpečně je přenášet, čímž se zlepší kvalita, bezpečnost a náklady na péči o pacienta. Každý HIE musí přijmout všechny předpisy, která platí pro daný národní stát, kde je systém provozován. Například v USA je nutné se řídit HIPAA, včetně pravidel ochrany osobních údajů a zabezpečení. V Evropě pravidla vychází z národních zákonů a eHealth European Interoperability Framework, která je různě implementována v jednotlivých státech. V České republice nyní probíhá projekt Strategické řízení rozvoje elektronického zdravotnictví v rezortu MZ s koncem v roce 2021. [5]



Obrázek 1.A Příklady HIE [6]

Údaje o zdravotním stavu pacienta zahrnují elektronické zdravotní/lékařské záznamy (EHRs/EMRs), což jsou záznamy o dlouhodobé anamnéze pacientů, obsahující souhrny o návštěvě lékaře, diagnózy, laboratorní testy, popisy léčby atd. HIE spravuje multi-direction toky elektronických zdravotní informací pacientů mezi různými poskytovateli zdravotní péče, jak je znázorněno na obrázku 1.A.

Existují tři způsoby výměny, které HIE používá ke sdílení informací o pacientech mezi různými poskytovateli zdravotní péče [6]:

1. Directed Exchange: - Umožňuje poskytovatelům zdravotní péče koordinovat zabezpečené elektronické přenosy (zasílání a příjem) informací o pacientech.
2. Query-based Exchange: - Umožňuje poskytovatelům zdravotní péče vyhledat a požadovat informace o pacientech od jiných poskytovatelů zdravotní péče.
3. Consumer-mediated Exchange: - Jedná se o způsob přenosu, který je zprostředkován spotřebiteli tedy pacienty. Umožňuje pacientům shromažďovat a kontrolovat používání zdravotních informací poskytovateli zdravotní péče.

1.3. Příklady použití

Jeden z příkladů, který pokrývá více problémových oblastí u HIE je například nositelný monitor srdeční funkce. Tento případ použití nositelného zdravotnického prostředku demonstruje klady i složitosti spojené s interoperabilitou v oblasti zdravotní péče. Lékařský přístroj, v tomto příkladu srdeční monitor, přenáší data přímo do cloudu poskytovatele zdravotní péče. Jakmile je poskytovatel zdravotní péče přijme, údaje jsou zapsány do záznamů pacienta a jsou k dispozici pacientovi či poskytovateli zdravotní péče pacienta.

Překvapivě jednoduchý příklad interoperability může být velmi obtížné realizovat kvůli mnoha regulačním, pracovním, procesním a technologickým bariérám, které musí být překonány, aby bylo dosaženo hladké interoperability. Tyto bariéry postupně překonávají nové technologie.

Tento případ nepopisuje, jak kardiolog by měl vykonávat svou práci, ale zaměřuje se jak na technologii, tak na procesy nutné k dosažení kýžených cílů. Na tomto případu jsou ukázány problémy takového řešení, ale také jak účinná interoperabilita může poskytnout významné přínosy pro pacienta.

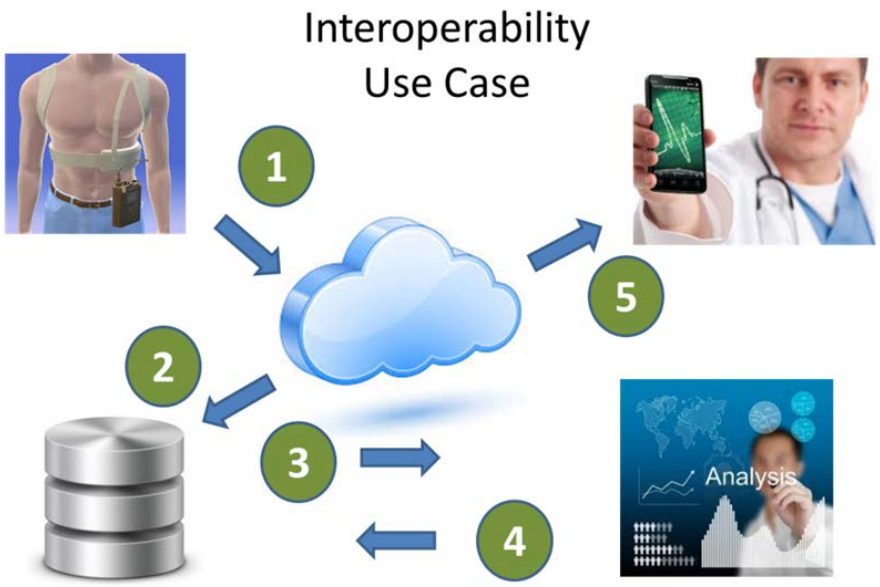
- Datový tok od pacienta k poskytovateli

Mobilní nebo přenosné zařízení kardiostimulátoru monitoruje srdeční rytmus pacienta ve svém domově. Zařízení přenáší data přes internet na webovou službu, která zprostředkovává přenos pomocí HIE. Data jsou dále směřována do elektronického zdravotního záznamu (EHR) zdravotnické organizace. EHR prezentuje získané údaje v rámci záznamů o pacientech pro pacienta či lékařský tým. Poskytovatelé lékařské péče používají tyto informace k vyhodnocení stavu pacienta a identifikaci všech požadovaných léčebných kroků.

Jedná se o jeden z mnoha příkladů, jak lze v praxi realizovat interoperabilitu. Schéma datového toku pro zmíněný příklad využití je vyobrazeno na obrázku 1.B a souhrn oblastí, které jsou v něm zahrnuty v tabulce 1.A.

- Výhody

Přínosem pro pacienta v tomto případě je možnost být pod kontrolou lékařského týmu doma. Výhodou pro nemocnici a lékařský tým je to, že pacient nemusí vynaložit čas, náklady a riziko spojené s návštěvou nemocnice. Přínosem pro lékaře a další členy týmu je zlepšení přístupu k údajům pomocí inteligentních výpočetních systémů. [7]



Obrázek 1.B Schéma přenosného monitoru srdeční činnosti [7]

Tabulka 1.A Oblasti a skupiny lidí, které jsou zahrnuty u přenosného monitoru srdeční činnosti [7]

	Pacient	Výrobce zdravotnických přístrojů	Poskytovatel sítě / internetu	Gateway poskytovatel	Poskytovatel softwaru	Cloud Hosting poskytovatel	Software analýza / Personál	Nemocnice	Lékař
Životní funkce pacienta jsou shromažďovány doma v nositelném zdravotnickém zařízení. Data jsou přenášena prostřednictvím domácí sítě a brány gateway.	•	•	•	•					
Data zdravotnického zařízení jsou přijímána v cloudové databázi.		•	•		•	•			
Pacientovi data jsou analyzovány na známky srdečního onemocnění nebo poruchy.			•		•	•	•		
Výsledky jsou uloženy v cloudové databázi, aby byly podle potřeby načteny.			•		•	•	•		
Pacientův lékař se přihlásí do nemocničního systému EHR kvůli kontrole a analýze údajů pro pacienta.	•		•		•			•	•

1.4. Soukromí, důvěrnost a bezpečnost HIE

Na poskytovatele zdravotnických služeb s HIE je vyvíjen velký tlak na ochranu, řízení a zpracování dat uživatelů. Je to dáno snahou zajistit soukromí, důvěrnost a bezpečnost informací využívané v poskytované službě.

Jednou z hlavních složek ochrany je soukromí uživatelů, kde se jedná o právo uživatele chránit a spravovat jeho data. Jako zvláštní případ je soukromí pacienta, který se týká práva pacienta na ochranu a kontrolu údajů týkajících se jeho zdravotního stavu a péče. Pacienti by měli být schopni určit, kdy, jak a jaké části jejich zdravotních informací jsou zveřejněny nebo šířeny. Důvěrnost uživatelů je právo jednotlivce uchovávat své osobní a lékařské informace soukromé, pokud neudělí někomu povolení odhalit část nebo všechny tyto informace. [6] Nakonec bezpečnost informací pacienta je právo k zajištění takových opatření a bariér, aby došlo k zamezení přístupu k informacím nepovolaným osobám, které by měli snahu o jejich odcizení.

Ačkoliv touto problematikou se zabývají odborníci již delší dobu a existuje řada prověřených bezpečnostních technik, existuje několik běžných nedostatků z praxe v oblasti zdravotnictví, na které je vhodné se navíc zaměřit. Následující pravidla mohou pomoci řešit nedostatky v soukromí a zabezpečení:

- **Vyhnout se přístupu k údajům od neoprávněných osob**

Uživatelé často nechávají počítače přihlášené v době, kdy jsou mimo pracoviště. Oblasti omezeného přístupu musí být sledovány. Prohlídka během a po pracovních hodinách může poskytovatelům pomoci určit, zda mohou neoprávněné osoby fyzicky získat přístup k chráněným údajům.

- **Monitoring ovládacích prvků na klíčových systémech a kontrola, zda nedošlo k chybnému zaznamenání**

Pokaždé, když uživatelé systému přistupují k počítačovým záznamům, nechávají elektronické stopy nebo záznamy v informačních systémech. Většina zdravotnických organizací se spoléhá na kontroly přístupu, které pomáhají zajistit dodržování pravidel bezpečnosti. Nicméně bezpečnostní mezery se vyskytují, když poskytovatelé používají zastaralé systémy, které nepovolují protokolování. Mohou také nastat situace, kdy aktualizují na nové systémy, aniž by umožňovaly protokolování nebo jednoduše nepřiměřeně monitorovaly zaznamenávané činnosti.

- **Ochrana kontrolu přístupu**

Poskytovatelé by měli potvrdit, že hesla jsou vyžadována pro přístup ke všem jejich systémům, databázím a aplikacím, které pracují s PHI. Všechna požadovaná hesla by měla splňovat požadavky na složitost, například kombinaci čísel, symbolů, velkých písmen a malých písmen, a měly by být obnovovány pravidelně. Účty by měly být uzamčeny po sérii neúspěšných pokusů o přihlášení a měl by být vytvořen protokol o všech neúspěšných pokusech o přihlášení, tak lze lépe identifikovat účty, které jsou cíleny ke kompromitaci.

- **Vypracování plánů řízení nepřetržitého provozu a reakce na incidenty**

Mnoho poskytovatelů má plán obnovy po havárii, který poskytuje návod, jak by měla péče o pacienty pokračovat v případě, že nejsou k dispozici systémy IT. Součástí tohoto plánu by měl být i plán obnovy po havárii specifický pro bezpečnost informací. Zatímco v případě porušení bezpečnosti by měl být vypracován plán reakce na bezpečnostní incident.

Ochrana soukromí pacientů a bezpečné zajištění jejich informací o zdraví je základním požadavkem na aplikace pracující s PHI. Dále účinná ochrana soukromí a bezpečnosti chrání poskytovatele lékařských služeb před občanskými a trestními sankcemi, které by mohly vzejít z neplnění zákonem definovaných záruk. Technické a jiné záruky definované zákonem jsou popsány níže.

Mnoho poskytovatelů se na základě i zvýšených požadavků na bezpečnost rozhoduje, zdali vybudovat vlastní infrastrukturu nebo spolupracovat s jinými zpravidla většími poskytovateli a přenést tak část odpovědnosti na ně. Existuje již velké množství soukromých zdravotnických platforem, které různými způsoby řeší přenosy zdravotnických informací. Často se jedná o přímo na míru vyrobené systémy, které mohou být vývojově a finančně značně náročné. I přesto se velké množství poskytovatelů zdravotní péče obrací na velké hráče na trhu, které jsou schopni zajistit fungování jejich služeb na externích serverech s ucelenými aktuálními zdravotnickými standardy. Ty jsou připraveny i na splnění technických a jiných záruk definovaných zákonem. Takto je velká část odpovědnosti za informace předána nasmlouvaným společnostem. [8]

Konkrétní zdravotnické standardy budou detailně rozebrány v samostatné kapitole.

2. Legislativa HIPAA

HIPAA (Health Insurance Portability and Accountability Act) je americká legislativa podepsána prezidentem Billem Clintonem roku 1996. Je také známý jako Veřejný zákon 104-191 a má dva hlavní účely: poskytovat nepřetržité zdravotní pojištění pro pracovníky, kteří ztrácejí nebo mění své zaměstnání, a snížit administrativní zátěž a náklady na zdravotní péči prostřednictvím standardizace elektronického přenosu administrativních a finančních transakcí. Mezi další cíle patří boj proti zneužívání, podvodům a plýtvání v oblasti zdravotního pojištění a poskytování zdravotnické péče. Dále také zajišťuje soukromí a zabezpečení pro zdravotnické informace. Zákon tudíž dohlíží na využívání, přístup a zveřejňování PHI v USA.

Jedná se o jednu z prvních právních norem, které byly na toto téma ve světě vydány. Celý zákon se dělí do 5 sekcí:

- Reforma zdravotního pojištění:
  - Sekce I chrání zdravotní pojištění pro jednotlivce, kteří ztratí nebo změní zaměstnání.
- Zjednodušení administrativy
  - Sekce II nařizuje americkému ministerstvu zdravotnictví a sociálních služeb (HHS) vytvoření národních standardů pro zpracování elektronických zdravotnických transakcí. Vyžaduje také od zdravotnických organizací, aby zavedly bezpečný elektronický přístup ke zdravotním údajům, a aby zůstaly v souladu s předpisy o ochraně osobních údajů stanovené ministerstvem.
- Zdravotní daňové předpisy
  - Sekce III obsahuje ustanovení týkající se daní a pokyny pro lékařskou péči.
- Uplatňování a prosazování požadavků na zdravotnické plány
- Kompenzace výnosů
  - Sekce IV a V dále definuje reformu zdravotního pojištění.

2.1. Zjednodušení administrativy

Ve zdravotnických kruzích je dodržování zákona HIPAA sekce II to, co většina lidí míní, když odkazují na dodržování zákona HIPAA. Sekce II, známá také jako ustanovení o zjednodušení administrativy, obsahuje následující pravidla na dodržování zákona zahrnující i podmínky, kdo musí tato pravidla dodržovat:

- Standard identifikátoru národního poskytovatele
- Standard transakcí a sady kódů
- HIPAA Pravidlo ochrany osobních údajů
- HIPAA Zabezpečovací pravidlo
- HIPAA Vynucovací pravidlo

Roku 2009 navíc proběhla revize zákona HIPAA nazvaná Health Information Technology for Economic and Clinical Health (HITECH). Specifikovala limity používání konkrétních typů PHI zdravotnickými subjekty, jako jsou poskytovatelé zdravotní péče, pojistitelé či jejich obchodní společníci. Limity používání se vztahovaly na vybírání informací od jednotlivců, sdílení s jinými organizacemi nebo používání v marketingu. Kromě toho musí organizace poskytovat přístup pacientům k vlastním PHI, a to nejlépe v elektronickém formátu PHI (ePHI).

Dále úřad HHS pro občanská práva (OCR), který uplatňuje HIPAA, vydal návod v 2016, který upřesňuje, že poskytovatelé cloudových služeb a další obchodní partneři zdravotnických organizací jsou zahrnuty do pravidel HIPAA ochrany osobních údajů, zabezpečení a oznámení o porušení předpisů. Porušení zákona HIPAA může být pro zdravotnické organizace poměrně nákladné.

Ustanovení tohoto zákona dosáhly větší důležitosti až v nynějších letech, kdy šíření informací zdravotnického charakteru se stalo běžnou věcí. Spolu s tím se objevují rizika úniku informací spojené s kybernetickými a ransomware útoky na zdravotnická zařízení, jako jsou pojišťovny a poskytovatelé zdravotnických služeb. [3]

Dále budou rozebrány více některá pravidla zákona HIPAA, které mají účinnost na zabezpečení zdravotní informace a jejich přenosu.

- ## HIPAA Pravidla ochrany osobních údajů

Americké ministerstvo zdravotnictví a sociálních služeb (HHS) vydalo pravidla ochrany osobních údajů HIPAA pro implementaci požadavků a předpisů požadovanými stejnojmenným zákonem. Pravidla podporují vysoce kvalitní zdravotnické služby pro jednotlivce s cílem zlepšit zdraví lidí a jejich komfort. Dále toto pravidlo, oficiálně známé jako normy pro soukromí individuálně identifikovatelných zdravotních informací, stanovuje národní normy pro ochranu zdravotních informací pacientů. Toho lze dosáhnout poskytnutím vhodných záruk, podmínek a omezení na ochranu soukromí chráněných zdravotních informací (PHI), jakož i omezování jejich používání, přístupu a zveřejňování mezi poskytovateli zdravotnických služeb v USA. [6]

Pravidlo upravuje také, jak zahrnuté entity musí vyhodnocovat schopnosti IT a pravděpodobnost bezpečnostního rizika u PHI. Dále udává, že organizace nemohou prodávat PHI, pokud se nejedná o veřejné zdravotní aktivity, výzkum, zpracování či poskytnuté služby, na které se vztahuje HIPAA. Zákon také dává jednotlivcům právo písemně požádá o změnu PHI u příslušného subjektu.

Zdravotnické zákony byly původně určené k ochraně zdravotních informací v papírových záznamech. Po zavedení dodatku HITECH začaly poskytovatelé zdravotní péče následně implementovat EHR a další moderní zdravotní IT systémy. Díky tomu došlo k velké migraci údajů o pacientech do elektronickým formátům. Přestože pravidla zákona HIPAA regulují papír a elektronická data stejně, existují rozdíly mezi těmito dvěma formáty. Největší rozdíl je v metodě likvidace PHI, kde papírové soubory mohou být skartovány nebo jinak znečitelněny. Zatímco elektronické PHI by měly být vymazány ze systému, ve kterém byly dříve drženy, a to takovým způsobem, aby nebyly zpět dohledatelné.

V oblasti informačních technologií není tento zákon konkrétní a žádné typy technologií pro používání ePHI, které by měly být v praxi aplikovány, nejsou v daném zákoně specifikovány. Zákon obecně zahrnuje akce potřebné k zamezení hackerům a malwaru v přístupu k údajům o pacientech. [3]

- ## Program MyHealthEData

V březnu 2018, americká prezidentská administrativa oznámila nový program s názvem MyHealthEData, ve kterém vláda podporuje myšlenku, že pacienti by měli mít přístup k jejich PHI a že tyto údaje by měly zůstat bezpečné a soukromé. Základním bodem MyHealthEData je podporovat zdravotnické organizace, aby sledovaly interoperabilitu zdravotních údajů jako způsob, jak umožnit pacientům větší přístup k jejich záznamům. [4]

- **HIPAA Zabezpečovací pravidlo**

Vzhledem k tomu, že většina z nových PHI je vytvářena, ukládána, používána a šířena elektronicky pomocí počítačových systémů, zavedla HHS zabezpečovací pravidlo HIPAA. Jeho cílem bylo zajištění důvěrnosti, integrity a bezpečnosti elektronických chráněných zdravotních informací jednotlivců (ePHI) a zároveň umožnění trhu se zdravotní péčí technologický vývoj. [3] Bezpečnostní standardy ochrany elektronických chráněných zdravotních informací jsou velmi provázané s pravidlem ochrany osobních údajů. Obě dvě problematiky se na mnoha místech prolínají a závisí jeden na druhé.

Pravidlo zabezpečení HIPAA vyžaduje provádění tří úrovní záruk k zajištění bezpečného transportu, údržbě a příjmu PHI. Jsou jimi záruky fyzické, správní a technické. Při řešení rizik a zranitelností spojených s PHI a elektronickými chráněnými zdravotnickými informacemi by se zdravotnické organizace měly zaměřit na klíčové oblasti. Zdali existuje možnost, jak identifikovat zdroje PHI včetně všech forem, které jsou vytvořeny, přijaty a přeneseny. Existují-li hrozby pro informační systémy, které obsahují PHI, a jaké jsou vnější zdroje PHI.

Je třeba poznamenat, že zabezpečovací pravidlo se vztahuje především na PHI, která jsou přenášena nebo uložena v elektronické podobě, zatímco pravidlo ochrany osobních údajů se vztahuje na důvěrnost PHI ve všech formátech, včetně elektronické, papírové a ústní. Pokud poskytovatelé zdravotní péče přijmou a budou dodržovat pravidla ochrany soukromí a bezpečnosti HIPAA, může být výměna údajů o zdravotním stavu jednotlivců usnadněna a posílena. [6]

- **HIPAA Vynucovací pravidlo**

Toto pravidlo stanoví pokyny pro vyšetřování porušení předpisů HIPAA.

2.2. Uplatňování pravidel HIPAA

Zákon HIPAA je uplatňován v USA institucemi, jako je například Úřad pro občanská práva (OCR) spadající pod ministerstvo zdravotnictví a sociálních služeb (HHS). HHS rozšířila zákon v roce 2013 v rámci revize HITECH, když přidalo Omnibusovou sadu pravidel. Jedná se o sadu pravidel týkající se odpovědnosti obchodních partnerů zahrnutých subjektů. Omnibusová pravidla také zvýšila sankce za porušení dodržování zákona HIPAA na maximálně $1 500 000 za incident.

Dále pravidlo oznamování porušení zákona HIPAA v rámci Omnibusové sady vyžaduje, aby dotčené subjekty a postižení obchodní partneři informovaly pacienty v důsledku úniku informací. Kromě nákladů na oznámení mohou zdravotnické organizace narazit na pokuty po HIPAA auditech, které provádí úřad pro občanská práva. Poskytovatelé by také mohli čelit trestním sankcím vyplývajícím z porušení pravidel ochrany osobních údajů a bezpečnostních předpisů HIPAA.

V roce 2010 Federální obchodní komise rozšířila pravidlo pro oznamování porušení předpisů a jeho prosazování na zdravotnické organizace nezahrnuté pod zákon HIPAA, včetně dodavatelů elektronických zdravotních záznamů (EHRs) a systémů souvisejících s EHR.

Úřad pro občanská práva uskutečnil své první kolo HIPAA auditů zdravotnických organizací v roce 2012 a 2013. Tyto pilotní audity nevedly k žádným pokutám ani sankcím. Podstatně širší a formální kolo auditů u asi 200 zdravotnických subjektů a jejich obchodních partnerů začaly v roce 2016 a pokračovaly dále v 2017. Z těchto auditů vychází již nějaké pokuty nebo opravné plány.

Organizace jako Národní institut standardů a technologie mohou snížit riziko regulačních opatření a jejich následků prostřednictvím vzdělávacích programů na dodržování zákona HIPAA.

Úřad pro občanská práva má šest vzdělávacích programů o dodržování pravidel ochrany osobních údajů a zabezpečení. Řada poradenských a školicích skupin nabízí také vícero programů. Poskytovatelé zdravotní péče se také mohou rozhodnout vytvořit své vlastní školicí programy, které často zahrnují aktuální zásady ochrany osobních údajů a zabezpečení dle organizace HIPAA. I když neexistuje žádný oficiální certifikační program pro dodržování zákona HIPAA, vzdělávací společnosti nabízejí informace, které napomáhají porozumění pokynům a předpisům stanoveným zákonem. [3]

2.2.1. Technické záruky dle HIPAA

Technická ochrana PHI je zahrnuta v zákonu a prováděcích předpisech HIPAA. Zahrnuje obrany před neoprávněným přístupem k datům přes komunikační sítě. Jsou k tomu využity principy jako kontrola přístupu, kontrolní audity, ověřování osob a entit, zabezpečení přenosu a právní zástupce či úředník pro dodržování předpisů.

Kontrola přístupu je hlavním prvkem zabezpečení PHI. Ovládací prvky přístupu se spoléhají na ověřování a identifikaci uživatele. Proces řízení přístupu zkontroluje, zda byl uživatel oprávněn používat tento zdroj. Uživatelé musí mít oprávnění k přístupu k informacím prostřednictvím HIE. Nemocnice a střediska mohou provádět čtvrtletní audit oprávněných uživatelských účtů a porovnávat informace, které byly zpřístupněny. Mohou omezit přístup do HIE založený na různých rolích. Zaměstnanci budou mít v rámci HIE přístup k jejich úrovni přístupu, což bude pod pravidelnou kontrolou jejich nadřízených nebo zodpovědných osob pro ochranu osobních údajů. Autorizovaný uživatel, který přistupuje k systému s PHI, potvrdí účel přístupu při zobrazení dat.

Kontrolní audity jsou dalším prvkem technických záruk dle HIPAA. Ty mohou zahrnovat kontroly použití digitálních certifikátů, šifrování, ověřování uživatelů pro každou akci, skryté jméno nebo přidělené číslo a přístup založený na rolích.

Dalším důležitým prvkem je integrita dat. Bezpečnostní opatření mohou zahrnovat jak integritu zpráv, tak i šifrování. U integrity zpráv se používá infrastruktury veřejného klíče (PKI). Tato ochrana na úrovni zpráv zakazuje neoprávněnou změnu. Často je využito digitálního podpisu generovaného původcem zprávy. Šifrování poté vyžaduje stav, kdy všechna ePHI a data ověřování uživatele jsou šifrována.

Mezi technické záruky se řadí i ověřování osob nebo entit, kdy autorizovaní uživatelé mohou obdržet jedinečné uživatelské jméno, který je využit při ověřování. Jedinečný identifikátor umožňuje sledování konkrétních aktivit uživatele, když je uživatel přihlášen do informačního systému.

Identifikace uživatele je způsob, jak určit konkrétní uživatele informačního systému, obvykle podle jména či čísla. Může být použito jméno osoby, ale velmi doporučeným systémem je však soubor náhodných čísel a znaků. To může být pro oprávněného uživatele těžší na zapamatování, ale pravděpodobněji neoprávněným uživatelem brání získat neoprávněný přístup.

Zabezpečení přenosu a dat zahrnuje jak technické parametry přenosu HIE, tak i principy při práci uživatelů. Například uživatelé by měli být vyškoleni k odhlášení systému, pokud je jejich pracoviště bez dozoru. Automatické odhlášení je účinný způsob, jak zabránit neoprávněným uživatelům získat přístup k bezobslužné pracovní stanici. [8]

3. Evropská legislativa k eHealth

Evropský legislativní rámec k elektronickému zdravotnictví a eHealth služeb je založen na jednotlivých národních zákonech v každé členské zemi EU. Tyto zákony v mnoha členských státech včetně České republiky jsou neúplné či úplně chybí. Existuje zde ovšem Obecné nařízení o ochraně osobních údajů (GDPR), které je platné ve všech státech EU. Toto nařízení ovlivňuje krom osobních údajů také PHI v širokém měřítku. GDPR se tak obecně vztahuje i na zdravotní údaje, včetně genetiky. Tedy zdravotnické organizace, které léčí pacienty z EU, musí být seznámeni s GDPR předpisy a získat od pacienta souhlas ke zpracování PHI. [4] Nařízení ovšem není primárně určeno k regulaci elektronického zdravotnictví ani eHealth služeb, ale má záměr obecné ochrany osobních údajů.

3.1. eHealth European Interoperability Framework

Každý stát EU je v různé fázi implementace eHealth do jejich právních i IT systémů. Rozvoj eHealth vychází mimo jiné i z programu eHealth European Interoperability Framework (eHealth EIF), který si nechala v roce 2013 zpracovat Evropská komise. Ukazuje vizi eHealth v EU a dále definuje její koncepci, jednotlivé komponenty a obecné principy zabezpečení, ochrany osobních údajů a dalších aspekty celého systému elektronického zdravotnictví. Projednává o různých technických i zdravotnických standardech včetně těch přenosových od organizace Health Level 7, které budou probírány níže podrobněji. Dále řeší problematiku organizace správy elektronického zdravotnictví a mnoho dalšího. Práce pochází už z roku 2013 a uvádí tak mnoho zejména technických standardů, které se za poslední dobu vyvinuly. [9]

Nejnovější pokrok v této oblasti je doporučení Evropské komise o evropském formátu pro výměnu elektronických zdravotních záznamů z února 2019. S Evropskou komisí na tomto doporučení úspěšně spolupracovalo eHealth Network a související pracovní skupiny, kde se zapojila i Česká republika. Hlavním pilířem doporučení je právo občana EU na přístup k údajům o jejich zdravotním stavu dle nařízení (EU) 2019/679 Evropského parlamentu. V nynější době ovšem stále většina občanů nemá možnost přístupu k údajům o zdravotní péči a ani bezpečné sdílení těchto informací. [5]

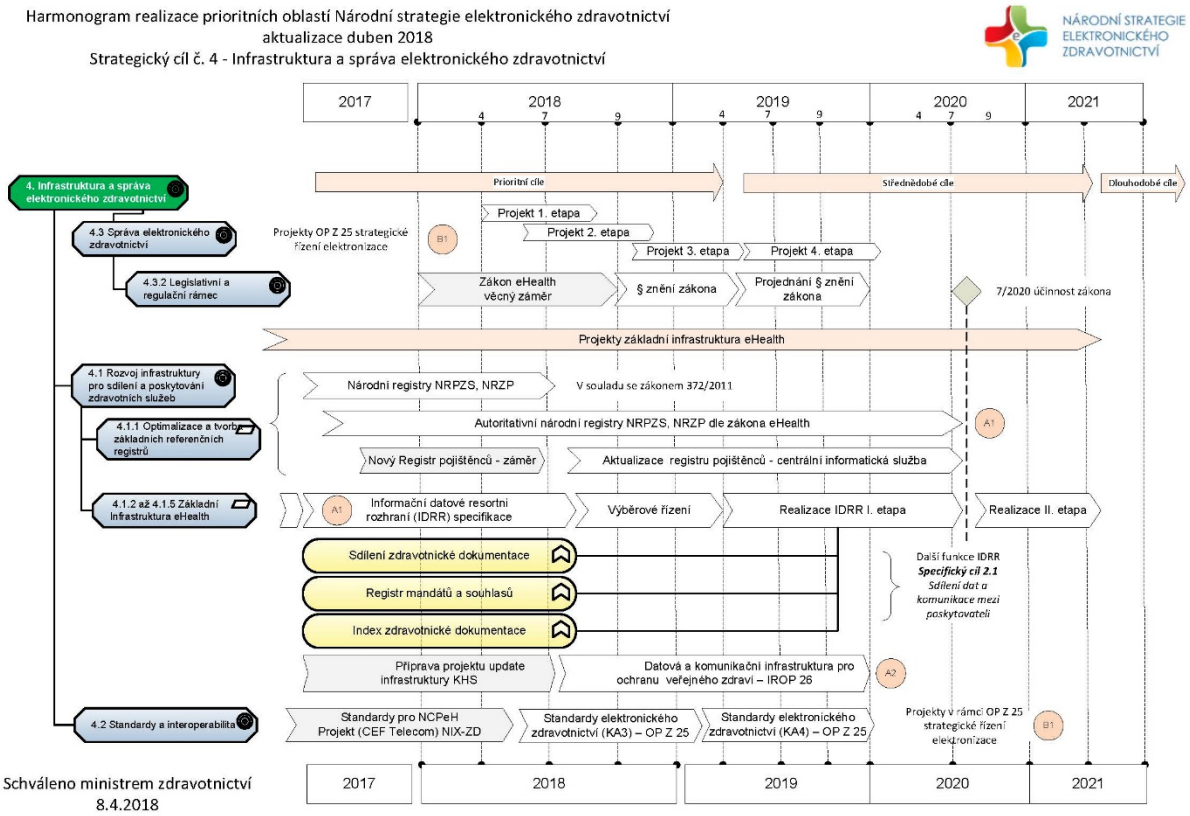
Toto doporučení navazuje na program eHealth European Interoperability Framework. Hlavním cílem této iniciativy je nastavení počátečních podmínek pro vypracování technických specifikací HIE, které by se měli používat v rámci EU. Přímo zde zmiňuje pro specifické účely konkrétní technologie jako Health Level 7 (HL7) Clinical Document Architecture (CDA) Release 2 či Digital Imaging and Communications in Medicine (DICOM). Uvádí i možnosti pro zpřesnění výměnného formátu, kterou nabízejí informační modely založené na zdrojích (např. Fast Healthcare Interoperability Resources (HL7 FHIR)). Zmíněné technologie budou více rozebrány níže. Doporučení také neopomíná zdůraznit, že všechny specifikace musí stále splňovat ochranu a bezpečnost údajů v souladu s GDPR a kybernetickou bezpečností. [10]

3.2. Národní strategie elektronického zdravotnictví

Pravidla a regulace o využívání PHI jsou specifikovány rozdílně v každé zemi v závislosti na jejich vlastní legislativě. V České republice je upravuje zákon č. 111/2007. Sb., o ochraně osobních údajů a nově i GDPR. Ovšem systém elektronického zdravotnictví zatím nebyl vytvořen.

Byla vytvořena pouze Národní strategie elektronického zdravotnictví na Ministerstvu zdravotnictví. Tato strategie určuje směr rozvoje elektronického zdravotnictví v České republice s horizontem alespoň 5 let do roku 2021. Strategie si vytyčuje řadu cílů a účelných opatření vycházející i z programu eHealth EIF.

Strategie obsahuje i projekt Informačního a datového resortního rozhraní (IDRR), který se zaměřuje na vytvoření bezpečné infrastruktury pro komunikaci elektronického zdravotnictví, zajištění autentizace, autorizace uživatelů a řízení přístupu u poskytovatelů. Správa těchto budovaných služeb spadá pod Ministerstvo zdravotnictví ČR a technická správa pod Ústav zdravotnických informací a statistiky ČR. Do budoucna se předpokládá i eliminace duplicitních služeb a zajištění procesního a infrastrukturního propojení se službami eGovermentu. Podrobněji harmonogram je na obrázku 3.A.



Obrázek 3.A Harmonogram realizace prioritních oblastí Národní strategie elektronického zdravotnictví [5]

Dříve problematika narážela na nízkou motivaci lékařů, pacientů a státních institucí, nedostatečnou legislativu a nedostatek financí jako hlavní rizika pro úspěšné zavedení systému elektronického zdravotnictví v České republice. Existuje však již nyní řada pilotních projektů, z nichž některé jsou docela úspěšné.

Do budoucna se očekává i na základě zmíněné strategie výrazný vývoj v této oblasti. Odpovídá tomu i pokrok v oblasti legislativy, kdy bude od konce roku 2018 projednáván vládou nový zákon o eHealth. Jeho části byly předneseny na Sympoziu klinické biochemie FONS 2018 v Pardubicích s názvem Datové standardy a rozvoj jejich využití v eHealth ČR. [5] [11]

4. Bezpečnostní výzvy v informačním systému zdravotní péče

Většina zdravotnických organizací či výrobců se spoléhá na dodavatele komplexního informačního systému, který zaručí bezpečnost dané aplikace. Dodavatelé jsou tedy těmi, kteří implementují řešení a vymýšlí, jakým způsobem zajistit bezpečnost. Při takové implementaci je důležité vědět, jaké hrozby jsou těmi hlavními a jak se chovají. Na základě těchto informací je možné následně tvořit takové řešení, které je dokáže eliminovat. Nejnebezpečnější hrozby zdravotnických systémů jsou útoky skenováním, útoky při injekcích, rozbité ověřování a útoky na relace a útoky DoS. V této části jsou představeny vlastnosti těchto útoků a jak jim předejít.

- **Útoky skenováním**

Před zahájením sofistikovaných útoků k narušení zabezpečení zdravotních systémů, útočníci zpravidla skenují zařízení v daném systému a shromažďují informace o síti. Běžně používané skenovací techniky pro shromažďování informací o počítačové síti zahrnují skenování IP adres, skenování portů a skenování verzí protokolů. Nebezpečnější hackeři mohou také získat verze protokolů, jako je HL7 a MQTT, odposlechem pole ID verze zpráv, které mohou dále zneužít. Pro ochranu zdravotnických systémů před útoky na skenování je lepší zavřít porty, které nejsou běžně používány. Kromě toho musí být aktualizována pravidla pro detekci a ochranu proti narušení, aby se škodlivé požadavky zasílané do aktivních portů zahazovaly.

- **Spoofing Útoky**

Spoofing útoky spočívají v tom, že útočníci předstírají, že jsou legitimní uživatelé. Maskování a zosobnění jsou dva typy útoků spoofingu. Maskování je pasivní útok, kdy útočníci nejprve extrahují legitimní údaje účtu a pak se přihlásí k systému jako legitimní uživatelé. Zosobnění je aktivnější způsob spoofing útoku než maskování. Útočníci zachytí autentizační provoz a převedou ho k sobě, aby získali přístup k systému. Jakmile protivníci kontrolují ohrožený systém, mohou extrahovat důvěrná data, vyčerpat systémové prostředky nebo šířit škodlivý software, aby ohrozili ostatní sítě. Aby bylo možné detekovat a chránit informační zdravotnický systém před spoofing útoky, musí strany serveru často měnit ověřovací údaje a povolit duplicitní metody detekce.

- **Injekční útoky**

Na úrovni datové vrstvy mohou útočníci využít zranitelnosti SQL jazyka, JavaScriptu a jiných počítačových programů, aby mohli cíl napadnout vložením nedůvěryhodných dat. V důsledku toho mohou útočníci získat přístup k databázi, útočit na webové uživatele, šířit počítačové červy či vkládat škodlivé segmenty ke snížení bezpečnosti systému. Za tímto účelem musí být zprávy informačního zdravotnického systému zašifrovány a odesílatelé si musí předat vzájemné ověření.

- **Narušení ověření**

Útočníci využívají zranitelnosti v mechanismech ověřování, aby mohli převzít legitimní identitu uživatelů. Příkladem je útok hrubou silou. Využívá slabých hesel a krátkých šifrovacích klíčů. Tyto útoky posílají odhadované hodnoty uživatelských jmen a hesel na server. Útočníci mohou opakovat zasílání svých tipů, dokud úspěšně neprovedou přístup. V důsledku úspěšného útoku mohou protivníci dělat, co by mohli dělat legitimní uživatelé. V rámci bezpečnosti musí servery zdravotnických systémů omezit pokusy o přístup k účtu, aby se vyhnuly podobným útokům hrubou sílou. Zároveň musí být do pravidel filtrování škodlivých paketů přidány IP adresy nepřátelských stran.

- **Denial of Service útoky**

DoS útoky fungují na principu vyřazení z provozu fyzické zdroje cíleného systému, aby se stal nedostupným. Jsou k tomu určeny různé metody a taktiky k vyčerpání systémových a síťových zdrojů. Jedním z příkladů jsou flood-based DoS útoky, při kterých je vysíláno obrovské množství paketů na webové servery. Tímto způsobem fiktivní požadavky blokují legitimní požadavky u zdrojů systému (např. CPU, paměť, šířka pásma atd.). Nejlepším způsobem ochrany systémů před útoky DoS je skrýt systémy (např. Adresy IP) od uživatelů. Záplavové zprávy mohou být tak přesměrovány do honeypotů. Pro úspěšnou detekci a prevenci ochrany proti útokům je nutné aktualizovat informace o útočnících, jako jsou adresy IP, typy protokolů, informace o zdrojovém portu atd. [12]

Všechny tyto potencionální útoky jsou vysokým rizikem pro jakékoliv zdravotnické zařízení. Narušení bezpečnosti může mít dalekosáhlé důsledky v mnoha oblastech, a proto je nutné se při implementaci bezpečností více zabývat. Patřičná opatření k ochraně citlivých údajů jako PHI připadá z velké části na správce a poskytovatele serverů a databází. Ty musí nastolit taková pravidla a opatření při ověřování uživatelů, přenosu a ukládání dat atd., aby nedocházelo k úspěšným výše zmíněným útokům.

5. Způsoby implementace

Tato práce se zaměřuje na implementaci cloudové služby pro zdravotnické zařízení. V tomto případě se jedná o zařízení na detekci mikro pohybů ve svalech. Konkrétně se skládá z inteligentního zařízení, jakými je mobilní telefon či mikropočítač (například Raspberry Pi), který je naprogramovaný pro funkci snímání dat ze senzoru mikro pohybů na bázi Dopplerova radaru. Na tento problém lze pohlížet ze dvou odlišných pohledů, které mezi sebou mají výrazné rozdíly. Velké odlišnosti se týkají jak právní roviny, tak i roviny využívaných standardů a způsobu implementace.

První způsob sleduje problém z pohledu Internetu věcí (IoT). Zdravotnické zařízení bere jako malé zařízení se svou specifickou zdravotnickou funkcionalitou. Z pohledu IoT se tedy obecně jedná o zařízení, které je malé, zpravidla mobilní, s malým výpočetním výkonem, specificky vytvořené k dané činnosti a využívající síťová připojení. Z toho pohledu se zmíněná celá aplikace považuje za přenos dat, která také musí být svým způsobem zabezpečena, z malého zařízení do cloudového úložiště. To může provádět další zpracování dat, jejich vizualizaci a spravovat připojená komunikační zařízení. K provedení tomuto záměru slouží celá velká škála IoT standardů, ze kterých bylo možnost vybírat.

Druhý pohled na tuto problematiku je z pohledu zdravotnického. Celá aplikace je považována za zdravotnickou eHealth službu poskytovanou pacientovi a je na to proto také tak nahlíženo. U těchto služeb se předpokládá nejenom zvýšená bezpečnost, ale i určitá integrace na úrovni zdravotnických informačních systémů pro ucelený sytém elektronického zdravotnictví. Na zdravotnické služby pracující s PII a PHI a využívající HIE spadají i přísnější uzákoněná opatření o ochraně takovýchto informací. Doposud byly rozebrány terminologické a právní aspekty takovéto zdravotnické eHealth služby v předcházejících kapitolách. Na základě i těchto informací bylo nutné vybrat vhodný protokol splňující všechny požadavky.

U obou variant budou více rozebrány možné protokoly a standardy, které se v oblasti používají. Ty mohou být svým charakterem i značně odlišné. Dále budou porovnány jednotliví poskytovatelé cloudových služeb se zaměření na podporované standardy v obou oblastech. Následně bude popsána realizace či model experimentální cloudové služby pro zdravotnické zařízení jak z pohledu IoT, tak eHealth prostředí.

5.1. Standardy a protokoly v oblasti IoT

První způsob sleduje zdravotnické zařízení z pohledu Internetu věcí. Ten pokrývá širokou škálu průmyslových odvětví a případů využití, které se pohybují od jednoho omezeného zařízení až po masivní nasazení embedded technologií a cloudových systémů, které se připojují v reálném čase. Všestranné spojení mezi nimi spočívá v řadě starších i vznikajících komunikačních protokolů, které jsou častokrát hojně používány i mimo oblast IoT. Tyto protokoly umožňují zařízením a serverům vzájemně komunikovat mnoha způsoby a zároveň vedou k vytváření desítky aliancí a koalic s nadějí na sjednocení značně rozděleného IoT prostředí. Pro snadnější orientaci lze IoT standardy a protokoly rozdělit do několika kategorií.

- Infrastruktura (př.: 6LowPAN, IPv4/IPv6, RPL)
- Identifikace (př.: EPC, uCode, IPv6, URIs)
- Komunikační / Transportní (př.: Wi-Fi, Bluetooth, LPWAN)
- Discovery (př.: Physical Web, mDNS, DNS-SD)

- Datové Protokoly (př.: MQTT, CoAP, AMQP, Websocket, Node.js)
- Device Management (př.: TR-069, OMA-DM)
- Sémantický (př.: JSON-LD, Web Thing Model)
- Multi-layer rámce (př.: Alljoyn, IoTivity, Weave, Homekit)

V této práci se budeme zajímat zejména datovými protokoly, které dávají hlavní formu tomu, jak a v jakém formátu jsou data přenášena z jednoho zařízení na druhé. Jedná se o velice důležitý prvek v komunikačním řetězci. Protokolů v dané oblasti je celá řada, ale zde jsou zmíněny pouze ty významnější a standardnější, jelikož jednota v oblasti IoT protokolů je také velmi důležitá pro další rozvoj. Jedná se například o protokoly:

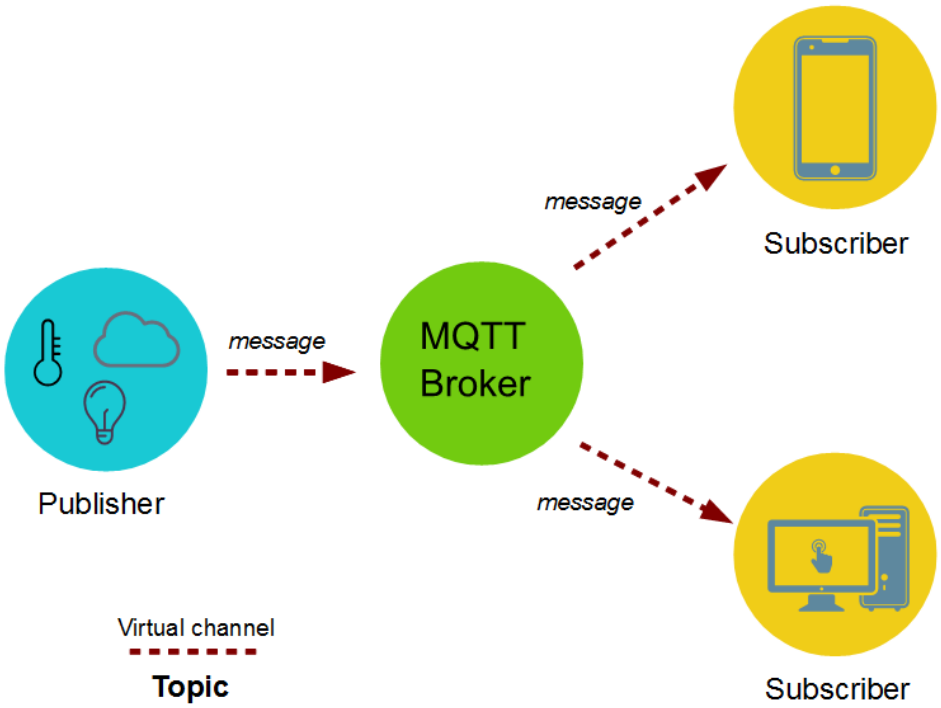
- MQTT (Message Queuing Telemetry Transport)
  - Protokol MQTT umožňuje extrémně lehký způsob publikování / odebírání zasílaných zpráv. Je užitečný pro spojení se vzdálenými místy a zabírá pouze malou šířku pásma. Detailněji bude rozebrán níže.
- CoAP (Constrained Application Protocol)
  - CoAP je protokol aplikační vrstvy, který je určen pro použití v internetových zařízeních s omezeným přístupem k prostředkům, jako jsou uzly WSN. CoAP je navržen tak, aby se snadno překládal na HTTP pro zjednodušení integrace s webem a zároveň splňoval specializované požadavky, jako je podpora více směrového vysílání, nízká režie a jednoduchost.
- REST (Representational state transfer)
  - REST nebo RESTful API je navržen tak, aby využíval stávajících protokolů. Zatímco REST lze použít téměř na jakýkoli protokol, obvykle při použití webového rozhraní API používá HTTP. To znamená, že vývojáři nemusejí instalovat knihovny ani další software, aby využili design REST API. [13]
- HTTP / 2.0
- SOAP (Simple Object Access Protocol)
- JSON / XML
- Websocket
  - Specifikace WebSocket byla vyvinutá jako součást iniciativy HTML5. Představila rozhraní WebSocket JavaScript, které definuje plně duplexní připojení s jediným soketem, přes které mohou být odesílány zprávy mezi klientem a serverem. Standard WebSocket zjednodušuje většinu složitostí v oblasti obousměrné webové komunikace a připojení.
- JavaScript / Node.js projekty IoT
  - Na této platformě je provozována řada nástrojů a jednou z nich je i aplikace Node-RED. Node-RED je programovací nástroj pro propojení API, hardwarových zařízení, a služeb online novými způsoby. Poskytuje editor založený na prohlížeči, který usnadňuje provázání toků dat pomocí širokého spektra modulů v nabídce. Ty lze vzájemně propojovat a programovat do jednoho běhu. [14] [15]

Pro implementaci cloudové služby ke zdravotnickému zařízení z pohledu IoT bylo ze zmíněných protokolů použito MQTT, JSON a JavaScript / Node.js. Jedná se o hojně používané open-source protokoly s dobrou dokumentací a velkou podporou od dalších společností včetně poskytovatelů cloudových služeb. Implementace je detailně a s postupem popsána níže.

5.1.1. MQTT

Pro IoT aplikace se velice často používá protokolu MQTT. Jedná se o nenáročný protokol vhodný pro malá zařízení běžící na TCP/IP. Jedná se o otevřený standard původně od IBM s asynchronní komunikací pro shromažďování dat z mnoha zařízení a přenášení těchto dat do IT infrastruktury typicky cloudu. Otevřený standard umožnuje jeho časté použití v mnoha aplikacích s minimálními náklady.

Architektura MQTT je postavena na modelu klient / server, kde každý senzor či koncové zařízení je klient a připojuje se přes TCP/IP ke společnému serveru nazývaného broker. Protokol MQTT funguje na principu publikování a odběru zpráv na brokerovi na rozdíl od protokolu HTTP, který funguje na principu request / response. Každá zpráva je zde diskrétní objem dat, který je nečitelný pro brokera. Každá zpráva je publikována na své konkrétní téma, které je interpretováno jako jeho adresa. Klienti se skrze dané téma mohou přihlásit k odběru jednoho či více témat. Každý klient, který se k tématu přihlásil, obdrží každou zprávu zveřejněnou na toto téma. V MQTT jsou navíc témata hierarchická, což umožňuje klientům sledovat celé hierarchie témat. Přehledně to ukazuje obrázek 5.A.



Obrázek 5.A Princip komunikace pomocí MQTT protokolu [30]

MQTT je vhodnější komunikační protokol pro IoT prostředí, které má svá specifika a omezení, než protokol HTTP. Protokol MQTT je například díky menší režii přenosu více úspornější na datový přenos i energetickou náročnost. [16] Další rozdíl k HTTP je, že broker posílá zprávy klientům, zatímco HTTP klienti o ně musí žádat pomocí zprávy request. [17] Porovnání obou protokolů je vidět v tabulce 5.A.

Tabulka 5.A Porovnání MQTT a HTTP protokolu [17]

	MQTT protokol	HTTP protokol
Architektura	Publikovat / Odebírat	Request / Response
Velikost zprávy	Malá	Velká
Zabezpečení dat	Ano	Ne, proto HTTPS slouží k zabezpečení dat.
Složitost	Nízká	Vyšší

Bezztrátovost dat je u MQTT zajištěna pomocí TCP protokolu, což poskytuje jednoduchý a spolehlivý tok dat. MQTT podporuje tři úrovně kvality služeb: „Fire and forget“, „Delivered at least once” a „Delivered exactly once”.

MQTT má také podporu pro trvalé zprávy uložené v brokerovi. Při publikování zpráv mohou klienti požádat brokera o uložení zprávy. Uloží se pouze poslední trvalá zpráva. Když se klient přihlásí k odběru tématu, bude klientovi odeslána jakákoli zpráva s trvalým umístěním. Klienti MQTT mohou také zaregistrovat vlastní zprávu jako „poslední vůle a testament“, kterou má zprostředkovatel odeslat, pokud se odpojí. Tyto zprávy mohou být použity k signalizaci účastníkům, když se zařízení odpojí.

Bezpečnost dat je zajištěna pomocí autentizace a šifrování. Broker MQTT může vyžadovat ověřování pomocí uživatelského jména a hesla od klientů, kteří se připojují. Pro zajištění soukromí může být TCP spojení šifrováno pomocí SSL / TLS. [18]

Tělo zprávy MQTT je složeno ze 3 částí: fixní hlavičky, volitelné hlavičky a payload. Fixní hlavička je povinná pro každou zprávu a je dlouhá 2 byty. Je vyobrazena v tabulce 5.B.

Tabulka 5.B Formát fixní hlavičky zprávy MQTT [16]

Bit	7	6	5	4	3	2	1	0
Byte 1	MessageType				DUP flag	QoS Level		Retain
Byte 2	Remaining Length							

- MessageType: 14 možností typů zprávy
- DUP flag: značka duplicity, využito pouze u QoS 2
- QoS: 3 druhy kvality služby (QoS 0-2)
- Retain: zachování trvalé zprávy
- Remaining Length: určení zbývající délky zprávy zahrnující volitelnou hlavičku a payload

Dále podle rozdílných témat se liší i payload. Základní struktura payloadu je v tabulce 5.C.

Tabulka 5.C Formát payloadu zprávy [16]

Počáteční bit	0	64	68	70
Funkce	Sender	TS	Type	Content

- Sender: informace o odesílateli, může zůstat prázdné
- TS: časová značka
- Type: typ payloadu
- Content: posílaná data zprávy využívající JSON formát [16]

5.2. Zdravotnické standardy a protokoly

Implementace zdravotnické aplikace je na rozdíl od IoT aplikace založena na jiných principech a protokolech. Pro případ aplikace, řešené v této práci, je i bezpodmínečně nutné využití HIE, který byl obecně popsán výše.

K tomu, aby HIE fungovalo bez chyb a ve velkém měřítku v celém rozsahu možných aplikací, musí existovat pravidla pro zapojení všech účastníků nebo „aktérů“. Pokud se všechny strany dohodnou, že budou používat společné standardy a podobné procesní rámce, může být pomocí HIE zajištěna vysoká interoperabilita společně s bezpečností u mnoha aplikací najednou. Zároveň se tak významně sníží i úsilí a čas potřebný k implementaci. Výsledná interoperabilita velkou měrou přispívá k dosažení spolehlivějšího, inteligentnějšího a efektivního systému zdravotnických aplikací k výměně PHI.

Teoreticky může každá skupina organizací, které se rozhodnou vyměňovat klinické informace, se jednoduše dohodnout na standardech, které budou používat a zahájit proces implementace standardů. V realitě se jedná pouze o úzkou skupinu organizací, které se standardizací zabývají.

Rozsáhlé standardy založené na dohodě vícero institucí jsou důležité, protože jejich použití minimalizuje náklady, riziko a čas na trhu spojené s prováděním výměny informací mezi organizacemi. Bez těchto standardů by každý pár organizací, kteří si chtějí vyměňovat informace či zavádět jiný druh zdravotnické služby, musel před zahájením implementace vyjednávat a dohodnout se na všech podrobnostech takových výměn včetně kódování, slovní zásoby, formátů dokumentů, komunikačních protokolů a integračních strategií. Složitost, která by zahrnovala tento úkol, by znamenala obrovský a těžko zvládnutelný úkol.

I když je stále potřeba vytvářet nové standardy a aktualizovat specifikace, sada stávajících standardů pro HIE je již docela velká. Široce používané komunikační standardy pro zdravotnictví jsou například HL7, DICOM, NCPDP, X12N a ADT. Standardizační subjekty a zmíněné standardy týkající se problematiky HIE a PHI jsou popsány dále:

- Health Level 7 je interoperabilní standard umožňující různým aplikacím zdravotní péče výměnu, integraci, sdílení a získávání klinických a administrativních informací. Přenos dat mezi klinickým systémem a databázemi by proto měl odpovídat standardu HL7.
- Digitální zobrazování a komunikace v medicíně (DICOM) upravuje standardy pro výměnu digitálních radiologických a kardiologických obrazů v medicínském prostředí.
- Národní rada pro léky na předpis (NCPDP) vytváří standardy pro elektronickou komunikaci pro léky na předpis, fakturaci a jiný lékárenský materiál. Telekomunikační standard NCPDP podporuje elektronickou komunikaci transakcí mezi lékárnami, pojišťovnami a jinými odpovědnými stranami.
- X12N je standard, který umožňuje elektronickou výměnu informací u zdravotního pojištění včetně zpracování údajů a fakturačních informací. Podobně jako standard HL7 lze X12N použít pro získávání dat z fakturačních systémů a systémů hlášení.

- Zprávy o vstupu, propuštění a převodu (Admission, discharge, and transfer – ADT) přenášejí informace o pacientech, jako je ID pacienta, číslo zdravotního záznamu, věk, jméno a kontaktní informace. Zprávy ADT mohou také poskytovat informace týkající se například přijetí, propouštění, přenosu a registrace pacienta atd.
- Další standardy jsou definovány protokoly pro přenos a příjem zdravotnických dokumentů a zpráv, jako jsou například pokyny pro implementaci HL7 v2.x & v3.0.
- V některých případech standardy ukazují, jak mají softwarové aplikace integrovat přijaté informace do svých databází (např. Pracovní skupina HL7 pro klinické kontextové objekty (CCOW)) a umožňovat okamžitou dostupnost a využití komerčních produktů a softwaru (Commercial off-the-shelf – COTS).

Dále existují standardy, které se týkají HIE z jiného pohledu. Ty jsou využity zejména při práci lékařů a obecně poskytovatelů lékařských služeb. Zde jsou uvedeny jen ty nejdůležitější z nich:

- Unified Medical Language System (UMLS)
- Mezinárodní klasifikace nemocí (ICD)
- Systémová nomenklatura lékařských a klinických pojmů (SNOMED-CT)
- Názvy a kódy identifikátorů logických poznatků (LOINC) jsou standardem pro identifikaci pozorování lékařských laboratoří. Klinické a laboratorní normy LOINC umožňují elektronickou výměnu a shromažďování klinických výsledků, jako jsou laboratorní testy a výzkum. Dále udává slovní zásobu používanou v dokumentech, které se týkají chorob, jejich diagnózy a léčby.

Pro vytváření, správu a aktualizaci těchto standardů odpovídá řada organizací pro rozvoj standardů (Standards development organizations – SDOs). Jedním z nejvýznamnějších SDO v zdravotnicko-technickém průmyslu pro komunikační standardy je mezinárodní soukromá aliance známá jako Health Level 7 (HL7), jejíž standardy se bude tato práce více zabývat. [12]

Dalším typem spolupráce při vytváření a zveřejňování standardů pro interoperabilitu ve zdravotnictví je například v USA Standards & Interoperability (S&I) Framework. S&I Framework je partnerská iniciativa Úřadu národního koordinátora (ONC) v oblasti zdravotnických informačních technologií spadající pod Ministerstvo zdravotnictví a sociálních služeb. Dále také Národní institut pro standardy a technologie (NIST) se podílí na přijetí stávajících standardů a k definování nových podle potřeby. NIST také například poskytuje zařízení pro validaci interoperabilních klinických dokumentů. [19]

Existuje i řada dalších iniciativ SDO a standardů zaměřených na data zdravotní péče, Internetu věcí, stejně jako na finanční údaje. Zde byly uvedeny jen některé z nich. [7]

5.2.1. Health Level 7

Informační standardy používané v oblasti zdravotní péče jsou tradičně rozvíjeny organizací „Health Level 7“ (HL7). První standard pro výměnu dat byl standard HL7-v2, který je stále velmi využíván, zejména pro výměnu dat v rámci jedné nemocnice nebo nemocniční organizace. Použití těchto zpráv k výměně dat mezi různými organizacemi je však vzácné. Standard HL7-v3 byl vyvinut k překonání některých omezeních HL7-v2, z nichž nejvýznamnější je skutečnost, že HL7-v2 je vhodný pouze pro zprávy, nikoliv pro dokumenty. Jednalo se o obrovský problém, jelikož poskytovatelé péče využívají k výměně informací prostřednictví právě dokumentů. HL7-v3 se však stal úspěšným pouze pro dokumenty zejména ve formě CDA (Clinical Document Architecture), která je také základem interoperabilního systému zdravotních záznamů ELGA v Rakousku. Přestože byla vyvinuta řada zpráv HL-v3, nikdy nebyly úplně úspěšné. To je pravděpodobně způsobeno složitostí HL7-v3, která

je založena na Referenční informační model (RIM), ve kterém musí být každá informace modelována buď jako „act“, „participation“, „role“, „entity“, „actrelationship“, „rolelink“ nebo některé z jejich podtříd. To udělalo HL7-v3 těžké implementovat softwarově pro IT personál. Proto byl vyvinut nový standard FHIR (Fast Healthcare Interoperability Resources), který zahrnuje jak zprávy, tak dokumenty, a využívá nejmodernější technologie, jako jsou RESTful web služby a různé další implementace jako JSON, XML a Turtle.

Paralelně k HL7 vyvinula CDISC (Clinical Data Interchange Standards Consortium), jedna z organizací pro rozvoj standardů (SDO), jiný zdravotnický standard ODM (Operational Data Standard) pro výměnu dat v klinickém výzkumu. Její model je stále většinou založen na paradigmatu shromažďování dat pomocí formulářů na papíře během návštěv nebo v elektronické podobě v lepším případě. To byl také původní účel tohoto standardu. Na rozdíl od FHIR je u ODM ovšem možné využívat pouze formátů XML, což ještě není vhodné pro výměnu dat pocházejících z nositelných zařízení na těle či jim podobným zařízením. Pro ně ani nikdy původně nebylo ODM navrženo, jelikož tyto využití jsou dány teprve nedávným vývojem. [20]

Vlivem těchto nedostatků u ODM a velmi rozvinutými možnostmi od organizace HL7 se tato práce bude dále zabývat vlastnostmi, řešením a využitím zdravotnického a komunikačního standardu FHIR.

5.2.2. Fast Healthcare Interoperability Resources (FHIR)

Na základě tlaku z nedostatků implementace programu HL7-v3 a předcházející HL7-v2 v lednu 2011 představenstvo guvernérů HL7 zahájilo novou pracovní skupinu, aby zjistila, jak mohou být standardy pro zasílání zpráv HL7 vylepšeny. To inspirovalo nezávislou skupinu architektů HL7, aby začali diskutovat o novém přístupu k výměně informací o zdravotní péči, který původně nazvali „Resources for Health (RFH)“, který byl později přejmenován na „Fast Healthcare Interoperability Resources (FHIR)“. FHIR je nový a stále vznikající standard vyvinutý pod záštitou organizace Health Level 7 (HL7). FHIR je určen jako další generace standardů pro vyšší interoperability v oblasti zdravotní péče. Snaží se spojit nejlepší funkce HL7 verze 2 a verze 3. Autoři tvrdí, že HL7 v3 nebyl vyhozen, ale FHIR byl vytvořen na základech HL7 v3. [21] Cílem FHIR je zjednodušit a urychlit zavádění HL7 tím, že je snadno použitelný, ale robustní. Snaží se využívat otevřené internetové standardy, kde je to možné. Používání snadno použitelného formátu u mnoha řešení zamezuje potřebě vlastních složitých transformačních nástrojů. Tyto problémy byly často vídané u předcházejících verzí. Vzhledem uvedeným skutečnostem FHIR nabízí mnoho vylepšení oproti stávajícím standardům:

- Je to otevřený zdroj, což je velice důležité pro budoucí využití bez dalších omezení. Jedná se o první snahu o to, aby integrace zdravotnictví byla transparentnější a přístupnější. Otevřená diskuze vytvořila významnou komunitu včetně vývojářů, prodejců a podniků.
- Vývojáři se zaměřili na snadnou a rychlou implementaci. Díky tomu vznikla stručná a snadno pochopitelná dokumentace v porovnání s předchozími verzemi. Dobrá dokumentace standardu FHIR vychází zároveň z RESTful API, kde se jedná o běžnou praxi.
- RESTful: Design založený na REST přináší značné výhody, a to že API, který dodržuje zásady REST, nevyžaduje, aby klient znal něco o struktuře API. Spíše server musí poskytovat jakékoli informace, které klient potřebuje k interakci se službou.

- Rozšiřitelnost: Rozšiřitelnost v rámci RESTful zajišťuje, že přídavky mohou být snadno přidány na pokrytí specifických případů použití bez ovlivnění základních modelů.
- Modulárnost: Modulární funkce zajišťuje, že téměř všechny požadavky mohou být ztvárněny pomocí základních modelů nebo zdrojů a přidružených rozšíření.
- Podpora moderních webových standardů: Základní standardy, které FHIR využívá jsou XML, JSON, HTTP, Atom, OAuth, REST. Jedná se o standardy, které jsou prověřeny a prokázaly svou funkčnost i při významných bezpečnostních požadavcích.

FHIR má i za cíl integraci s dalšími aspekty autentizace a bezpečnosti. Časem to eliminuje potřebu drahých integračních projektů a licencí. Navíc použití moderních konceptů, jako jsou RESTful API a doprovodná dokumentace, umožní vývojářům a aplikacím mnohem jednodušší rychlé připojení a získání potřebných dat. Standard obsahuje příklady implementace a referenční implementace pro několik platforem, včetně živých testovacích serverů dostupných přes internet. [21] [22]

- **Zdroje**

Základem FHIR je definování klíčových subjektů zapojených do výměny informací o zdravotní péči. Jsou jimi zdroje či v anglickém jazyce „resources“. Každý zdroj je odlišná identifikovatelná entita, u které je známa její identita (URL), skrze kterou může být adresována. Je vždy jedním ze skupiny definovaných a obsahuje sadu řádně strukturovaných datových položek, jak je popsáno v definici zdroje. Je vždy u ní i určitelná verze, která se mění při změně obsahu.

Standard FHIR popisuje dále následující obecná specifika zdrojů:

- Prostředky by měly mít jasnou hranici, která by odpovídala jednomu nebo více logickým transakčním účelům.
- Zdroje by se měly vzájemně lišit ve smyslu nikoliv pouze v použití (např. Různé způsoby použití laboratorního přehledu by neměly mít za následek různé zdroje).
- Zdroje musí mít přirozenou identitu.
- Zdroje by měly být velmi běžné a používané v mnoha různých transakcích.
- Zdroje by neměly být specifické nebo dostatečně podrobné, aby zabránily podpoře široké škály transakcí.
- Zdroje by měly být vzájemně jedinečné.
- Zdroje by měly využívat jiné zdroje, ale měly by být více než jen složení jiných zdrojů. Každý zdroj by měl představovat nový obsah.
- Zdroje by měly být uspořádány do logického rámce, založeného na společné funkci zdroje a na tom, s čím souvisí.
- Zdroje by měly být dostatečně velké, aby poskytovaly smysluplný kontext.

Na množství definovaných zdrojů se stále pracuje a většina z nich je ve zkušební verzi. Vývojový tým odhaduje, že celkově bude definováno přibližně 150 zdrojů. Návrháři FHIR uvedli: „FHIR se snaží udržet designovou přesnost verze 3, ale učinit reprezentaci zdrojů a transport jednoduchým.“ [23] Mezi příklady zdrojů patří například „Patient“, „Observation“ či „Binary“. Každý zdroj je samostatně definovaný a detailně popsaný standardem FHIR na webu HL7 [22].

Všechny zdroje se řídí standardním modelem, jehož obsah a přidružená rozšíření jsou jedinou věcí, kterou se různé zdroje od sebe liší. Znamená to, že zatímco zdroj „Patient“ a „Observation“ mají stejnou obecnou strukturu, obsah v rámci každého popisu zdroje bude jiný a specifický pro tento zdroj. Obecná struktura libovolného zdroje je následující:

- Typ zdroje – identifikuje specifický model zdroje, tj. Pacienta, léků, měření atd.

- Lidsky čitelná souhrnná sekce – XHTML sekce, která poskytuje lidskou čitelnou verzi obsahu uvnitř zprávy. Lze to považovat za záložní i ověřovací sekci pro developery. Toto je volitelný prvek.
- Sekce identifikátoru – jedinečný identifikátor URI či adresa URL pro každý zdroj identifikující, že se jedná o specifický typ. Identifikátor může obsahovat záznamy jako SSN (social security number), MRN (medical record number) a další.
- Sekce rozšíření – Umožňuje definovat všechna rozšíření, která mohou být požadována pro podporu specifických klinických pracovních postupů. Může být vložen do kterékoliv sekce, aby se pokryly specifické případy použití a potřeby pracovních postupů. To je nutné, pokud prostředky obsahují datové prvky či objekty, které nejsou součástí základních modelů FHIR.
- Obsažené zdroje – další zdroje používané při identifikaci a zpracování transakcí, např. záhlaví zprávy a datový objekt odpovídající dříve identifikovanému typu nebo obrazy spojené s pacientem.
- Metadata – Obsahuje číslo verze zdroje. Toto je volitelný prvek.
- Obsah zdroje – Jedná se o základní obsah zdroje. V případě zdroje „Patient“ obsahuje všechny relevantní údaje o pacientovi, jako je jméno, adresa, telefon, opatrovník, MRN (Medical Record Number) nebo jiné kontaktní informace a tak dále. Každý zdroj má definovaný datový model.
- Tagy – Sekce určená pro různé druhy značek. Tato sekce je stále nejasná a stále ve vývoji. Značky mohou být například popisky zabezpečení, které mohou zahrnovat seznamy ACL. Toto je volitelný prvek. [24]

Ukázka struktury zdroje „Patient“ včetně jednotlivých sekcí je na obrázku 5.B.


```
<Patient xmlns="http://hl7.org/fhir">
  <id value="glossy"/>
  <meta>
    <lastUpdated value="2014-11-13T11:41:00+11:00"/>
  </meta>
  <text>
    <status value="generated"/>
    <div xmlns="http://www.w3.org/1999/xhtml">
      <p>Henry Levin the 7th</p>
      <p>MRN: 123456. Male, 24-Sept 1932</p>
    </div>
  </text>
  <extension url="http://example.org/StructureDefinition/trials">
    <valueCode value="renal"/>
  </extension>
  <identifier>
    <use value="usual"/>
    <type>
      <coding>
        <system value="http://hl7.org/fhir/v2/0203"/>
        <code value="MR"/>
      </coding>
    </type>
    <system value="http://www.goodhealth.org/identifiers/mrn"/>
    <value value="123456"/>
  </identifier>
  <active value="true"/>
  <name>
    <family value="Levin"/>
    <given value="Henry"/>
    <suffix value="The 7th"/>
  </name>
  <gender value="male"/>
  <birthDate value="1932-09-24"/>
  <careProvider>
    <reference value="Organization/2"/>
    <display value="Good Health Clinic"/>
  </careProvider>
</Patient>
```

Obrázek 5.B Ukázka zdroje „Patient“ [22]

Ve výsledku se FHIR může jevit také jako poměrně „zrnitý“ v tom smyslu, že zdroje jsou individuálně definovány jako diskrétní prvky, kde neexistuje zjevná soudržnost sjednoceným modelem. To ovšem umožňuje maximální flexibilitu. Proto se během vývoje FHIR vyskytl i hybridní přístup. Spočíval v mapování zdrojů FHIR na RIM HL7 v3. Důvod pro to není jasný, protože existuje málo, pokud nějaké reálné implementace HL7 v3. Níže poskytuje tabulka 5.D srovnání charakteristických vlastností standardů HL7 v2, v3 a FHIR. [23]

- **REST**

Nový přístup FHIR je založen na principech REST. Representational State Transfer (REST) či často označované jako RESTful byly nedávno široce adaptovány jako dominantní informační abstrakce World Wide Web. Významné platformy internetových služeb migrovaly na služby RESTful a další možnosti, jako jsou přístupy SOAP a WSDL. Jedná se o rozhraní API klient / server, které je navrženo tak, aby se řídilo zásadami návrhu RESTful. Rozhraní API RESTful je tak univerzální rozhraní, které lze použít k pohybu dat mezi různými systémy. Toto rozhraní podporuje jak synchronní, tak asynchronní použití. Praktické výhody architektury RESTful zahrnují rozhraní umožňující snadnější a rychlejší přenos a zpracování datových struktur.

RESTful API popisuje prostředky FHIR jako sadu operací známé také jako „interakce“. Rozhraní využívá základní operace Create, Read, Update a Delete, spolu s podporou dalších jako Search a Execute operací. [22] Operace probíhají na jednotlivých prostředcích neboli zdrojích, které jsou jednotlivě spravovány ve sbírkách podle jejich typu. Tyto zdroje jsou lokalizovány na základě Service Base URL obsahující adresu serveru, cestu ke zdroji a jméno zdroje.

Servery si mohou vybrat, které z operací budou využívat a které typy prostředků podporují. Servery by měly poskytovat prohlášení o způsobilosti, které říká, jaké interakce a zdroje jsou podporovány. Implementace systému REST vychází ze čtyř základních principů návrhu:

- použití metod HTTP
- bezstavovost požadavků
- uvedení struktury adresářů jako URL zdrojů
- reprezentace zdrojů pomocí přenosu XML nebo JSON [25] [22]

- **Safety & Security**

FHIR sám o sobě není bezpečnostní protokol ani nedefinuje žádné funkce související s bezpečností. FHIR však definuje komunikační protokoly a modely obsahu, které je třeba použít s různými bezpečnostními protokoly, které byly již definovány a ověřeny dříve.

Celý systém pro bezpečné fungování FHIR zahrnuje mnoho bezpečnostních metod či dalších subsystémů. Využití těchto metod je závislé na konkrétním využití a umístění. Zpravidla vyspělé FHIR servery by měly být schopny podporovat všechny níže zmíněné metody, aby poskytly spotřebitelům možnost plné volby jejich zabezpečení. Koncová zařízení, například zdravotnická zařízení či platformy pro pacienty, budou většinou podporovat pouze některé pro ně vhodné metody pro zajištění bezpečného spojení. Proto využití bezpečnostních metod a subsystémů je vždy v závislosti na konkrétní aplikaci. Dále jsou uvedeny všechny bezpečnostní metody či subsystémy, které jsou podporovány FHIR:

- Udržování času – všechny hodiny by měly být synchronizovány pomocí NTP či SNTP
- Zabezpečení komunikace – veškerá výměna produkovaných dat by měla být zabezpečena pomocí TLS (např. HTTPS).

- Ověřování – nutnost ověření každého klienta zpravidla pomocí jména a hesla. Pro webové platformy se doporučuje použití OAuth. V případě potřeby je možnost zvážit použití technologie Smart-On-FHIR, která je nadstavbou nad FHIR.
- Labely – FHIR umožňuje nastavit sadu značek souvisejících s bezpečností, které ovlivňují způsob, jakým jsou zdroje zpracovávány.
- Autorizace / řízení přístupu – FHIR definuje infrastrukturu labelů pro zabezpečení a podporu řízení přístupu. Rozhoduje, zdali jsou operace FHIR povoleny.
- Audit – FHIR definuje způsoby kontroly původu zdroje a auditní události vhodné pro sledování původu, autorství, historie, stavu a přístupu zdrojů. Vhodné pro možnost následné kontroly a detekci neoprávněného použití.
- Digitální podpisy – FHIR obsahuje několik specificky vyhrazených míst pro digitální podpisy.
- Přílohy – FHIR umožňuje binární zdroje a přílohy.
- Politiky správy dat – FHIR definuje sadu schopností pro podporu výměny dat. Ne všechny možnosti, které FHIR umožňuje, mohou být vhodné nebo legální pro použití v některých kombinacích kontextu a jurisdikce (např. HIPAA, GDPR). Je povinností realizátorů zajistit, aby byly splněny příslušné předpisy a další požadavky.
- Validace vstupu – Ověření všech vstupů obdržených od jiných aktérů, aby byla zajištěna správná forma dat a neobsahovala obsah, který by způsobil nežádoucí chování systému. Testování zajišťuje, že vstup není náchylný k chybám. Ověřování vstupu dat funguje pomocí technik, jako je fuzzing tedy neplatné vstupní útoky a injekční útoky.

Hlavní prvky zabezpečení u FHIR ze zmíněných jsou protokol TLS, ověření identity, autorizace, řízení přístupu a záznamy auditu. Tyto metody jsou takřka nepostradatelné pro bezpečný přenos FHIR zdrojů. [22]

Tabulka 5.D Srovnání charakteristických vlastností standardů HL7 v2, v3 a FHIR [23]

	HL7 v2	HL7 v3	HL7 FHIR
Rok počátku	1987	1997	2011
Architektura	Zprávy, pole a záznamy	Orientovaný na zprávy	RESTful
Vzdělání režie	Řádově týdny	Řádově měsíce	Řádově týdny
Nutný speciální nástroj	Ano – analyzátor	Ano – kompilátor modelu	Ne
Přímo k použití	Ano	Ne	Ano
Řádově velikost specifikací	Stovky stran	Tisíce stran	Stovky stran
Implementační příklady ve specifikacích	Ano	Minimum	Ano
Referenční implementace dostupné od HL7	Ne	Ne	Ano
Podpora průmyslu a komunity	Silná	Slabá	Silná
Vhodné pro mobilní zařízení	Ne	Ne	Ano
Počet typů zpráv	?	450	30
Mezinárodní podpora znakové sady	Ne (ASCII)	Koncepčně ano	Ano (UTF8)
Podpora formátu mezinárodních zpráv	Jednotný globální standard	Místní lokalizace	Jednotný globální standard

6. Cloud servery

V celém řetězci aplikace osobní zdravotní péče se po senzorech, kontrolérech, síťových branách či jiných zařízeních se cloud servery nalézají na tom nejvyšším stupni hierarchie. Probíraná aplikace cloudové služby pro zařízení na detekci mikro pohybů ve svalech je sama o sobě velice specifická. Kombinuje totiž 2 odlišné přístupy. Za prvé se jedná o malé zařízení, které svými specifikacemi a technologickou výbavou spadá do oblasti Internetu věcí (IoT). Jedná se totiž pouze o malé přenosné zařízení s omezenou technologickou výbavou, konkrétní funkcí, a i s mnoha limity. Na druhé straně je zde důležité na věc pohlížet i z pohledu jeho využití. Zde dochází k práci s citlivými zdravotnickými informacemi. Na základě toho se i s takovou aplikací musí zacházet a pohlížet na ni jako na zdravotnickou službu.

Žádná z podobných aplikací by nefungovala bez žádné z jednotlivých částí řetězce od zařízení k serverům, ovšem cloud servery v tomto případě jsou hlavním pilířem. Jedná se tedy o jakousi páteř většiny podobných zdravotnických aplikací, která nabízí databáze pro ukládání dat, služby pro datovou analýzu, bezpečnostní moduly pro zachování důvěrnosti a soukromí, API ke komunikačním standardům a další služby. Cloudy se obecně nyní velmi využívají pro mnoho aplikací realizovaných zpravidla jako SaaS (Software as a service), což má mnoho výhod. V tabulce 6.A je zhodnocena finanční rozvaha řešení IaaS (Infrastructure as a service), PaaS (Platform as a service) a populárním SaaS oproti řešení On-Premises. Řešení On-Premises znamená provozování aplikací na vlastních strojích či ve vlastních prostorách za použití dodaných či pronajatých prostředků.

Tabulka 6.A Finanční zhodnocení z pohledu jednorázových a pravidelných nákladů [26]

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

Nedávno několik hlavních aktérů v oblasti IoT a výzkumné komunity pro cloud řešení zahájili výzkumné práce s cílem podpořit a usnadnit vývoj, rozšiřování aplikací IoT včetně oblasti zdravotnictví. Každý subjekt postavil svůj přístup v závislosti na své vizi směrem k Internetu věcí. Vybraná sada platforem IoT zahrnuje: AWS IoT z Amazonu, Azure IoT Suite od společnosti Microsoft, Brillo / Weave od společnosti Google, Watson IoT od společnosti IBM a další. Tyto uvedené platformy budou více rozebrány dále. Byly vybrány na základě kritérií jako pověst dodavatelů v softwarovém a elektronickém průmyslu, podpora rychlého vývoje aplikací a počtu

aplikací v obchodě s ohledem na ty se zaměřením na zdravotní využití a podpory komunikačních protokolů jako MQTT a HL7 FHIR.

Navzdory tomu, že všechny platformy cílí na podobný cíl byly navrženy různé přístupy. Zejména vznikají následující otázky týkající se konstrukčních detailů těchto platforem:

- Jak každý zpracovává komunikační procesy mezi zařízeními IoT a cloud? Jaké jsou použité protokoly a techniky?
- Do jaké míry tyto rámce používají společné bezpečnostní normy?
- Jaké jsou bezpečnostní funkce nabízené každým prvkem či vrstvou?
- Jak každá platforma řeší problém zachování bezpečnosti a soukromí mezi všemi zúčastněnými stranami? Jaké jsou techniky používané k poskytování ověřování, autorizaci, řízení přístupu, kryptografie a dalších bezpečnostních prvků?
- Jak společnosti pracují se zdravotnickými komunikačními standardy a jaká je jejich podpora a propojenost s dalšími systémy?

Tato kapitola se zabývá odpověďmi na výše uvedené otázky pro každou platformu. Platformy budou také porovnány, aby byl získán ucelený obraz stávajících platforem IoT i s ohledem na zdravotnické aplikace, identifikovat trendy současných návrhů těchto platforem a poskytnout srovnání na vysoké úrovni mezi různými architekturami. Dále je za cíl ukázat výhody a nevýhody těchto platformy společně s prozkoumáním bezpečnostních prvkům. [27]

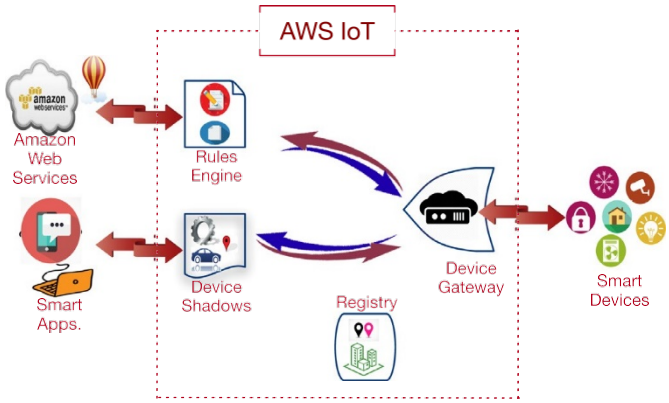
6.1. Amazon Web Services

Amazon Web Services (AWS) je cloud platforma od společnosti Amazon. Spadá pod ní i platforma AWS IoT pro Internet věcí. Cílem této platformy je nechat inteligentní zařízení snadno připojit a bezpečně spolupracovat s cloudem AWS a dalšími připojenými zařízeními. S AWS IoT je snadné používat a využívat různé služby jako Amazon DynamoDB, Amazon S3, Amazon Machine Learning, InterSystems IRIS for Health Community a další.

6.1.1. Architektura

Jak je znázorněno na obrázku 6.A, architektura AWS IoT se skládá ze čtyř hlavních komponent: Gateway, Engine Rules, Registr a Device Shadows

Zařízení Gateway funguje jako prostředník mezi připojenými zařízeními a cloudovými službami, které umožňují těmto zařízením komunikovat. Další funkce zajišťuje, že senzory a jiná embedded zařízení, která se pohybují a komunikují se zařízením Gateway, nemusí vědět, kdo jim posílá data. Prostě odesílají data definovanou trasou a ti, kteří se přihlásí k datům, ji obdrží. To umožňuje škálovatelné prostředí pro komunikaci s nízkou latencí, nízkou režií a obousměrnou komunikaci. Zabezpečená komunikace mezi zařízeními IoT a aplikacemi je zaručena, protože je využíváno TLS (Transport Layer Security), nástupce SSL (Secure Socket Layer). Gateway podporuje komunikační protokoly pro možné zdravotnické IoT aplikace jako MQTT, WebSockets a HTTP.



Obrázek 6.A Architektura AWS IoT [27]

Dále entita Engine Rules zpracovává příchozí publikované zprávy a poté je transformuje a předává dalším zařízením nebo cloudovým službám AWS pro další zpracování nebo analýzu. To umožňuje vytvářet aplikace IoT, které organizují, shromažďují, zpracovávají, analyzují a pracují na datech generovaných a publikovaných připojenými zařízeními v celosvětovém měřítku, aniž by musely dávat pozornost síťovým protokolům nízké úrovně nebo řídit jakoukoli infrastrukturu. V zájmu zachování použitelnosti mohou vývojáři vytvářet pravidla a přidávat je do modulu Rules Engine psaním příkazů podobných příkazům SQL nebo pomocí služby AWS Management Console. Engine Rules může přijímat data z více zdrojů, různých zařízení, a dokonce i z cloudu AWS. Integruje a přenáší tyto informace do dalších zařízení IoT a cloudových služeb AWS, jako jsou Amazon Kinesis, Amazon S3, Amazon DynamoDB atd.

Jednotka Registr odpovídá za přiřazení jedinečného identifikátoru ke každému připojenému zařízení bez ohledu na typ zařízení, dodavatele nebo způsob připojení. Také ukládá metadata (např. jméno zařízení, ID, atributy atd.) připojených zařízení, aby byla schopna je sledovat. Pokud zařízení již není aktivní a nezobrazuje se v síti po dobu 7 let, budou metadata odstraněna z registru.

AWS IoT vytváří instanci každého připojeného zařízení vytvořením virtuálního obrazu nazvaného Device Shadow. Tento „stín“ je trvalý a uložený v cloudu, aby byl dostupný a přístupný po celou dobu. Představuje poslední stav zařízení, když byl on-line, a vynucuje budoucí stav na fyzickém zařízení, jakmile se znovu objeví v síti. To znamená, že cloudové služby a další zařízení mohou integrovat, komunikovat a přečíst aktuální stav určitého zařízení prostřednictvím jeho „stínu“, i když je zařízení off-line. Čtení posledního hlášeného stavu a nastavení požadovaného budoucího stavu se provádí interakcí se Shadow zařízení pomocí rozhraní REST API nebo pomocí Engine Rules. Tato funkce pomáhá snadněji řídit zařízení a provádět akce na něm, aniž by musel být znám stav připojení. To znamená, že Shadow urychluje vývoj aplikací tím, že poskytuje jednotné a dostupné rozhraní pro zařízení, i když používají různé komunikační a bezpečnostní protokoly IoT nebo dokonce i když jsou omezeny přerušovanou konektivitou, omezenou šířkou pásma, omezenými výpočetními schopnostmi nebo omezeným napájením. Z programového hlediska je Device Shadow dokument JSON, který slouží k ukládání a získávání aktuálního stavu určitého zařízení.

AWS IoT poskytuje sadu SDK (Software Development Kit) pro zařízení, která usnadňuje zařízení synchronizovat svůj stav se Shadow a přijmout požadované budoucí stavy. Zejména AWS IoT Device SDK je sada knihoven, které pomáhají připojovat hardwarová zařízení, autentizovat s cloudem, instalovat mobilní aplikace a snadno vyměňovat zprávy.

AWS IoT neobsahuje žádná omezení týkající se programovacích jazyků vývoje inteligentních aplikací. Podporuje různé programovací jazyky včetně C a JavaScript. Uživatelé mohou využívat různé platformy (například mobilní telefony, notebooky atd.), aby mohli komunikovat se svými

zařízeními IoT připojenými v cloudu prostřednictvím API rozhraní REST. Stejné rozhraní je pak použito i pro aplikace počítačů a serverů, které mohou přistupovat ke Shadow zařízení v cloudu.

- **Specifikace hardwaru**

AWS IoT poskytuje zařízením klientské knihovny s open-source kódem a SDK, což zpřístupňují platformu pro několik embedded operačních systémů a mikro kontrolérů. Jakékoliv zařízení IoT se může tedy připojit ke cloudu AWS, pokud má možnost konfigurace pomocí některého z programovacích jazyků jako jsou C, Node.js či platformy Arduino. Dokonce i zařízení, která se připojují k soukromým sítím IP nebo komunikují pomocí protokolů jiných než IP (např. ZigBee) mohou přistupovat k cloudu AWS, pokud jsou připojeny k fyzickému rozbočovači. [27]

6.1.2. Bezpečnostní funkce

Amazon využívá vícevrstvou bezpečnostní architekturu pro AWS IoT, ve které je bezpečnost aplikována na všech úrovních technologie pro zajištění bezpečnosti soukromých či zdravotnických informací. Prvním krokem k bezpečnosti je autentifikace. Aby bylo vůbec možné připojit nové zařízení ke cloudu AWS IoT, musí být zařízení ověřeno. AWS IoT podporuje vzájemné ověřování ve všech bodech připojení, takže zdroj přenášených dat je vždy znám. Obecně platí, že AWS IoT poskytuje tři způsoby ověření totožnosti:

- Certifikáty X.509
- Uživatelé, skupiny a role služby AWS IAM
- Identity AWS Cognito

Nejčastěji používanou metodou pro autentizaci v AWS IoT jsou certifikáty X.509. Jedná se o digitální certifikáty, které závisí na kryptografii s veřejným klíčem, a měly by být vydávány důvěryhodnou stranou nazývanou certifikační autorita (CA). V našem případě jednotka zabezpečení a identity v cloudu AWS IoT funguje jako CA. Tyto certifikáty jsou založené na protokolu SSL/TLS, aby zajistily bezpečnou autentizaci. Požadavky HTTP a WebSockets odeslané do AWS IoT jsou ověřovány pomocí AWS Identity and Access Management (AWS IAM) nebo AWS Cognito. Oba jsou podporovanými metodami autentizace AWS a souhrnně se nazývají AWS Signature Version 4 (SigV4). Pro protokol HTTP je volitelné použít jednu ze všech možných metod k ověřování. Naproti tomu připojení pomocí WebSockets je omezeno pouze na použití SigV4 pro ověřování. [28]

Každé zařízení připojené k AWS IoT je ověřeno pomocí jedné z diskutovaných metod, které si zvolil koncový uživatel. Zprostředkovatel zpráv je zodpovědný za ověřování a autorizaci všech akcí na účtu uživatele. Zejména je zodpovědný za autentizaci všech připojených zařízení, bezpečného získávání dat zařízení a dodržování oprávnění k přístupu, které používají uživatelé na svých zařízeních.

Další krok je autorizace a kontrola přístupu. Proces autorizace v systému AWS IoT je založen na zásadách (policy-based). To může být aplikováno buď stanovení pravidel a zásad autorem pro každý certifikát nebo využití politik IAM. To znamená, že pouze zařízení nebo aplikace uvedené v těchto pravidlech mohou mít přístup k příslušnému zařízení, ke kterému patří daný certifikát. Tyto politiky mohou být zajištěny použitím Engine Rules. Ty se navíc v rámci AWS IoT řídí i zásadami co nejmenšího počtu privilegií pro zajištění vyšší bezpečnosti. Engine Rules mají dále za povinnost využívat systém řízení přístupu AWS k bezpečnému přístupu a přenosu dat do konečného cíle podle předem stanovených pravidel a zásad. Vlastník zařízení připojeného k cloudu tedy může v Engine Rules zavádět některá pravidla, která korigují možnosti přístupu některým zařízením nebo aplikacím k jeho zařízení. Použití politik AWS nebo politik IAM nabízí úplnou kontrolu nad vlastními zařízeními a reguluje právo ostatních na přístup k jejich schopnostem a provádění operací nad nimi.

Výsledná bezpečnost by byla znehodnocena, kdyby komunikace nebyla zabezpečena. Veškerá komunikace s AWS IoT je tak šifrována přes protokol SSL/TLS. TLS se používá k zajištění důvěrnosti aplikačních protokolů (MQTT, HTTP) podporovaných AWS IoT. Pro oba protokoly TLS šifruje spojení mezi přístrojem a Message Broker. Ve službě AWS IoT jsou podporovány mnohé šifrovací sady TLS, které zahrnují: ECDHE-ECDSA-AES128-GCM-SHA256, AES128-GCM-SHA256, AES256-GCM-SHA384 atd. Všechna soukromá data jsou zašifrovaně uložena pomocí symetrické šifrovací funkce (např. AES128). [27]

6.1.3. Zdravotnické služby

Jedna ze základních podmínek pro zdravotnickou cloudovou službu je i zajištění podpory pro HL7 FHIR, která je stěžejní pro budoucí zdravotnické IT aplikace. Amazon v rámci svých cloudových služeb AWS nabízí několik variant služeb i s podporou FHIR.

Hojně využívaná služba Amazon API Gateway, která se neustále vyvíjí a vývojáři rychle reagují na nové technologie, podporuje celou řadu technologií včetně těch potřebných k funkci FHIR jako RESTful API a HTTP. Ale přímou integraci s FHIR službou neprovádí. Jedná se o službu, která primárně zajišťuje přistup k datům z různých zdrojů a posílá je dále. Za pomocí konzole AWS Management Console je možné vytvářet například rozhraní RESTful API a WebSocket, které fungují jako „vchodové dveře“ pro aplikace pro přístup k datům z jakékoliv webové aplikace nebo komunikační aplikace v reálném čase. Je to služba typu pay-as-you-go, tedy se platí pouze za to, co se skutečně využívá. Platí se pouze za množství dat, které se předalo skrze API. Amazon API Gateway je možné použít s celou řadou dalších aplikací jako AWS IoT, Amazon DynamoDB a další Amazon služby. Jejich kombinací je tak možné dosáhnout kýžené využitelné aplikace. [29] [30]

Další možnost, kterou Amazon nabízí, je platforma InterSystems IRIS for Health. Jedná se o platformu zaměřenou přímo na zdravotnické služby. Ta poskytuje veškeré možnosti pro vytváření komplexních, kritických a náročných aplikací pro zdravotnické účely. Jedná se o komplexní platformu zahrnující správu dat, interoperabilitu, zpracování transakcí a analýzu. Vzhledem k rozmanitosti informací o zdravotní péči tato platforma umožňuje velkou škálu využití. Dále platforma InterSystems IRIS for Health poskytuje přirozenou podporu pro FHIR a všechny standardy pro poskytování důležitých zpráv ve zdravotnictví po celém světě. Umožňuje také vývojářům rychle a efektivně vytvořit aplikaci od nuly, vybrat z mnoha plánů financování i vhodné škálování k možnosti efektivně zpracovat jakékoli pracovní zatížení, objem dat nebo uživatel. [31]

6.2. Azure

Microsoft provozuje cloudové služby Azure. Jedna z nich je Azure IoT Suite, platforma složená ze sady služeb, které umožňují koncovým uživatelům komunikovat se svými zařízeními IoT, přijímat data z nich, provádět různé operace přes data (např. agregace, multidimenzionální analýza, transformace atd.) a vizualizujte jej vhodným způsobem pro mnoho účelů. Azure IoT podporuje širokou škálu hardwarových zařízení, operačních systémů a programovacích jazyků.

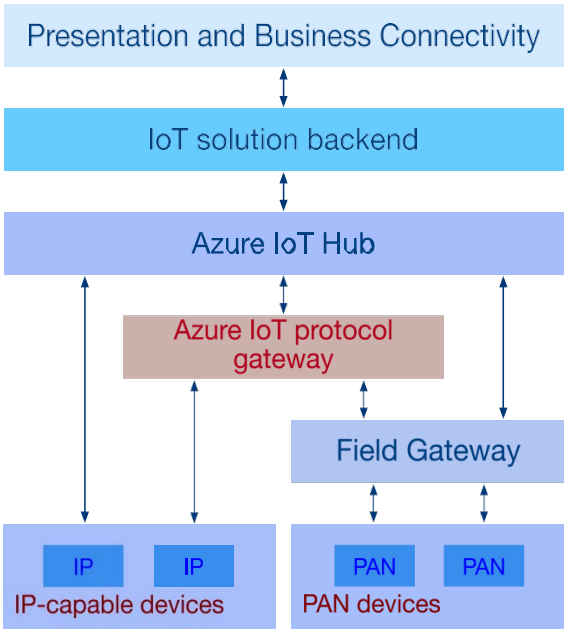
6.2.1. Architektura

Architektura Azure Cloudu je vrstvová. Na nejnižší vrstvě koncová zařízení komunikují s Azure Cloud přes předdefinovanou cloud gateway. Příchozí data z těchto zařízení jsou buď uložena v cloudu pro další zpracování a analýzu prostřednictvím cloudových služeb Azure nebo okamžitě

nabízené některým službám pro analýzu v reálném čase. Výstup obou směrů je prezentován a vizualizován přizpůsobeným způsobem, který odpovídá požadavkům zákazníků a jejich podnikání. Azure IoT Hub je webová služba, která umožňuje obousměrnou komunikaci mezi zařízeními a službami cloudu při zohlednění všech bezpečnostních požadavků. Azure IoT hub má Identity registry pro uchovávání informací o totožnosti a autentizaci jednotlivých zařízení. Má také jednotku Device identity management, která spravuje všechna připojená a ověřená zařízení.

Existují zde 2 třídy zařízení IoT: IP-capable a PAN. Zařízení IP-capable mají schopnost komunikovat přímo s Azure IoT Hub přímo jedním z podporovaných komunikačních protokolů. Azure IoT Hub nativně podporuje komunikaci prostřednictvím protokolů AMQP, MQTT nebo HTTP. Podpora dodatečných protokolů je možná přes Azure IoT protocol gateway. Brána umožňuje přizpůsobení protokolu a funguje tak jako obousměrný most. Field Gateway je jednoduše agregačním bodem pro zařízení v síti PAN. Vzhledem k tomu, že tato omezená zařízení nemají dostatečnou kapacitu pro spouštění zabezpečených relací protokolu HTTP, odesílají data do Field Gateway, aby je mohly agregovat, uložit a předat bezpečně do Azure IoT Hub.

Vyšší vrstva dále představuje širokou škálu služeb Azure Cloud (např. Azure Machine Learning a Azure Stream Analytics). Nejvyšší vrstva architektury Azure Cloud je prezentační vrstva. Uživatelé mohou volně vizualizovat své údaje, jak chtějí. Společnost Microsoft poskytuje službu Business Intelligence (BI), která efektivně a atraktivně prezentuje data a mnoho dalšího.



Obrázek 6.B Architektura Azure IoT [27]

Společnost Microsoft poskytuje různé sady SDK, které podporují různá zařízení a platformy IoT, aby se vývojáři mohli připojit k Azure IoT Hub a umožnit uživatelům spravovat jejich zařízení. Sada SDK zařízení IoT umožňuje vývojářům implementovat klientské aplikace pro širokou škálu zařízení, od jednoduchých síťových senzorů až po výkonné samostatné výpočetní zařízení. Programovací jazyky C, Node.js, Java, Python a .NET jsou podporovány právě v SDK.

- **Specifikace hardwaru**

Azure IoT podporuje širokou škálu operačních systémů a hardwarových zařízení. V každé zařízení musí vyhovovat následujícím minimálním podmínkám, aby bylo schopno komunikace s cloudem Azure IoT:

- Podpora TLS pro bezpečnou komunikaci
- Podpora SHA-256 pro účely autentizace
- Minimální požadavek na paměť RAM používanou modulem SDK je 64 kB
- Hodiny v reálném čase nebo je možné připojit se k serveru NTP. Je to důležité pro vytváření spojení s TLS a vytváření zabezpečených tokenů pro autentizaci.

Pouze zařízení s technologií IP mohou komunikovat přímo s Azure IoT Hub. Jiné limitované zařízení s nízkým příkonem se mohou připojit prostřednictvím Field Gateway, pokud splňují výše uvedené podmínky. Mezi kompatibilní operační systémy a platformy patří Windows, Android, Debian, OS Windows, IoT Core, Arduino, TI-RTOS a mnoho dalších. [27]

6.2.2. Bezpečnostní funkce

Azure IoT využívá výhod zabezpečení a ochrany soukromí zabudovaných do platformy Azure. V architektuře Azure IoT je bezpečnost začleněna do každé vrstvy a vynucena v každé složce ekosystému.

Autentizace uživatele či entity je důležitý bezpečnostní prvek. Vzájemné ověřování je nutná podmínka pro možné vytvoření spojení mezi zařízeními IoT a Azure IoT Hub. Pro zašifrování procesu handshakingu se používá protokol TLS (Transport Layer Security). K ověřování slouží digitální certifikáty X.509. Azure IoT takto vydá jedinečný klíč pro identifikaci zařízení pro každé nové zařízení. Přístroj se pak otestuje na Azure IoT Hub zasláním tokenu obsahujícího podpisový řetězec HMAC-SHA256, který je kombinací vygenerovaného klíče spolu s ID uživatelem vybraným zařízením.

Dále dochází k autorizaci a kontrole přístupu. Azure IoT využívá výhod Azure Active Directory, aby zajistil model autorizace na základě zásad (policy-based) pro data uložená v cloudu, což umožňuje snadný přístup, správu a audit. Tento model také umožňuje téměř okamžité odvolání přístupu k datům uloženým v cloudu a k připojeným zařízením. Azure IoT Hub kontroluje řadu zásad a pravidel pro přístup a následně uděluje či zamítá oprávnění připojených zařízení nebo inteligentních aplikací.

Dále je pro bezpečnost zcela klíčové, aby komunikace byla zabezpečená. Azure používá protokol SSL/TLS k šifrování komunikace a zajištění integrity a důvěrnosti dat. Identity Registry poskytuje bezpečné ukládání identit zařízení a bezpečnostních klíčů. Data jsou dále uložena buď v databázích DocumentDB nebo v databázích SQL, což dohromady s předcházejícími kroky zajišťuje vysokou úroveň ochrany soukromí. [27]

6.2.3. Zdravotnické služby

Microsoft ve své Azure Cloud aktuálně nemá přímo platformu zaměřenou na zdravotnické služby na rozdíl od jiný poskytovatelů cloudových služeb. Dále také neexistuje ani služba agregace pro konkrétní HL7 FHIR, ačkoliv v rámci Azure IoT je možné využít jak služeb protokolu MQTT, tak i RESTful API.

Na druhou stranu společnost Microsoft již nějakou dobu vyvíjí FHIR Server pro svůj Azure Cloud. Tento server bude také schopen mapovat zdroje přímo do Azure Active Directory (Azure AD) a bude schopen povolit řízení přístupu založené na rolích (Role-Based Access Control). Od konce roku 2018 se zaměřují na vývoj FHIR Serveru, který poskytují i jako volně dostupný projekt k dalšímu vývoji dalším vývojářům. Využili k tomu známy server GitHub, kde ho společnost Microsoft na konci roku 2018 vydala veřejně. Aktivita pravděpodobně vychází ze srpna 2018, kdy společnost Microsoft se společností Amazon, Google, IBM a dalšími společnostmi se zavázaly

odstranit překážky při zavádění technologií, které podporují interoperabilitu v oblasti zdravotní péče, zejména těch, které jsou podporovány prostřednictvím cloudu a umělé inteligence. [32]

6.3. Google Cloud

Společnost Google provozuje platformu Google Cloud. V rámci ní se nalézá několik platforem jako je například Brillo/Weave pro rychlou implementaci aplikací IoT. Platforma se skládá ze dvou hlavních zadních částí: Brillo a Weave. Brillo, nazýván také Android Things, je operační systém založený na androidu pro vývoj vestavěných zařízení s malým výkonem. Zatímco Weave působí jako komunikační vrstva pro interakce a zasílání zpráv. Hlavní úlohou Weave je zaregistrovat zařízení přes cloud a odesílat/přijímat vzdálené příkazy. Obě složky se navzájem doplňují a společně tvoří rámec IoT. Brillo/Weave se zaměřuje především na inteligentní domovy a rozšiřuje možnosti podpory obecných zařízení IoT.

6.3.1. Architektura

Architektura se skládá ze 2 dílčích částí Brillo a Weave. Brillo je lehký vestavěný operační systém založený na Androidu a plně implementován v programovacích jazycích C/C++. Skládá se z několika vrstev. Nejnižší je vrstva hardwaru dále poté vrstva jádra a nejvýše vrstva Android HAL (Hardware Abstraction layer). Android HAL je middleware, který překlenuje mezeru mezi hardwarem a softwarem.

Zatímco Brillo představuje segment nízké úrovně (OS) této architektury, Weave je vysoká úroveň. Jedná se o komunikační sadu protokolů a rozhraní API, které umožňují inteligentní telefony, zařízení IoT a cloud komunikovat navzájem. Kromě toho poskytuje služby pro ověřování, zjišťování, poskytování a interakci dat. Weave se řídí formátem JSON. Navíc Weave existuje jako mobilní SDK pro chytré telefony a jako cloudová webová služba. Aplikace Mobile SDK běží na telefonech s Androidem nebo iOS a je tak možné propojit mobilní aplikace k zařízením s Brillo. Mobilní aplikace tak mohou používat rozhraní API pro ovládání a správu připojených zařízení IoT. Weave podporuje více komunikačních a aplikačních protokolů.

Obecně vývojáři třetích stran mohou implementovat aplikace na libovolné platformě pomocí libovolného programovacího jazyka podporující Weave. Na druhou stranu by zařízení IoT měla fungovat na Brillo, aby mohlo komunikovala s inteligentními aplikacemi bez dalších požadavků.

- **Hardwarové specifikace**

Operační systém Brillo je kompatibilní pouze se zařízeními s mikroprocesorem (MPU), které mají minimální paměť alespoň 35 MB paměti RAM. ARM, Intel (X86) a MIPS jsou jedinou podporovanou architekturou [69].

Minimální hardwarové požadavky inteligentního zařízení pro hostování Brillo jsou:

- 32 MB RAM
- 128 MB ROM
- podpora jedné z následujících architektur: ARM, X86 nebo MIPS
- WiFi 802.11n
- Bluetooth 4.0+ [27]

6.3.2. Bezpečnostní prvky

K zajištění bezpečnosti byla udělena vysoká priorita od společnosti Google. Hlavním bezpečnostním prvkem je použití protokolů SSL/TLS. Weave plní hlavní funkce jako Discovery, provisioning, a autentizace zařízení a uživatele. Pro autentizaci jakožto klíčový prvek v bezpečnosti se používá protokol OAuth 2.0 spolu s digitálními certifikáty. Bez ohledu na cloudový server s povoleným Weave, který uživatel zvolil, poskytuje Google autentizační server. Další platformy Google Cloud využívají i Identity and Access Management (IAM) systém. [33]

Další klíčový prvek je autorizace a řízení přístupu. Právo přístupu je zajištěno jádrem Linuxu. Modul SELinux (Security Enhanced Linux) je zodpovědný za zajištění bezpečnostních zásad kontroly přístupu, v nichž majitel zařízení IoT může dle potřeby používat více úrovní řízení přístupu. Vynucení řízení přístupu se provádí přiřazením vlastních práv (čtení, spouštění, psaní) pro každého uživatele nebo skupinu uživatelů. Opět platí, že vzhledem k tomu, že tento rámec IoT je založen na Linuxu, používá se metoda sandboxing pro oddělování jednotlivých běžících procesů s ohledem na User ID a Group ID. Poskytuje zdokonalený mechanismus pro vynucení oddělení informací na základě požadavků na důvěrnost a integritu pro každý profil.

Zabezpečená komunikace je zajištěna službou Weave tím, že poskytuje protokol SSL/TLS zabezpečení na úrovni spojení. Kromě toho jádro Linuxu podporuje úplné zakrytí uložených dat. [27]

6.3.3. Zdravotnické služby

Společnost Google v rámci svých rozsáhlých cloudových služeb nabízí jak rámce čistě pro IoT jako zmíněný Brillo a Weave, tak i platformy rozvíjející činnost v oblasti zdravotnických služeb a jejich propojení s jinými platformami. Nazývají se Cloud Healthcare API a poskytuje řešení pro ukládání a přístup k datům zdravotní péče v Google Cloud. Jedná se o most mezi stávajícími systémy péče a aplikacemi provozovanými ve službě Google Cloud. Rozhraní API se skládá ze tří částí podle světově rozšířených standardů pro údaje o zdravotní péči:

- FHIR
- HL7v2
- DICOM

Důležitým aspektem pro cloudovou službu je dodržování platných norem. Každé rozhraní je zde podporováno datovým úložištěm splňující platné normy, které zajišťuje čtení, zápis, vyhledávání dat a další operace. V prostředí Cloud Healthcare API je tak každé datové úložiště specifické pro určitý způsob transportu a jeho přidružené rozhraní API v souladu s příslušnou normou. Tyto úložiště dat dále také poskytují propojení s Cloud Pub/Sub, který poskytuje čistý a bezpečný přístupový bod k integraci dalších aplikací. Za pomocí Cloud Pub/Sub integrace je možné použít získaná data skrze API k dalšímu zpracování, vizualizaci atd. Aplikace Cloud Healthcare API poskytuje řadu dalších funkcí, které jsou klíčové pro překlenutí současných technologií do nové generace systémů a aplikací zdravotní péče.

Dále FHIR ukládá implementaci STU3 s její aktuální verzí specifikace a DICOM ukládá implementaci DICOMweb, což je webový standard pro výměnu lékařských obrazů. Navíc tyto standardy DICOM a FHIR v rámci Cloud Healthcare API podporují hromadné importy a export dat, což usnadňuje přenos dat přes systém úložišť.

Dalším důležitým aspektem je dodržování zásad ochrany osobních údajů. Google poskytuje podrobné pokyny ohledně toho, jak podporuje dodržování předpisů HIPAA a dalších globálních standardů ochrany osobních údajů. Cloud Healthcare API také zpracovává umístění dat jako hlavní

součást API. Je možnost vybrat umístění úložiště pro každou datovou sadu ze seznamu aktuálně dostupných umístění, které odpovídají odlišným zeměpisným oblastem.

Bezpečnostní model Cloud Healthcare API je založen na ověřeném systému Google Identity and Access Management (IAM) mimo dalších opatření běžných i pro jiné cloudové platformy společnosti Google. Systém IAM dává úplnou kontrolu nad přístupem ke zdravotním údajům. [33]

6.4. IBM Cloud

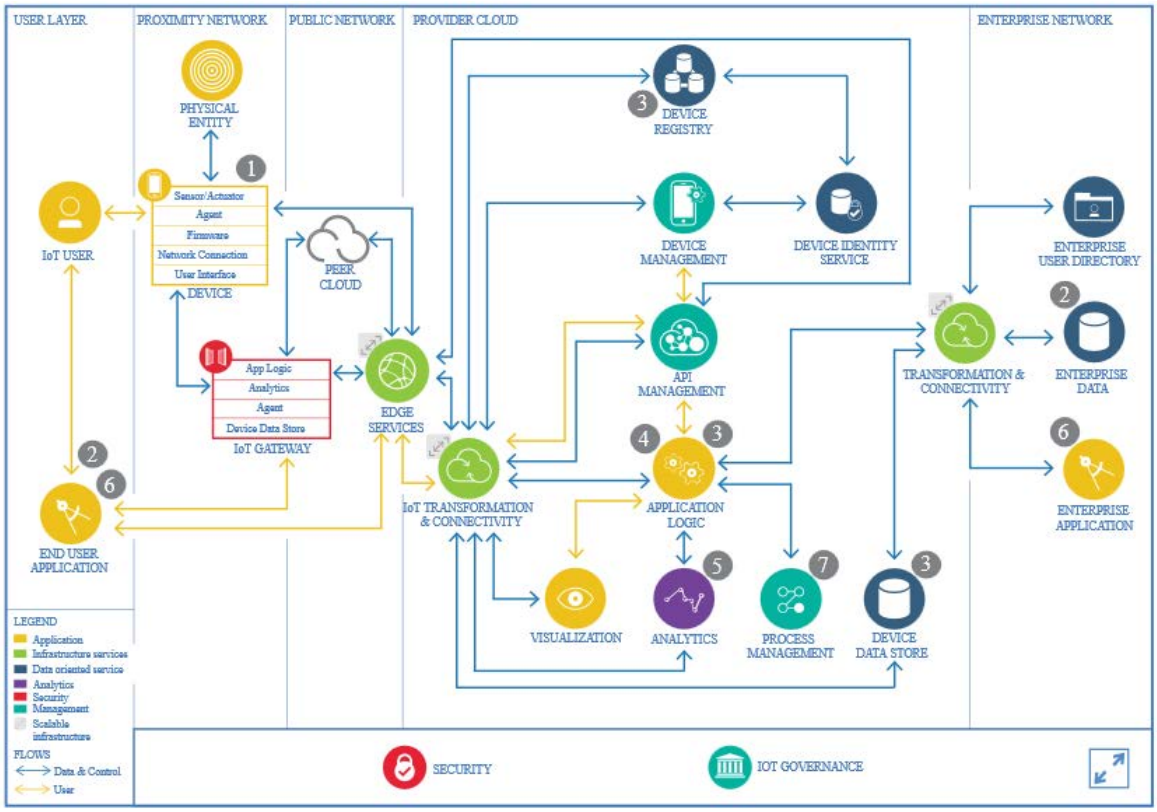
IBM je dlouhodobý hráč na poli cloudových služeb. Provozuje celý portál IBM Cloud obsahující nespočet platforem pro různá využití. Cloudová platforma IBM využívá jak platformu jako službu (PaaS), tak infrastrukturou jako službu (IaaS) k poskytování svých služeb zákazníkům. Platforma podporuje jak malé vývojové týmy, tak organizace a velké podniky. Řešení na IBM Cloud jsou celosvětově nasazeny v datových centrech po celém světě a spolehlivě fungují v testovaném prostředí.

Jednou z platforem IBM Cloudu je i platforma Watson IoT, která se zabývá aplikacemi v IoT. Platforma IBM Watson IoT je řízená hostovaná služba v cloudu určená k tomu, aby zaručovala snadnou správu zařízení IoT a jejich dat. Platforma Watson IoT a další doplňkové služby umožňují organizacím zachytit a prozkoumat data, zařízení a stroje a získat poznatky, které mohou přispět k lepšímu rozhodování či dalšímu využití. Platforma je uznávaná dále pro kognitivní analýzy, vícevrstvé zabezpečení, inovativní technologie a globální dostupnost pro místní i nadnárodní zákazníky. [34]

6.4.1. Architektura

Platforma Watson IoT se skládá z mnoha částí a je velmi komplexní. Celý referenční model této platformy je vidět na obrázku 6.C. Těmi hlavními jsou IoT Gateway, Edge services, Device registry, Application logic, API management a koncová zařízení.

IoT Gateway připojuje zařízení IoT a uživatelské aplikace k Edge services. Edge services poskytují schopnosti poskytovat obsah prostřednictvím internetu. Využívají služby jako DNS, firewall atd. Dále Device registry ukládá informace o připojených zařízeních, která může systém IoT využívat, komunikovat s nimi nebo je spravovat. Hlavní logika celé platformy je Application logic. Obsahuje komponenty základních aplikací, typicky koordinující manipulaci s daty zařízení IoT, provádění dalších služeb a podporu uživatelských aplikací. Součástí této části je i aplikace Node-RED. Dále API managementem inzeruje dostupné přístupové body služby. [35]



Obrázek 6.C Referenční model architektury platformy Watson IoT [35]

6.4.2. Bezpečnostní prvky

Bezpečnostní prvky musí zajišťovat jak zjištění skutečné identity zařízení, tak i zabezpečený přenos informace. Jednotlivé aspekty zabezpečení jsou založeny na často používaný principech jako jsou digitální certifikáty, Account management, Identity and Access Management (IAM) a další. [36]

Komunikační kanály jsou zabezpečeny standardně přes SSL/TLS protokoly, ačkoliv existuje podpora i mnoha dalších včetně IPSec a SSH. [37]

IBM Cloud poskytuje bezpečnou cloudovou platformu, což dokazuje i v součinnosti s bezpečnostními standardy. Platformy a služby v IBM Cloud dodržují standardy bezpečnosti včetně GDPR, HIPAA a ISO.

6.4.3. Zdravotnické služby

Pro zdravotnické aplikace v rámci IBM Cloudu je provozována IBM Watson platform for Health GxP. Platforma nabízí platformu pro poskytování zdravotních dat jako službu a pomáhá firmám zabývajícím se vědeckou praxí a zdravotnickým zařízením vytvářet inovativní digitální řešení a aplikace v oblasti zdraví, využívajících analytických funkcí, IoT a velkých dat. Platforma, dříve známá jako IBM Watson Health Core, nadále poskytuje zdravotní datovou platformu jako službu (PaaS), kterou mohou vědecké ústavy, společnosti zabývající se zdravotnickými zařízeními, výzkumníci a další využívat k vytváření inovativních řešení pro své klienty a zkrátit čas potřebný k implementaci. Dále také nabízí možnosti k tvorbě zdravotních aplikací v rámci IoT.

Pro platformu Watson for Health GxP byly provedeny příslušné kontroly v souladu s požadavky zákona HIPAA, aby zahrnovala příslušné administrativní, fyzické a technické záruky.

Platforma Watson for Health je navržena tak, aby zlepšovala zdravotní péči tím, že nabízí cloudovou infrastrukturu, která kombinuje shromažďování a zpracování zdravotnických informací z mnoha různých zdrojů díky velkému rozsahu APIs, a to včetně FHIR standardu s RESTful API. Samostatná API platforma jako IBM Watson Hub podporující FHIR neexistuje, ačkoliv je možné využít služeb RESTful API. [38]

Většinu zmíněných modulů včetně Watson for Health GxP používá firma IBM pro vývoj aplikací větších i menších rozměrů na zakázku. Proto s těmito moduly IBM Cloud standardně nedisponuje.

6.5. Cerner

Tato americká společnost je značně odlišná od předcházejících. Nejedná se totiž o velkou společnost v oblasti cloudových služeb jako Google či Amazon. Nýbrž se jedná o společnost zabývající se speciálně zdravotními informačními systémy a jejich využitím. Již nyní má za sebou mnoho úspěšných zdravotnických IT projektů pro velké organizace jako jsou například Truman Medical Centers, Pagosa Springs Medical Center a další. Napomáhají vyvíjet nové technologie v této oblasti pro rozvoj inteligentní zdravotní péče. Podporují řadu inovátorů, dodavatelů i klientů třetích stran k vývoji aplikací, které pracují napříč existujícími zdravotními záznamy. Zabývají se i oblastmi, které souvisí se zdravotnickými informačními systémy jako je hosting aplikací, cloudová uložiště a jejich zabezpečení, síťová zabezpečení a analýzou dat včetně elektronických zdravotnických informací (EHR).

Ale především sami nabízejí a provozují celou řadu zdravotnických aplikací pro komerční i nekomerční využití. Nabízejí také platformy, na kterých je možnost aplikace vlastní i třetích stran provozovat. Provozují platformy jako HealtheIntent a Cerner Millennium.

Platforma Cerner pro zdraví obyvatelstva HealtheIntent umožňuje zdravotnickým systémům agregovat a transformovat data v rámci zdravotní péče. Vytváří tak dlouhodobý zdravotní záznam pro jednotlivé členy populace. Platforma zpracovává data z interních a externích zdrojů, aby poskytovala ucelené informace umožňující organizacím identifikovat, vyhodnocovat a předvídat rizika jednotlivých pacientů. Organizace mohou tak sladit programy zdravotní péče, zlepšovat výsledky a snižovat náklady na zdravotní péči. Platforma dále podporuje aktivity, jako jsou komunitní péče, registry a populační zdravotní analýzy.

Na druhé straně platforma Cerner Millennium je komplexní platforma EHR. Společnosti Cerner slouží jako jediný zdroj informací pro klinické transakce s PHI. Využití rozhraní Cerner Ignited API pro Millennium umožňuje začlenit externí aplikace do procesů pracujících s EHR. Tato rozhraní API jsou Cerner implementací technologie SMART Health IT a standardu HL7 FHIR. [39]

6.5.1. Bezpečnostní prvky

Společnost Cerner přikládá velkou váhu i bezpečnosti. Jejich program pro zabezpečení se této problematice věnuje u všech Cerner platforem. Program se věnuje platformám jak z pohledu bezpečnostních politik a procedur, technické bezpečnosti a managementu systému, tak i managementu incidentů a dalších.

Program se řídí předpisy na ochranu osobních údajů, zabezpečení a řízení rizik s jasně definovanými rolemi, povinnostmi, postupy a politikou. Určuje například odpovědnost za zabezpečení a odpovědnost za údaje konkrétním jednotlivcům, popisuje přijatelné použití Cerner platforem,

definuje pravidla řízení přístupu, požadavky na autentizaci (IAM), autorizaci pomocí OAuth 2.0 a hesel pro koncové uživatele a administrátory. Dále popisuje protokolování, monitorování prostředí hostovaných v platformách Cerner a využití nástroje Security Information and Event Management (SIEM) k analýze a monitoringu protokolovacích záznamů. V neposlední řadě definuje i podrobný plán reakcí na bezpečnostní incidenty. Cerner pravidelně kontroluje a upravuje svůj bezpečnostní program tak, aby odrážel měnící se technologie, předpisy, zákony, rizika a další obchodní potřeby.

Cerner používá v rámci svého programu pro zabezpečení několik překrývajících se bezpečnostních aplikací a protiopatření k ochraně platforem. Níže jsou uvedeny některé příklady bezpečnostních technologií a postupů, které společnost Cerner zavádí pro ochranu platforem:

- Anti-Virus software je používán, podle potřeby, v celém hostitelském prostředí a aktualizace definic jsou nasazovány denně. Příchozí data jsou skenována v reálném čase a systémové jednotky jsou kontrolovány týdně.
- Síťové brány firewall jsou standardní součástí ochrany vnitřní síť a připojení kritické infrastruktury.
- Intrusion Prevention Systémy (IPS) jsou strategicky umístěny v infrastruktuře sítě, aby identifikovala škodlivé nebo anomální chování. Pro ověření správnosti fungování je zkontrolováno každé rozhraní brány firewall a každé hlavní spojení, které prochází sítí jádra platformy.
- Cerner úzce spolupracuje se svými poskytovateli internetových služeb, aby odhalil a bránil proti útokům typu Denial of Service (DoS).
- Externí přístup k aplikacím napříč veřejnými sítěmi je kontrolován na červy a viry před navázáním spojení s cílovým serverem. Požadavky jsou také filtrovány proti autorizovanému seznamu rizikových zdrojů.
- Servery jsou pravidelně aktualizovány pro účely zachování zabezpečení. Nové obrazy jsou načteny na všechny nové servery a na starších serverech podle potřeby.
- Cerner udržuje automatizovaný systémový inventář a opravný systém, který poskytuje přehled o změnách systému (Patch Management). Cerner získává aktuální oznámení o opravách prostřednictvím partnerů a testuje opravy pomocí různých procesů před použitím oprav v reálném provozu v rámci příslušné platformy.
- Cerner udržuje oddělené odpovídající logické a fyzické úrovně svých vývojových, testovacích a klientských prostředí.

Cerner používá k ochraně dat řádné šifrovací mechanismy. Data jsou šifrována jak při přenosu mezi klientem a serverem, tak i v Cerner datacentrech. Cerner využívá asymetrického šifrování jako je princip veřejného a privátního klíče. Cerner se snaží používat i algoritmy FIPS 140-2, pokud je podporován kryptografickým modulem. Cerner také podporuje šifrovací protokoly Advanced Encryption Standard (AES) a Transport Layer Security (TLS).

Cerner pravidelně provádí interní hodnocení a podrobuje se externím auditům pro ověření, že společnost pracuje efektivně v souladu s programem pro zabezpečení. Společnost dále provádí každoročně penetrační testování vlastními bezpečnostními pracovníky i externími společnostmi. Cerner také zavedl a udržuje potřebné kontroly pro dodržování pravidel HIPAA včetně každoročních kontrol. [40]

6.5.2. SMART on FHIR

Cerner se také velmi zabývá technologií FHIR a věnují se jak implementaci komplexní FHIR platformy, tak zjednodušování implementace zdravotnických aplikací za pomocí nadstavby SMART nad rámec technologie FHIR.

Platforma SMART (Substitutable Medical Apps and Reusable Technology) definuje specifikaci elektronického zdravotního záznamu (EHR) pro bezpečné otevírání jinými aplikacemi. Tyto aplikace SMART jsou běžně webové aplikace, ale mohou být také nativní mobilní aplikace, které používají standard HL7 FHIR ke čtení a zápisu dat z elektronických zdravotnických systémů. Cerner věří, že aplikace SMART budou hlavním uživatelem FHIR zdrojů a že budou klientům poskytovány jako Software as a Service (SaaS) model. To znamená, že aplikace SMART je hostována a spravována vývojářem či poskytovatelem služby. V tomto případě tak nemusí klienti instalovat žádný kód ani balíček, aby mohli implementovat konkrétní aplikaci. Cerner také podporuje přístup k FHIR prostřednictvím mobilních aplikací SMART. [41]

Společnost se dále skrze program Cerner Open Developer Experience snaží dosáhnout očekávání trhu v oblasti otevřené zdravotnické komunikace a zlepšit spolupráci s vývojáři třetích stran a klienty SMART on FHIR aplikací. Hlavní výhodou společnosti je rozsáhlé množství již existujících vlastních i externích aplikací. Veškeré aplikace je nejprve možné odzkoušet na funkčních demo serverech „SMART on FHIR Sandbox“ či „SMART Health IT Sandbox“ a ověřit správnou funkčnost vytvořené aplikace před jejím uvedení do ostrého provozu na Cerner serverech. Cerner má k dispozici několik FHIR serverů lišící se konkrétní specifikací zabezpečení či přístupu. Všechny vychází z verze DSTU 2 Final (1.0.2) standardu FHIR. Celý vývojový proces implementátorů aplikací je podpořen rozsáhlou vývojářskou komunitou a detailními specifikacemi. [39]

Pro jednodušší implementaci zdravotnické aplikace jsou k dispozici i open-source FHIR klienti. Ty se starají o autorizaci pomocí OAuth 2.0, obsahují zabudované knihovny pro volání a přístup k FHIR zdrojům a další nástroje. Klienti jsou k dispozici hned v několika verzích a skriptovacích jazycích jako Java, .NET, Python či iOS. [41]

6.6. Porovnání

Pro vytvoření aplikace cloudové služby k zařízení pro detekci mikro pohybů je potřeba vzdálenější pohled na celou problematiku. Jedná se totiž o komplexní aplikaci s aspekty z prostředí jak IoT, tak i zdravotnických služeb. Každá část má svá specifika a je nutné přihlížet k obou částem. Oblasti, které se týkají zmíněné problematiky u poskytovatelů cloudových služeb jsou bezpečnost, komplexnost a zapojení dalších aplikací a platforem, připravenost stávajících technologií, jejich vývoj a rozvoj včetně FHIR, složitost implementace a cena.

Bezpečnost je u rozebraných platforem na vysoké úrovni. Společnosti cítí, že tato oblast je pro IoT i čistě zdravotnické aplikace velkým tématem a významně se o něj zajímají, a to i na základě poptávky zákazníků. Problém bezpečnosti je u zdravotnických IoT aplikací o to vyšší. Všechny zmíněné platformy používají složitější více vrstvý model bezpečnosti. Ty tak podporují bezpečné a již časem ověřené způsoby pro autentizaci a kontrolu přístupu jako je například použití certifikátů X.509 či identity and access management (IAM), ačkoliv některé aspekty využití se u jednotlivých platforem mohou lišit. Přestože vlastní bezpečnostní model může být v některých aspektech rozdílný, sledují však stejný trend a v mnoha aspektech prosazují stejné standardy zabezpečení. Principy zabezpečení samotné komunikace mezi prvky sítě protokoly SSL/TLS jsou již ověřenou a fungující věcí, na které staví všechny platformy. U velkým cloudových poskytovatelů se předpokládají i záruky dostupnosti v případě nedostupnosti jednoho ze serverů například kvůli DoS útoku. Dostupnost dat pro koncové uživatele je tak zaručena ze sekundárního serveru, což menší poskytovatelé zpravidla zaručit nemohou.

Obecně je možné říci, že v oblasti bezpečnosti se platformy příliš neliší. Teoreticky se zdá, že prezentované bezpečnostní architektury jsou proti potenciálním hrozbám imunní. Prakticky vždy se

vyskytují významná bezpečnostní rizika, která se mohou časem vyskytnout, pokud nejsou dodržovány osvědčené postupy v užívání, návrhu a implementaci. Souhrn vlastností jednotlivých poskytovatelů cloudových služeb je shrnut v tabulce 6.B.

Komplexnost poskytovaných služeb je vždy závislá na konkrétní vybrané platformě. U aplikací čistě z oblasti IoT nabízí většina poskytovatelů velké množství komplexních aplikací a služeb. Je to dáno tím, že oblast IoT se rozvijí již delší dobu a poskytovatelé služeb měli dost času nabídnout zákazníkům komplexní řešení jejich problémů jako například Azure IoT, Watson IoT atd. Z oblasti týkající se i zdravotnictví není vývoj u těchto poskytovatelů ještě tak daleko, jelikož se jedná o vcelku nové téma posledních let. Poskytovatelé se i přesto zabývají rozvojem zdravotnických aplikací nejen na bázi FHIR. Nyní stále někteří poskytovatelé nabízí pouze platformy různých API podporující FHIR, které ovšem nemusí nijak zajišťovat komplexní podporu napojenou na další bezpečnostní prvky ke zdravotnické službě. Ty také ne vždy zajišťují bezproblémové napojení na další aplikace poskytovatele. Zpravidla to bývají služby typu pay-as-you-go. Těmto API službám se vymyká služba Cloud Healthcare API od Googlu, která navíc zajišťuje přímé napojení na další služby a datová úložiště včetně splňujících norem pro nakládáním s PHI.

Na druhou stranu někteří poskytovatelé nabízí komplexní možnosti platforem přímo určených ke zdravotnickým účelům. Tyto služby jsou určeny pro velkou škálu využití. Jsou vždy s plnou podporou nejnovějšího standardu FHIR s napojením na úložné diskové jednotky a v souladu s aktuálními právními normami. Tím se vyznačuje především společnost Amazon s platformou InterSystems IRIS for Health a společnost Cerner s platformou Millennium, která se zaměřuje především na možnosti zdravotnických SMART on FHIR aplikací. Společnost IBM sice nabízí podobné platformy jako konkurence, ovšem povětšinou pro aplikace na zakázku.

Tyto společnosti mají potenciál i v dalším rozvoji služeb ve zdravotnictví. Mají kapacity na tento rozvoj díky své velikosti a globálnímu dosahu a významně se touto oblastí včetně standardu FHIR zabývají. Dokonce se minulý rok sešli na konferenci CMS Blue Button 2.0 Developer Conference, kde se vedoucí pracovníci v oblasti zdravotnických informačních technologií shodli na společných základních bodech rozvoje eHealth. [42] Ovšem mnoho z nich se stále ještě nalézá ve fázi vývoje a jejich produkt není plně připraven na komerční využití. Hlavní výjimkou je společnost Cerner, která má vlastní platformy s FHIR velmi rozvinuté a má za sebou i celou řadu úspěšných a velkých zdravotnických projektů. Je to dáno i tím, že tato firma se zaměřuje na rozdíl od ostatních porovnávaných především na oblast zdravotnických aplikací.

Tabulka 6.B Souhrn poskytovatelů cloudových IoT služeb [27]

IoT platforma /Společnost	AWS IoT /Amazon	Brillo/Weave /Google	Azure IoT /Microsoft	Watson IoT /IBM
Komponenty architektury	+ Cloud services + Device Gateway + Rules Engine + Registry Unit + Device Shadow + Smart zařízení	+ OTA servery + Cloud služby + Zařízení s Brillo/Android jako OS	+ Cloud backend + Cloud služby + Cloud Gateway + Smart zařízení	+ IoT Gateway + Edge služby + Device registry + API management + Zařízení
Programovací jazyk	Libovolný jazyk může používat RESTful API	Libovolný jazyk může komunikovat skrze Weave SDK	+ C + Node.js + Java + Python + .Net	Libovolný jazyk může používat RESTful API
Podporované aplikační protokoly	+ HTTP + WebSockets + MQTT	+ HTTP + XMPP	+ HTTP + MQTT + AMQP	+ HTTP + MQTT
Podporované komunikační protokoly	Všechny používané	+ WiFi + BLE + Ethernet	+ WiFi + ZigBee + Z-wave a další	Všechny používané
Zabezpečení a autentizace	+ X.509 certifikáty +AWS IAM +AWS Cognito	+ OAuth 2.0 + Google IAM u dalších platforem	+ X.509 certifikáty + HMAC-SHA256 dig. podpis	+ digitální certifikáty + IBM Cloud IAM
Kontrola přístupu	+ IAM role + Rules Engine + Sandboxing	+ SELinux + ACL + Sandboxing: UID&GID	Azure Active Directory Policies + Access control rules v Azure IoT hub	+ IAM role
Zabezpečení komunikace	SSL/ TLS	SSL/TLS	TLS/DTLS	SSL/TLS
Zdravotnické služby	InterSystems IRIS for Health	Cloud Healthcare API	-	Watson for Health GxP

7. Implementace experimentální cloudové služby z pohledu IoT

Cílem této práce je navržení a realizace experimentální cloudové služby pro přenos, zpracování a vizualizaci dat z IoT senzoru detekce pomalých pohybů na bázi Dopplerova radaru. Tato práce přímo navazuje na projekt studenta Lukáše Gregory. Součástí tohoto projektu byla realizace senzoru pro detekci mikro pohybů kosterního svalstva na bázi Dopplerova radaru s využitím embedded platforem. Na základě výstupů z tohoto projektu jsou v rámci mé práce plánovány vstupy a zpracování dat pro experimentální cloudovou službu. Předěl se nachází ve výměnném bodě, který je zde představován zařízením Raspberry Pi, kde dochází k předání citlivých dat ze zmíněné přidružené práce, která do tohoto zařízení zasílá změřená data v přesně daném formátu. Tento formát závisí na partnerském projektu, ale nejvhodnějšími formáty jsou JSON či XML z důvodů absence nutnosti dalšího zpracování.

Tyto práce nejsou dále nijak více spojeny a práce probíhaly odděleně. Tato práce dále vychází ze sekce Způsoby implementace pro oblast IoT a jejich protokolů včetně MQTT protokolu. Tato problematika byla rozebrána v této práci výše.

Použité nástroje:

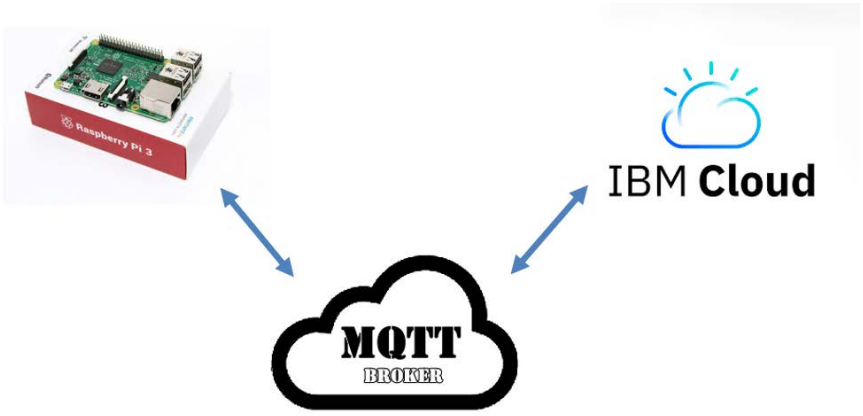
- Zařízení Raspberry Pi 3
- Aplikace Node-RED
- Cloudová služba IBM Cloud
- Webová aplikace CloudMQTT

7.1. Postup práce

7.1.1. Obecná analýza

Tato práce se stávala ze zásadních 3 sekcí. První část byla zařízení Raspberry Pi, které bylo využíváno k předcházejícímu projektu a stalo se tak výměnným bodem mezi oběma řešeními. Na tomto zařízení bylo potřeba vytvořit funkční aplikaci, která bude schopna data získaná do zařízení správně zpracovat dle požadavků a druhu dat a vhodně vykreslit. Vykreslování v tomto zařízení nemusí být nutně velmi složité. Stačí i jednoduší výstup o hodnotách dat. Další část projektu se týká transportu dat do cloudové služby, kde bylo vícero možností, jak toto realizovat, a bylo to hlavní částí této práce. Třetí část bylo samotné fungování služeb v cloudu, kde by data byla dále zpracována, ukládána a prezentována vyspělejší formou.

Na obrázku 7.A je vyobrazena základní jednoduchá topologie projektu rozdělená do zmíněných 3 částí. Tyto jednotlivé části budou dále v dokumentu rozebrány detailněji.



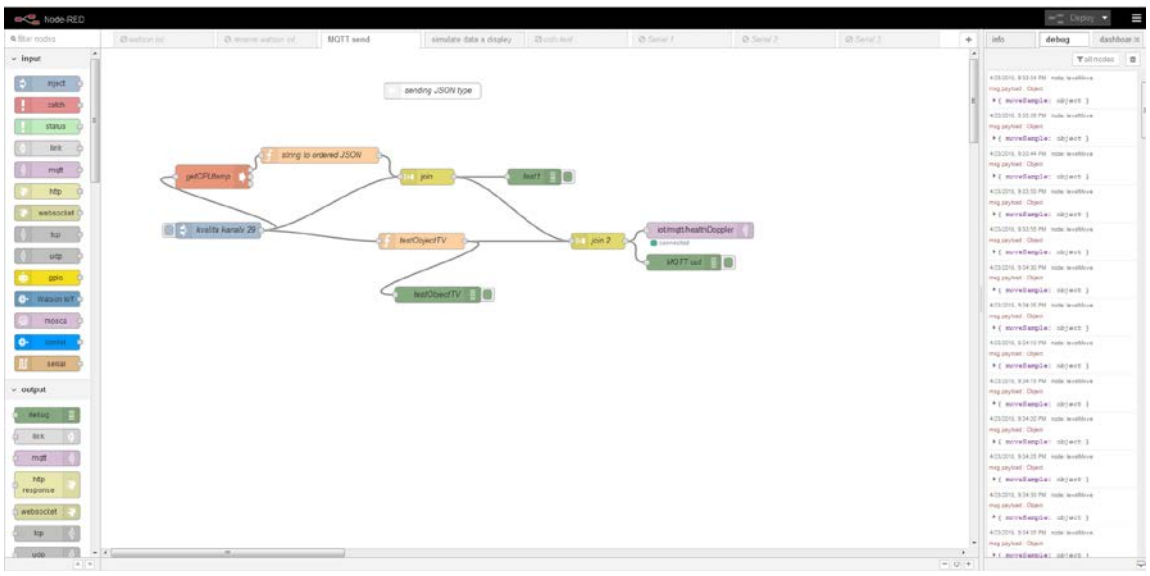
Obrázek 7.A Topologie spojení [43]

7.1.2. Node-RED

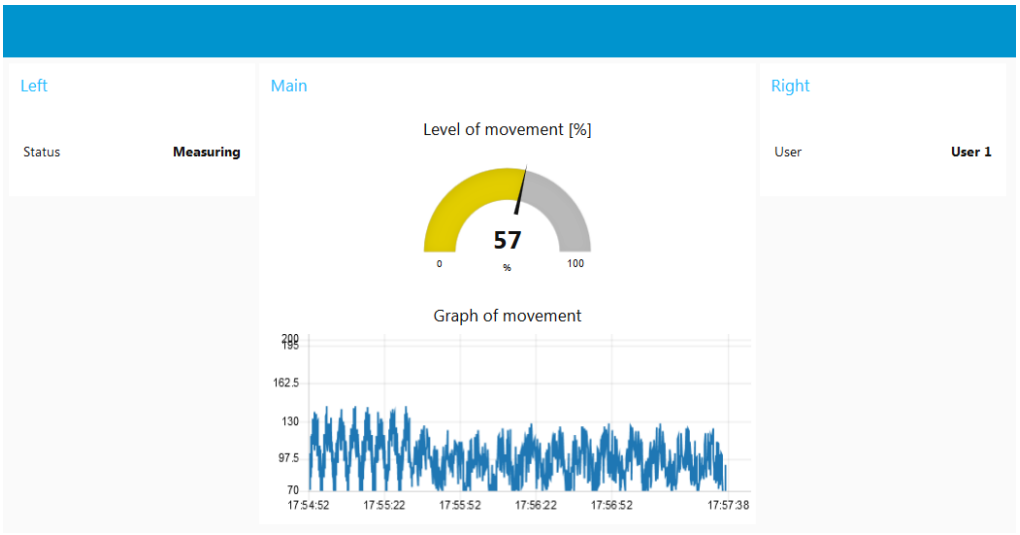
Pro 1. část Raspberry Pi bylo potřeba najít a zprovoznit aplikaci, která by zvládala potřeby jak zpracování a transportu dat, tak i jejich vizualizaci. Nejvhodnějším adeptem se jevila aplikace Node-RED. Tato aplikace je přímo určená pro nejrůznější druhy IoT aplikací. Jedná se o vývojový nástroj s velkou řadou funkcionalit a funkční na mnoho platformách. V operačních systémech založených na Linuxu je tato aplikace snadno doinstalovatelná a v operačním systému Raspbian, který je určený pro Raspberry Pi je přímo integrovaná. Node-RED je možné zprovoznit i v dalších operačních systémech.

Velká výhoda Node-RED je ve snadné konfiguraci a programování, které se skládá ze sestavování funkčních bloků za sebe. Tyto bloky je možné přidat přímo pro specifickou činnost. Aplikace je velmi hojně podporována dalšími vývojářskými firmami, kteří do ní implementují jejich vlastní služby jako volitelné funkce. Aplikace je také schopná jakéhokoliv dalšího programování v Javascript.

Z těchto důvodů je Node-RED používán i v řadě další komerčních i nekomerčních projektů v oblasti Internetu věcí a senzorových sítí.



Obrázek 7.B Ukázka aplikace Node-RED



Obrázek 7.C Ukázka vizualizace dat aplikací Node-RED

Ze zmíněných důvodů byla v tomto projektu tato aplikace implementována v zařízení Raspberry Pi a také jako cloudová služba na serverech IBM Cloud, které ji podporují. Tyto 2 instance aplikace jsou úplně totožné, i přestože každá běží na jiném druhu zařízení. Čím se tyto 2 instance liší, musely být konkrétní skripty, jelikož každá z nich byla nasazena na jiném místě a měly tedy i jinou funkci.

Pro Node-RED na zařízení Raspberry Pi bylo nutné sestavit skripty, které budou mít následující funkcionalitu:

- Přijímat data z portu zařízení
- Základní zpracování dat
- Základní vizualizace dat
- Přeposlání dat do cloudové služby

V cloudové aplikaci Node-RED běžící na serverech IBM cloud bylo nutné implementovat skripty, které budou mít následující funkcionalitu:

- Přijímat data z Raspberry Pi
- Zpracování dat
- Vizualizace dat
- Ukládání dat do databáze

Aplikace byla také nainstalována na domácí PC, které sloužilo jako testovací zařízení, na kterém byly všechny skripty programované a odzkoušené.

7.1.3. MQTT

Na to, aby spolu mohli 2 nezávislé instance aplikace Node-RED komunikovat, bylo zapotřebí prostředníka. Využit byl k tomuto účelu protokol MQTT (MQ Telemetry Transport). Tento protokol je přímo určen pro komunikaci v rámci IoT prostředí. Jedná se o protokol, který nabízí nenáročný přenos malého množství dat prostřednictvím TCP/IP sítě. Díky tomu je vhodný pro lokální či veřejné IoT projekty. Původně byl navržen v IBM. Nyní ho zastřešuje konsorcium „Eclipse foundation“ a je již také standardem dle OASIS. Detailněji i s principem fungování byl popsán v samostatné kapitole výše.

Pro komunikaci bylo nutné vytvořit MQTT brokera. Jedná se o jednoduché „přemostění“ mezi poskytovatelem informace a příjemcem. MQTT broker je tedy jednoduchý server v síti TCP/IP, přes kterého jsou přeposílány informace a poskytovatel i příjemce se k němu mohou připojit. Je důležité zmínit, že každý odběratel může být zároveň i příjemce a naopak. Detailnější problematika MQTT byla vysvětlena výše.

V tomto projektu byl v roli poskytovatele dat aplikace Node-RED běžící na zařízení Raspberry Pi a v roli příjemce instance Node-RED běžící jako cloudová služba. Variant MQTT brokera bylo vícero a jsou popsány dále.

- **Varianty MQTT brokera**

MQTT broker je nabízen mnoho společnostmi a v různých variantách, ovšem základní samotná funkce není zpravidla nijak odlišná. MQTT brokera je možné si pronajmout separátně jako například na webu CloudMQTT [44] nebo může být implementován jako služba v rámci cloudových aplikací. Pro tuto práci je možné využít obou možností, jelikož funkci plní stejně. Rozdíl mezi nimi je v způsobu placení za fungování brokera. Samotné weby nabízí varianty bezplatné s velmi omezenými možnostmi i placené více viz tabulka 7.A.

Tabulka 7.A Cenová nabídka webu CloudMQTT [45]

Verze	Cute Cat	Humble Hedgehog	Keen Koala	Loud Leopard	Power Pug
Cena za měsíc [$]	Zdarma	5	19	99	299
Počet spojení	5	25	100	1000	10000
Max. přenosová rychlost [kbit/s]	10	20	Bez limitů	Bez limitů	Bez limitů

Větší cloudová centra jako IBM nabízí služby MQTT broker v rámci balíčků či separátně viz tabulka 7.B. Služba MQTT brokera na IBM Cloud se nazývá Internet of Things Platform, která funguje opět na stejném principu MQTT protokolu, i když nabízí navíc mnoho dalších funkcí a například i přímé propojení do aplikace Node-RED.

Tabulka 7.B Cenová nabídka Internet of Things Platform [46]

Verze	Lite	Standard	Advanced Security
Cena za přeposlaný MB [€] (200 MB zdarma)	Zdarma	0,000965 (do 449 MB) 0,000675 (450 – 6 999 tis. MB) 0,000135 (+7 000 tis. MB)	0,000978 (do 449 MB) 0,000684 (450 – 6 999 tis. MB) 0,000137 (+7 000 tis. MB)
Počet spojení	500	Bez limitů	Bez limitů

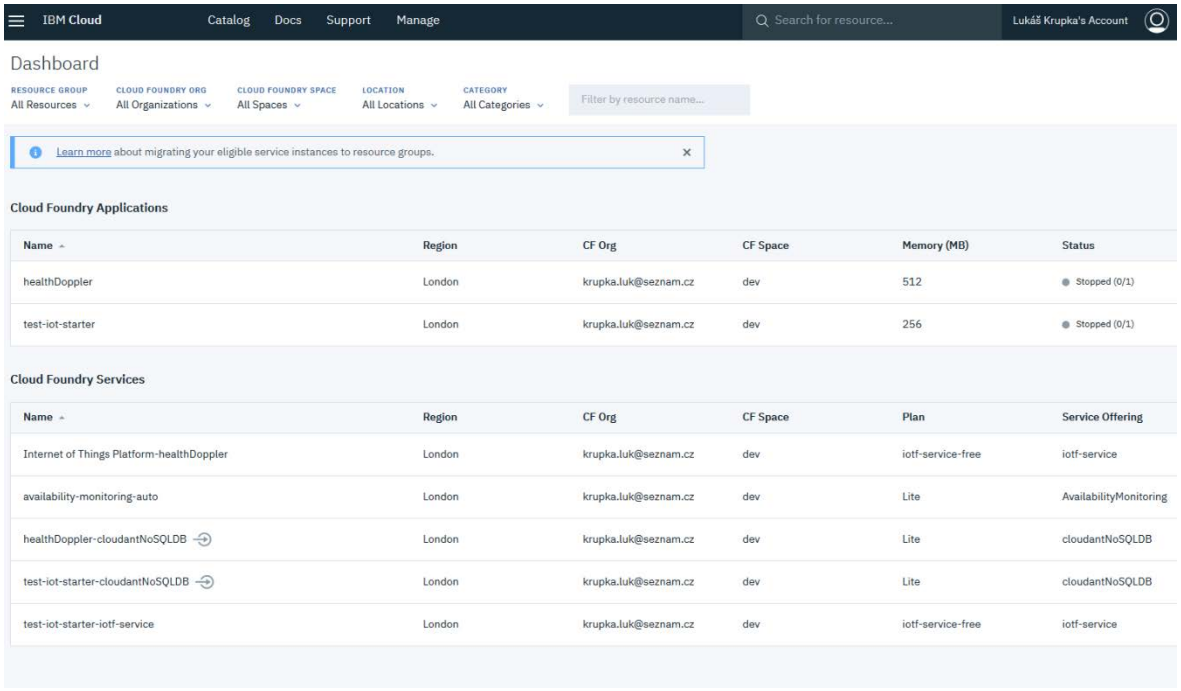
V rámci práce byly zprovozněny obě řešení, ovšem bez viditelných rozdílů ve výsledku mezi nimi. První řešení má nedostatky v omezené přenosové kapacitě a v absenci dalších funkcí. Druhá varianta je zase na druhou stranu složitější na implementaci. Otázka cenové politiky je problematická bez dlouhodobého plánu využití, který by vyžadoval další zkoumání, a není tedy momentálně možné rozhodnou, která varianta by vyšla levněji.

7.1.4. IBM Cloud

Třetí část projektu bylo navržení a realizace cloudové služby pro zpracování a vizualizaci dat z IoT senzoru. Ta byla realizována na serverech IBM Cloud, které nabízejí jak celou škálu aplikací pro IoT jako Node-RED, tak i službu MQTT brokera pod jejich názvem Internet of Things Platform. Aplikace byla realizována jako SaaS (Software as a service), což má mnoho výhod jak v oblasti implementace, tak i finanční.

Do této práce byla na IBM Cloud vytvořena instance Node-RED s názvem healthDoppler s následujícími parametry:

- Paměť na instanci 512 MB
- Propojení se službami:
  - availability-monitoring-auto
  - healthDoppler-cloudantNoSQLDB
  - Internet of Things Platform-healthDoppler



Obrázek 7.D IBM Cloud Dashboard aplikací a služeb

Společně s ní byly vytvořeny služby monitoringu aktivity, MQTT brokera a databáze NoSQL. Na obrázku 7.D je vyobrazen seznam funkčních aplikací a služeb zprovozněných na IBM Cloud. Databáze byla propojena s aplikací Node-RED a veškerá příchozí data jsou do ní ukládána. Některé základní funkce lze provádět již z grafického rozhraní a jiné je nutno konfigurovat textově. Některé vytvořené služby jsou zdarma. Cenové možnosti databáze Cloudant NoSQL jsou zaznamenané v tabulce 7.C.

Tabulka 7.C Cenová nabídka Cloudant NoSQL DB na IBM Cloud [46]

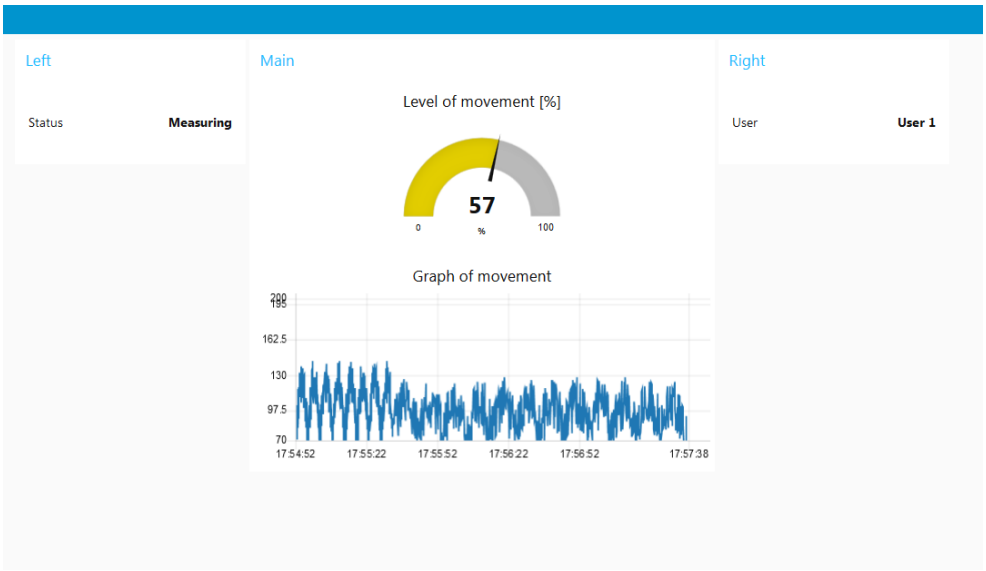
Verze	Lite	Standard	Dedikovaný hardware
Cena za měsíc [€]	Zdarma	0,7522 /GB dat. Úložiště navíc 0,188 /prohledání za sekundu navíc 0,3761 /zápis za sekundu navíc 3,76 /dotaz za sekundu navíc	3 761 / zařízení
Datové úložiště [GB]	1	20	-
Počet prohledání za sekundu	20	100	-
Počet zápisů za sekundu	10	50	-
Počet dotazů (queries) za sekundu	5	5	-

7.2. Výsledky

Celá práce na cloudové službě pro zdravotnické zařízení se skládá z hlavních 3 výstupů, které dávají dohromady celou funkční experimentální cloudovou službu pro zpracování a vizualizaci dat z IoT senzoru na bázi Dopplerova radaru k detekci pohybů kosterního svalstva.

7.2.1. Vizualizace na Raspberry Pi

První částí je vizualizace dat získané do Raspberry Pi. Tyto data byly zpracovány a vykresleny do základního grafického prostředí aplikace Node-RED. Na obrázku 7.E je především vidět aktuální hodnota a časový průběh během posledních 3 minut. Tento grafický výstup se předpokládá jako výstup přímo z Raspberry Pi, který může být zobrazen vzdálenou plochou či přímo připojeným displejem k zařízení.



Obrázek 7.E Grafický výstup aplikace Node-RED v Raspberry Pi

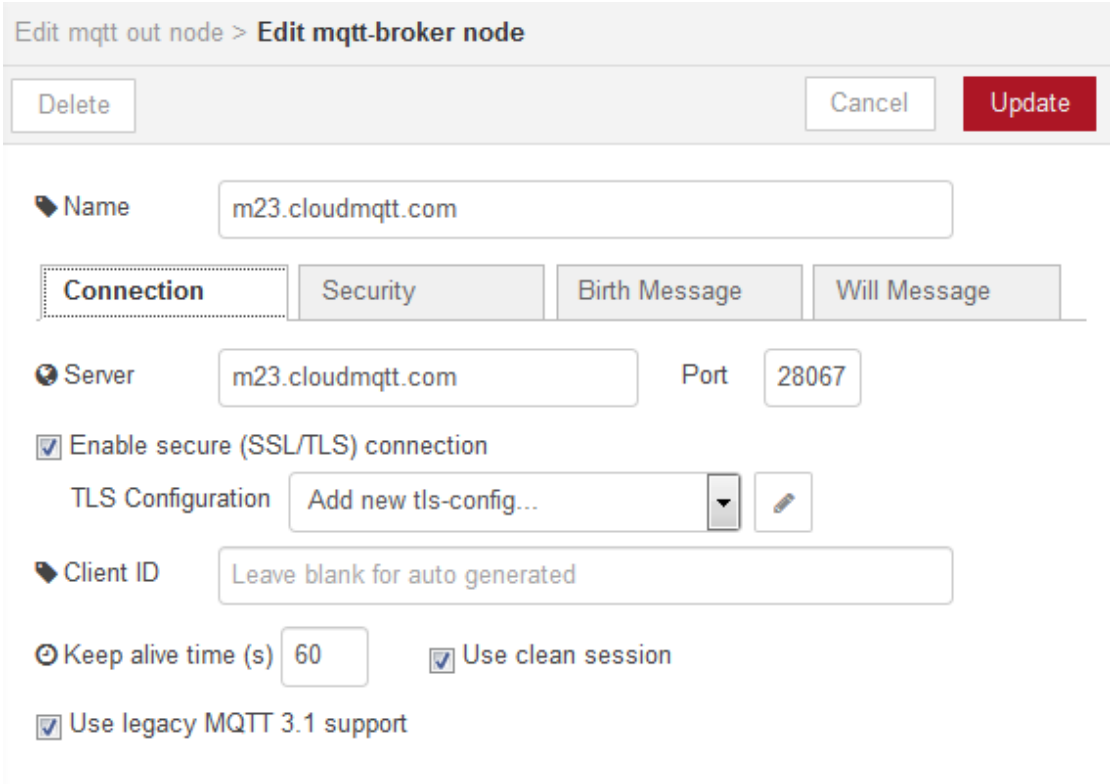
7.2.2. Spojení přes MQTT broker

Spojení je realizováno na straně Raspberry Pi v prostředí aplikace Node-RED s flow skriptem pro publikování dat do MQTT brokera s bloky vyobrazeny na obrázku 7.H a s parametry v tabulce 7.D. Data jsou zasílána ve formátu JSON, který obsahuje aktuální hodnotu a časovou značku.

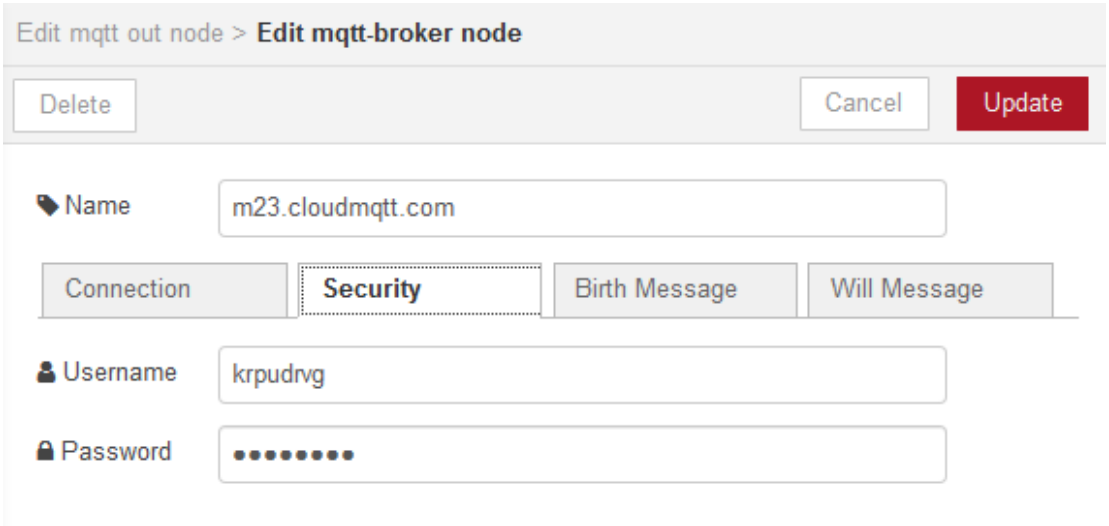
Tabulka 7.D Parametry MQTT brokera [44]

	Parametry MQTT brokera
Server	m23.cloudmqtt.com
Jméno služby	healthDopplerMQTT
Uživatel	Krpudrvg
Heslo	-
Port	18067
SSL Port	28067
Websocket Port (pouze TLS)	38067

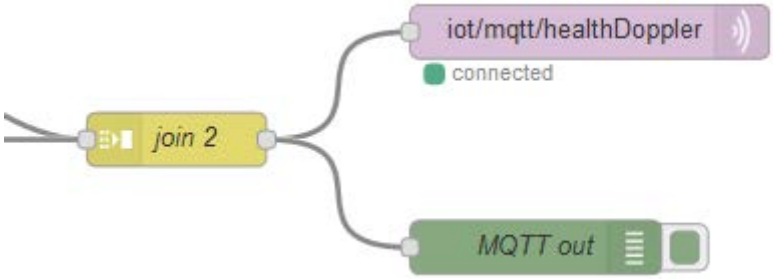
Jednotlivá nastavení včetně šifrování pomocí SSL/TLS se promítla do nastavení modulu ve flow skriptu vyobrazeny na obrázku 7.F a obrázku 7.G.



Obrázek 7.F Nastavení sekce „Connection“ modulu „iot/mqtt/healthDoppler“

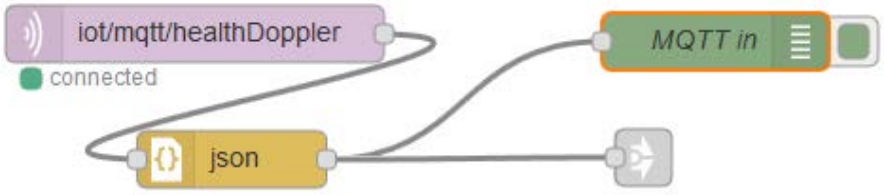


Obrázek 7.G Nastavení sekce „Security“ modulu „iot/mqtt/healthDoppler“



Obrázek 7.H Flow pro zasílání dat na MQTT brokera

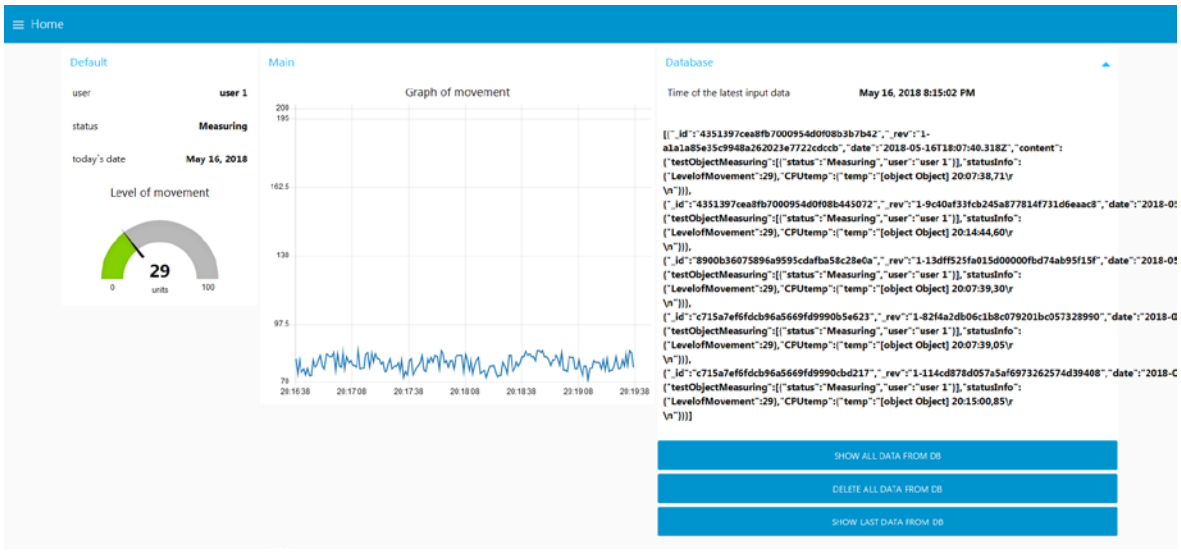
Data jsou posílány na server neboli MQTT broker na adrese m23.cloudmqtt.com. Na straně na IBM Cloudu jsou data odebírány od MQTT brokera pomocí data flow skriptu v aplikaci Node-RED vyobrazeného na obrázku 7.I s totožnými parametry jako flow skript pro publikování dat z tabulky 7.D a obrázků 7.F a 7.G.



Obrázek 7.I Flow pro přijímání dat od MQTT brokera

7.2.3. Vizualizace a ukládání dat na IBM Cloud

Závěrečná část bylo sestavení služby Node-RED na serverech IBM Cloud. Pro její zprovoznění bylo nutné provést i registraci účtu. Data jsou přijata data flow skriptem na obrázku 7.H. Ten data zasílá dále do databáze a grafického výstupu služby. Výstupem služby za pomocí modulů Dashboard je grafické rozhraní pro vizualizaci dat, které je vidět na obrázku 7.J. Je možné vidět aktuální uživatele, datum a intenzitu pohybu. Je zde také možné zjednodušeně nahlížet do databáze a také vymazat celou databázi.



Obrázek 7.J Grafický výstup aplikace Node-RED v cloudu

Celá experimentální cloudová služba pro senzor k detekci pohybů kosterního svalstva není v této verzi připravena na reálné použití. Jedná se především o demonstraci funkčnosti takového řešení s přihlédnutím na různé možnosti implementace a zejména na přenosové technologie jako MQTT. Celý grafický výstup i databáze je čistě experimentální, a proto k reálnému použití by bylo nutné na grafických výstupech z obou zařízení ještě dále zapracovat.

Ohledně bezpečnosti služby je přenos komplexně zabezpečen skrze přihlášení s uživatelským jménem a heslem, tak i šifrováním SSL/TLS. Pro možné reálné fungování takovéto služby je do budoucna dále bezpodmínečně nutné upravit autentizaci, autorizaci a řízení přístupu ke všem zařízením v řetězci. Týká se to jak zabezpečení přístupu k zařízení Raspberry Pi jakožto výměnnému bodu, kde stačí zabezpečení heslem, tak i cloudové služby. U té je i na nejvýš vhodné rozšířit zabezpečený přístup a protokolování pro vícero uživatelů, jako jsou pacient a ošetřující lékaři řádným ověřovacím procesem.

8. Model experimentální cloudové služby ze zdravotnického pohledu

Cloudová služba z pohledu zdravotnické služby je výrazně odlišná od pohledu z prostředí IoT. Rozdílné protokoly a technologie mezi těmito směry byly rozebrány výše v sekci Způsoby implementace. Zatímco IoT aplikace dává důraz zejména na efektivnost, energetickou nenáročnost a mobilitu, tak zdravotnická aplikace se zaobírá primárně integritou a klasifikací dat a její bezpečností. Tyto aspekty jsou proto zohledněny při výběru konkrétní technologie a způsobu návrhu.

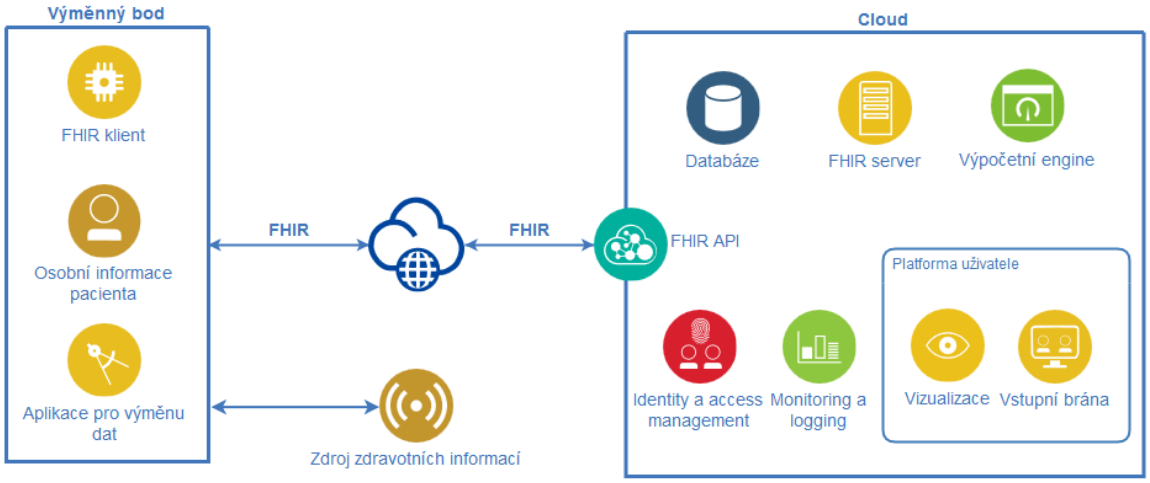
Cílem této práce bylo navržení modelu experimentální cloudové služby pro přenos a zpracování dat z IoT senzoru detekce pomalých pohybů kosterního svalstva na bázi Dopplerova radaru. Tato práce stejně jako z pohledu IoT přímo navazuje na práci studenta Lukáše Gregory. Součástí jeho projektu byla realizace senzoru pro detekci mikro pohybů kosterního svalstva na bázi Dopplerova radaru. Na základě výstupů z jeho projektu jsou v rámci této práce plánovány vstupy pro model experimentální cloudové služby.

8.1. Obecná analýza

Celá aplikace cloudové služby ke zdravotnickému zařízení se dělí na základní 2 části. Prvním z nich je zařízení, které slouží jako výměnný bod. Zde dochází k předání citlivých dat ze zmíněné přidružené práce, která do tohoto zařízení zasílá změřená data v přesně daném formátu. Tento formát závisí na partnerském projektu, ale nejvhodnějšími formáty jsou JSON či XML z důvodů absence nutnosti dalšího zpracování. Druhá část je cloudové úložiště společně s API interfacem a serverem zdravotnických informací.

Výměnný bod má hlavní úkol přijímat naměřená zdravotní data, přidružit je k osobním informacím pacienta a zabezpečeně a ve správné formě zasílat dále na cloudovou platformu zdravotnické služby. Data jsou do výměnného bodu přijímána jako nezosobněná. Teprve v daném zařízení jsou přidružena k předem definovanému účtu, a tedy i osobě. Výměnný bod může být proveden jako vícero typů zařízení. Jsou jimi například mobilní telefon či některý z druhů mikropočítačů (např. Raspberry PI).

Druhou částí je samotná cloudová platforma, který se skládá z mnoha částí zahrnující server, databázi, identity a access management, monitoring a logging řešení a API interface. Její hlavní účel je přijímání informací v definovaném formátu, bezpečné ukládání zdravotnických dat a jejich další zpracování. Všechny tyto operace musí dodržovat zásady o ochraně osobních a zdravotnických údajů. Musí být zajištěno, aby data byla přístupná pouze autorizovaným uživatelům. Další funkce platformy jako vizualizace dat, sestavování statistik a další nakládání s informacemi je již na možnostech a schopnostech provozovatele dané zdravotnické služby. Schématický model je vidět na obrázku 8.A.



Obrázek 8.A Model cloudové služby ze zdravotnického pohledu

8.1.1. Technologie FHIR

Vzhledem k charakteru aplikace bylo nutné vybrat vhodný protokol pro přenos informace mezi oběma částmi. Jedním z hlavních aspektů byla preference open-source standardů. Dalším hlavním aspektem bylo, že v tomto případě jsou přenášené informace velmi citlivé, jelikož se jedná přímo o PHI. Byl vybrán vcelku nový zdravotnický open-source protokol FHIR, který byl vytvořen přímo pro účely přenosu citlivých zdravotnických informací. Zároveň je vhodný i pro celou řadu dalších a větších aplikací, a tak je možné aplikace využívající FHIR sjednocovat do ucelených systému zdravotnické péče. Tento aspekt se pravděpodobně projeví až časem, jelikož nyní ještě nejsou větší zdravotnické systémy v České republice i jinde zpravidla připraveny na elektronickou výměnu informací pomocí FHIR. Zároveň mnoho velkých poskytovatelů cloudových služeb, které byly rozebrány výše, nejsou ještě připraveny na standard FHIR a jeho důležité části jako FHIR server jsou teprve ve vývoji. Toto je také velmi limitující pro implementaci experimentální cloudové služby ze zdravotnického pohledu.

Implementační návrh přenosového protokolu FHIR se skládá z FHIR serveru a FHIR klienta. FHIR server běžící na cloudové platformě je takovým srdcem celé aplikace a standardu FHIR, jelikož zde se koncentrují z klientů získaná data, ukládají do přidružených databází a jsou k dispozici k nahlížení pro autorizované uživatele. Jeden server může být centrem mnoha aplikací. Každý takový server má součástí i FHIR API interface pro komunikaci tímto protokolem. API interface může stát i samostatně bez serveru. V tomto případě má zřizovatel zdravotnické aplikace složitější pozici, kdy musí kompletně implementovat i serverovou jednotku. Touto cestou se dali někteří poskytovatelé cloudových služeb jako například Google. Na druhou stranu jsou i společnosti, kteří implementují komplexní prostředí včetně FHIR serveru a přidružených služeb. Jsou jimi například společnosti jako Amazon či Cerner, která je speciálně zaměřená pouze na zdravotnické služby a aplikace. Společnost Cerner provozuje i testovací servery „SMART on FHIR Sandbox“ a „SMART Health IT Sandbox“, které umožnují i testovací provoz vlastních zdravotnických aplikací včetně testovacích záznamů smyšlených pacientů.

Na druhé straně modelu funguje FHIR klient. Tento klient plní funkci komunikační entity pro uživatele, která poskytuje nahlížení i zapisování do FHIR serveru a jeho databází. Funguje na bázi JavaScriptu, Pythonu či iOS v závislosti na použitém zařízení či platformě. Tento klient zaručuje zabezpečení a správný formát správ dle vybraného FHIR zdroje. Uživatel skrze něj může využívat operací jako „read“, „write“, „update“ či „search“. Tyto operace se řídí dále i dle typu používaného

FHIR zdroje. U této aplikace je vhodné použít FHIR zdroje „Observation“ nebo „Patient“. Tyto dva se řadí mezi základní zdroje z velké škály. Pro zasílání naměřených dat na server je určen zdroj „Observation“ s operací „write“. Naopak pro nahlížení do již existujících záznamů je vhodný zdroj „Patient“ s operací „read“. Klient zde dále zajišťuje bezpečné ověření identity a autorizaci uživatele i pomocí OAuth 2.0 včetně zabezpečení komunikace s SSL/TLS.

Existuje dále i open-source nadstavba nad FHIR s názvem SMART. Někteří provozovatelé včetně společnosti Cerner využívají tuto nadstavbu a dávají k dispozici programy klienta. SMART on FHIR vznikl za účelem zjednodušení implementace FHIR technologie a snazší propojení jednotlivých systémů pracující s elektronickými zdravotnickými záznamy (EHR). Prvotní verze FHIR totiž nezahrnovaly formy autentizace, autorizace a profilů. Tyto nedostatky SMART nahrazoval vlastním řešením, které se postupem času dostalo i částečně do dalších verzí FHIR. [47] [48] Nyní SMART definuje i specifikaci elektronického zdravotního záznamu (EHR) pro bezpečné otevírání záznamu jinými aplikacemi. Tyto SMART aplikace jsou běžně webové aplikace, ale mohou být také nativní mobilní aplikace, které používají standard HL7 FHIR ke čtení, zápisu a změně dat z elektronických zdravotnických systémů. [41]

Technologie FHIR byla detailně rozebrána v samostatné kapitole výše. Celý model experimentální cloudové služby s využitím FHIR je schematicky vyobrazen na obrázku 8.A.

8.1.2. Výměnný bod

Výměnný bod je zařízení, které je sdíleno s prací Lukáše Gregory. Jedná se o zařízení, které přijímá pomocí lokálních komunikačních prostředků zdravotnická data snímaná senzorem mikro pohybů. Tyto data jsou bez informace o majiteli. Zařízení má za úkol přiřadit k datům informace o osobě, která bude měřená. Uvést data do správného formátu JSON či XML a bezpečně zaslat data na server. Toto zajišťuje FHIR klient. Ten je k dispozici v několika verzí dle programovacích jazyků i s nadstavbou SMART on FHIR [49] či bez ní [22]. Obsahuje FHIR knihovny, za pomoci kterých je možno definovat jeho činnost zasílání dat rovnou dále na FHIR server.

Tato práce si klade několik základních podmínek a parametrů, aby mohlo dojít ke úspěšnému fungování zařízení v reálné implementaci cloudové služby. Jsou jimi, že toto zařízení by mělo představovat malé chytré zařízení, které musí mít komunikační platformu do sítě internet, základní vlastnosti jako synchronizace času dle NTP či SNTP, podpora HTTPs a možnosti programů na bázi JavaScript, Python či iOS pro provoz FHIR klienta. Základními požadavky partnerské práce jsou především lokální komunikační standardy jako Wi-Fi či Bluetooth Low Energy. Na základě zmíněných podmínek lze usoudit, že hledanými zařízeními jsou mobilní telefony či vícero typů mikropočítačů s komunikačním interfacem jako například Raspberry Pi. Ten byl v této práci použit u implementace experimentální cloudové služby dle IoT.

8.1.3. Cloudová platforma

Cloudová platforma je prostředí, které spravuje přijímaná zdravotnická data od FHIR klientů. Platforma může mít vícero podob dle jednotlivých poskytovatelů. Může tomu být od využití pouze FHIR API až po komplexní systémy včetně FHIR serveru s vlastním API.

Tato práce se přiklání v tomto modelu k řešení cloudové platformy, jak ho poskytuje společnost Cerner. Jedná se tak o komplexní platformu včetně databáze, identity a access managementu, monitoring a logging řešení a FHIR serveru podporující navíc SMART on FHIR. Tato platforma spravuje i širokou řadu zdravotnických aplikací na vlastních cloudových úložištích.

Zabezpečená komunikace z FHIR serveru včetně šifrování, ověření a autorizace uživatele je u takovéto aplikace zajištěna knihovnami SMART on FHIR, které komunikují s FHIR klientem na druhé straně. Ty využívají vyzkoušených standardů k bezpečnému přenosu informace jako jsou OAuth 2.0 a SSL/TLS šifrování.

Implementátor celé aplikace díky zmíněným knihovnám klienta a serveru, který spravuje data, programuje především platformu uživatele pro přístup k datům. Jedná se o webovou či mobilní HTML aplikaci s FHIR klientem. Ty mohou být umístěny jak lokálně na uživatelově zařízení, který může fungovat i jako výměnný bod, či vzdáleně na dostupném cloudovém úložišti. Jím může být i úložiště od společnosti Cerner, jakožto i správce FHIR serveru. Tato webová či mobilní HTML aplikace je hlavní přístupovou branou k datům pro pacienty a lékaře. Možnosti zobrazení a interpretace dat v aplikaci, která má přístup díky knihovnám FHIR k údajům z FHIR serveru, jsou velké až neomezené v závislosti na vyspělosti výsledné HTML aplikace. V budoucnosti mohou mít samotní poskytovatelé FHIR serveru platformu uživatele přímo implementovanou a může tak odpadnout programování samotné HTML aplikace.

8.2. Ukázky fungování

Definovaný model je do značné míry obecný, ale je tak možné ho aplikovat na větší řadu možných reálně fungujících řešení. Model obsahuje jednotlivé části, které se totiž mohou lišit. Specifický úkol v rámci modelu mají FHIR elementy jako server a klient. Ty mohou být ve vícero verzí v závislosti na konkrétní realizaci. Dále se také liší, zdali pracují s nadstavbou SMART on FHIR či nikoliv.

Kompletní implementace aplikace popsaného modelu nebyla z časových a technologických důvodů možná. Hlavními důvody jsou, že poskytovatelé FHIR serverů jsou stále hojně ve fázi vývoje či implementace a testovací server SMART on FHIR Sandbox od společnosti Cerner, který byl v této práci použit, neumožňuje doposud způsoby zápisu dat na server. Naopak poskytuje ke čtení řadu smyšlených zdravotnických záznamů, ke kterým je možné přistupovat skrze FHIR klienta. Dále umožňuje důležité funkcionality zabezpečení a autorizace pro testovací aplikace. Rozdíly mezi zápisem a čtením klienta u této aplikace spočívá ve volbě jiných parametrů při registraci aplikace a využití odlišných FHIR příkazů v aplikaci klienta. Ovšem principy zabezpečení a autorizace zůstávají stejné, což je aktivita, na kterou se tato ukázka soustředí.

Cílem této testovací aplikace tak jsou ukázky pro dokázání funkčnosti takového modelu s technologií FHIR pro zdravotnické informační systémy a zejména způsob autorizace takovéto aplikace.

8.2.1. Cerner SMART on FHIR Sandbox

Ukázky funkčnosti popsaného modelu proběhly na zařízeních společnosti Cerner z důvodů velké rozvinutosti a vyspělosti Cerner platformy Millennium i v oblasti nadstavby SMART. Výhodou také bylo větší množství dokumentace a podpory od vývojářské skupiny. Na této platformě bylo využito standardu s nadstavbou SMART on FHIR, který tato společnost podporuje. Bylo při tomto experimentu využito následujících prostředků:

- FHIR klient s jednoduchou webovou HTML aplikací [50] od společnosti Cerner
- Vývojářský web [51] společnosti Cerner pro standard SMART on FHIR
- Testovací server Cerner SMART on FHIR Sandbox

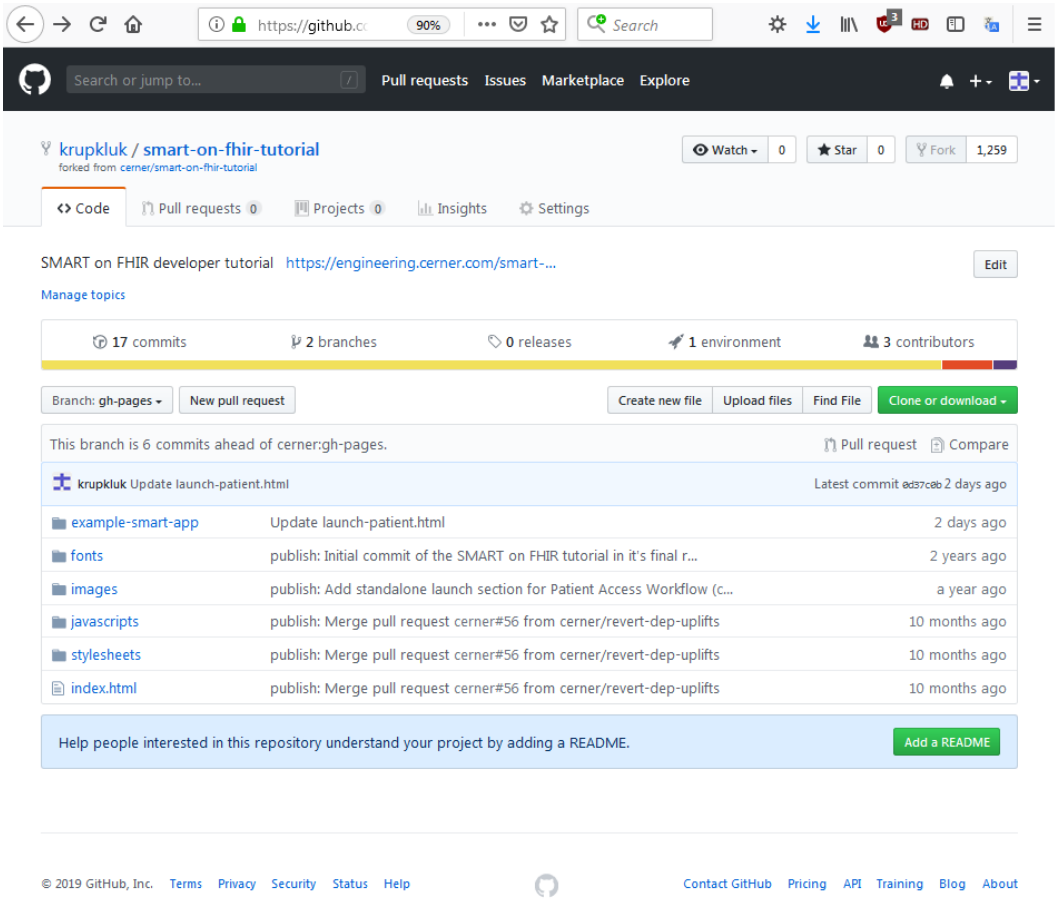
Vytvoření aplikace v systému společnosti Cerner na systému FHIR s testovacím serverem SMART on FHIR Sandbox vyžadovalo provést tyto základní kroky:

- Vytvoření základní webové aplikace SMART on FHIR
- Registrace aplikace v Cerner platformě
- Spuštění a autorizace aplikace v testovacím prostředí Cerner SMART on FHIR Sandbox

- **Základní webová aplikace**

K vytvoření základní webové aplikace byl převzat GitHub repositář cerner/smart-on-fhir-tutorial [50]. Společnost Cerner nabízí na webu GitHub volně k vícero druhům testování zmíněnou aplikaci, která obsahuje jak základní webovou HTML aplikaci, tak i JavaScript knihovny FHIR klienta se všemi potřebnými komponenty. Například konkrétně se jedná o soubor fhir-client.js, což je open-source knihovna určená pro volání rozhraní API FHIR a zpracování autorizačního procesu SMART on FHIR.

Základní webová aplikace pro tuto práci se nalézá v GitHub repositáři *krupkluk/smart-on-fhir-tutorial*, kde byla také upravována a provozována. Repositář je vidět na obrázku 8.B.



Obrázek 8.B GitHub repositář pro SMART on FHIR developer tutorial

- **Registrace aplikace v Cerner platformě**

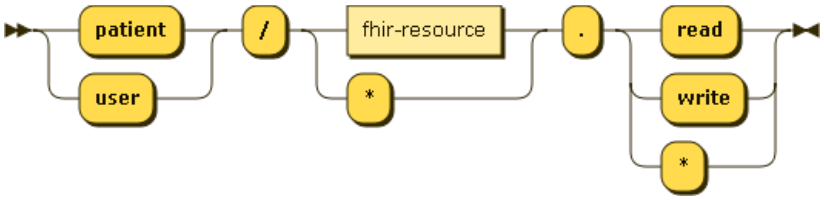
Pro fungování aplikace bylo nutné ji zaregistrovat skrze vývojářský web [51] společnosti Cerner. Tomu předcházela nezbytná registrace uživatele systému CernerCare. Pro aplikaci bylo při registraci zvoleny parametry definované v tabulce 8.A.

Tabulka 8.A Parametry registrované aplikace na vývojářský web společnosti Cerner

	Parametry registrované aplikace
Název aplikace	krupkluk SMART App – Patient
Přesměrovací URI	https://krupkluk.github.io/smart-on-fhir-tutorial/example-smart-app/
Typ aplikace	Pacient
FHIR specifikace	DSTU2
Autorizace	OAuth 2.0
Používané rámce	patient/Patient.read, patient/Observation.read, launch/patient, online_access, openid, profile

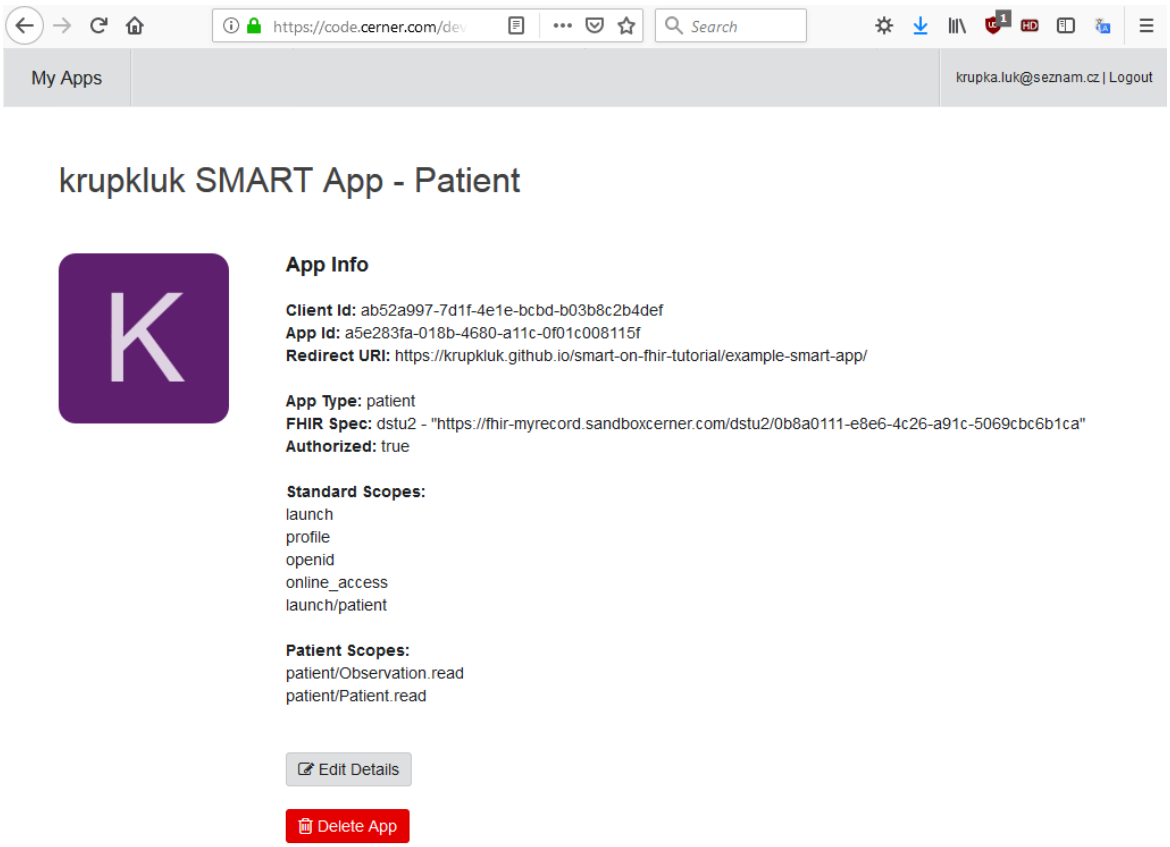
Přesměrovací URI je adresa vytvořené základní webová aplikace skrze, kterou se bude k údajům z Cerner systému přistupovat. V tabulce 8.A je dále vidět další parametry, které jsou důležité uvést v registraci pro správnou funkci aplikace.

Rámce, použité jako parametry registrované aplikace, nám definují přístup ke specifickým zdrojům o pacientovi či uživateli. Specifikace SMART na FHIR přímo definují rámce, které odpovídají přímo typům zdrojů FHIR. V tomto případě se jedná o rámce odkazující se například na čtení pacientova zdroje „Observation“ a „Patient“. Specifické rámce mají syntaxi vykreslenou na obrázku 8.C. Je také dáno, že systém EHR nemusí umožňovat přístup ke všem souvisejícím zdrojům u daného rámce.



Obrázek 8.C Syntaxe rámců zahrnující FHIR zdroje [22]

Výsledná zaregistrovaná aplikace s detaily je vidět na obrázku 8.D. Detail aplikace nám definuje důležité parametry aplikace, jako jsou Client ID, přístupový bod k serveru a další parametry, které byly zadány při registraci. Client ID je důležitý údaj, který musí být zapsán v aplikaci smart-on-fhir-tutorial do *launch-patient.html*, aby se prokázalo, že se skutečně jedná o stejnou aplikaci. Bez něj by nebyl možný úspěšný ověřovací proces aplikace. Soubor *launch-patient.html* je totiž vstupním bodem při spouštění samostatné aplikace. V reálném produkční realizaci by byl tento soubor v řadě případů vyvolán externí aplikací (například portálem EHR nebo pacientským portálem). V této práci je tato stránka vyvolána přímou adresací ve webovém prohlížeči.



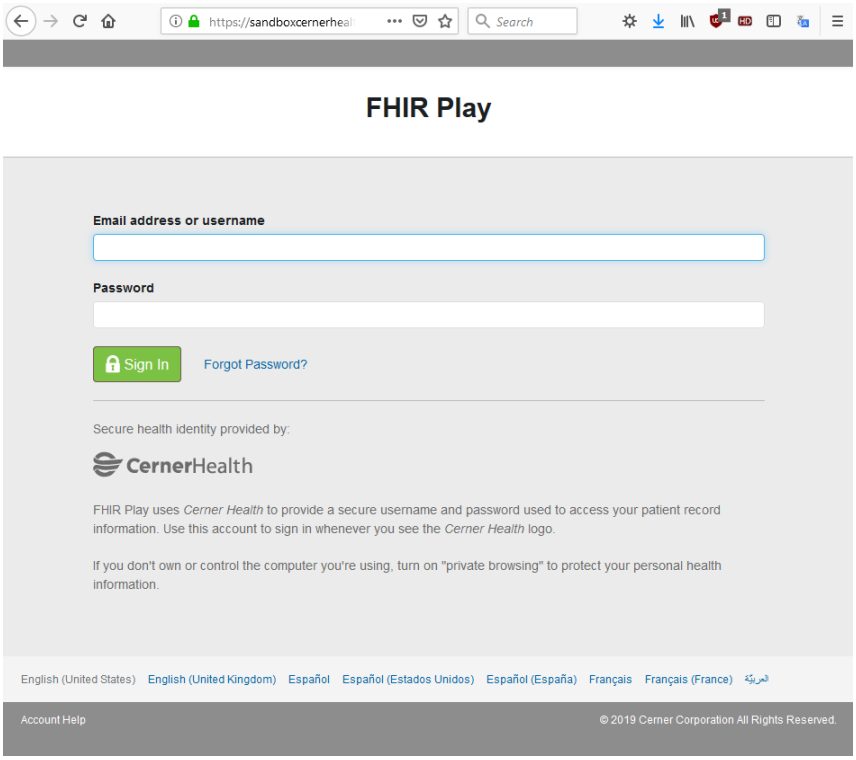
Obrázek 8.D Registrovaná aplikace na vývojářském webu společnosti Cerner

- **Spuštění a autorizace aplikace**

Aplikace se spouští přes soubor *launch-patient.html*. Ten je volán přímou adresací s parametrem „iss“ představující adresu přístupového bodu k testovacímu serveru Cerner Sandbox pro pacienty. Celá adresa poté zní:

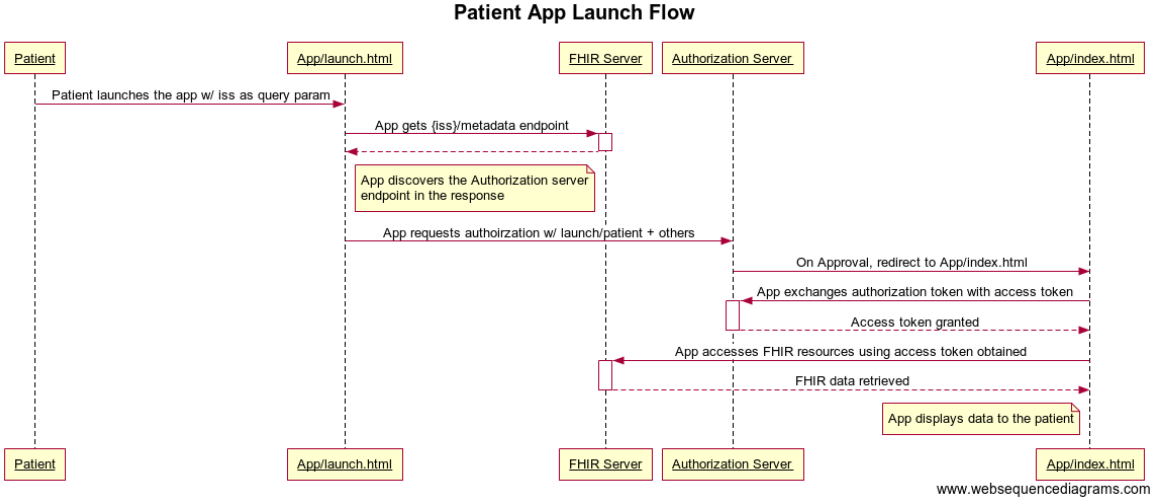
https://krupkluk.github.io/smart-on-fhir-tutorial/example-smart-app/launch-patient.html?iss=https://fhir-myrecord.sandboxcerner.com/dstu2/0b8a0111-e8e6-4c26-a91c-5069cbc6b1ca

Soubor *launch-patient.html* pracuje s knihovnami FHIR klienta a zahajuje tak postup OAuth 2.0 autorizace aplikace. Součástí autorizačního procesu jsou i parametry jako Client ID a jednotlivé rámce vypsané v tabulce 8.A. Uživatel či pacient se přihlašuje k Cerner systému skrze stránku na autorizačním serveru, na kterou je přesměrován a vyobrazenou na obrázku 8.E. Tento proces může být u jiných implementací i odlišný bez nutnosti vyvolání webové stránky, kdy přihlašovací údaje jsou rovnou zaslány autorizačnímu serveru.



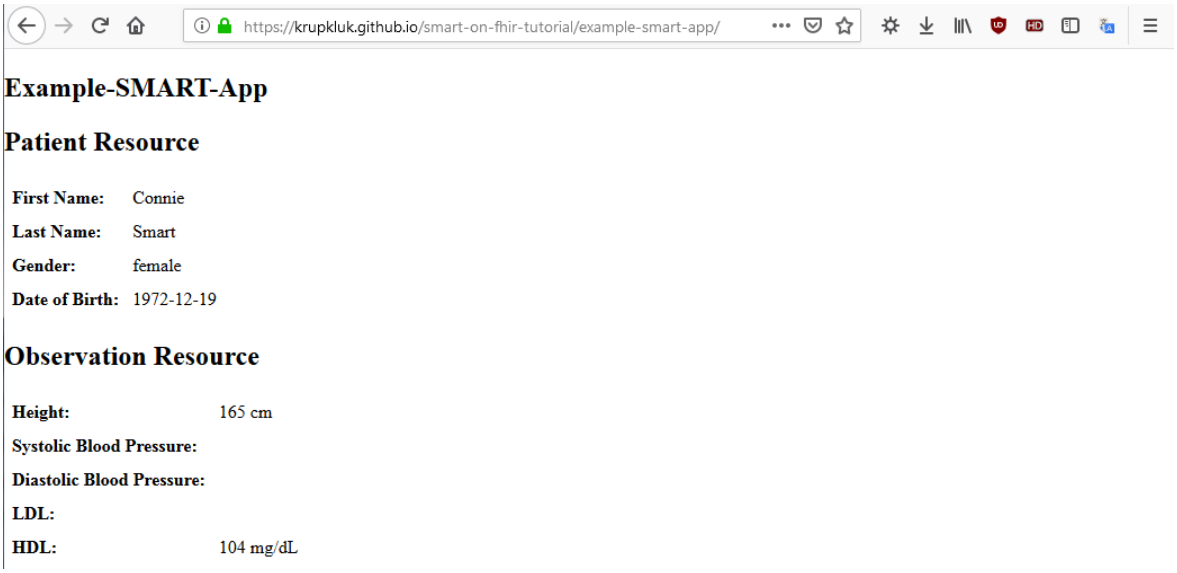
Obrázek 8.E Přihlašovací stránka pro autorizaci pacienta na autorizačním serveru Cerner

Celý autorizační proces i s OAuth 2.0 tokeny od pacienta skrze aplikaci až k FHIR serveru je rozkreslen na obrázku 8.F. Zahrnuje zahájení spojení aplikace na FHIR server a následně autorizační server. Zde probíhá ověření Client ID aplikace i autorizace přístupu. Po následném získání přístupového tokenu je možné úspěšně požádat o data z FHIR serveru.



Obrázek 8.F Diagram autorizace aplikace k FHIR serveru [50]

Na závěr úspěšného procesu, kdy si aplikace s autorizačním serverem vymění přístupové tokeny, jsou obdržená data zobrazena na stránce *index.html* vyobrazené na obrázku 8.G. Forma prezentace získaných dat je zde přímo závislá na formátu této stránky a je tedy možná velká variabilita vzhledu.



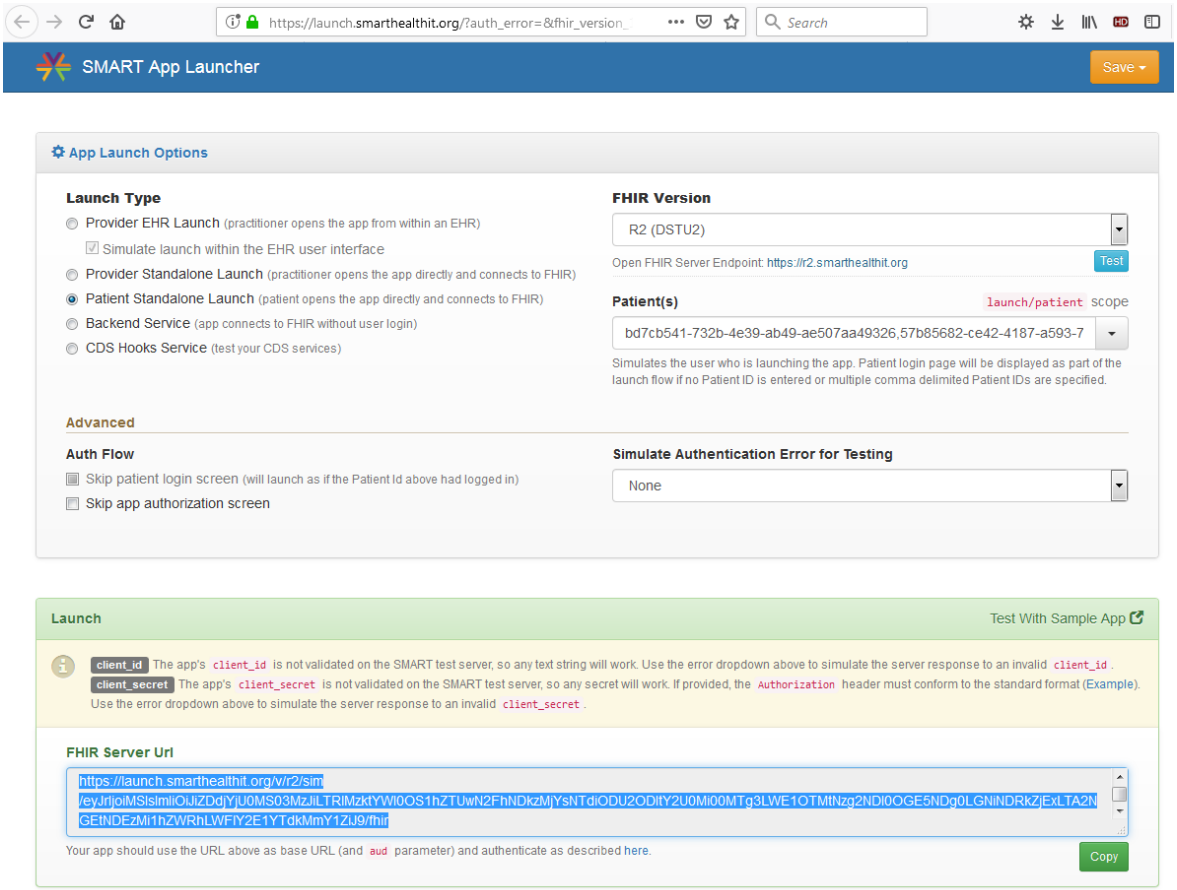
Obrázek 8.G Zobrazená stránka index.html s obdrženými PHI z Cerner FHIR serveru

V této testovací implementaci byla demonstrována zejména přenosová část celé aplikace, jelikož se jedná o klíčové místo pro zachování bezpečnosti PHI. Další části jako FHIR servery jsou tak v tomto případě pod správou specializovaných třetích stran, které ručí za uchovávaná data. Vybraná aplikace na cloudu GitHub s repositářem *krupkluk/smart-on-fhir-tutorial* zde plní funkci jak platformy pacienta pro čtení EHR záznamů, tak i výměnného bodu pro zapisování dat na FHIR server. V demonstrované aplikaci je ukázán pouze proces čtení skrze FHIR technologii, jelikož testovací Cerner server funkcionalitu zápisu neumožňuje. Rozdíl zápisu ke čtení je u aplikace ve volbě správného rámce *patient/Observation.write* při registraci aplikace a využití odlišných FHIR příkazů v aplikaci. Ovšem principy zabezpečení a autorizace zůstávají stejné.

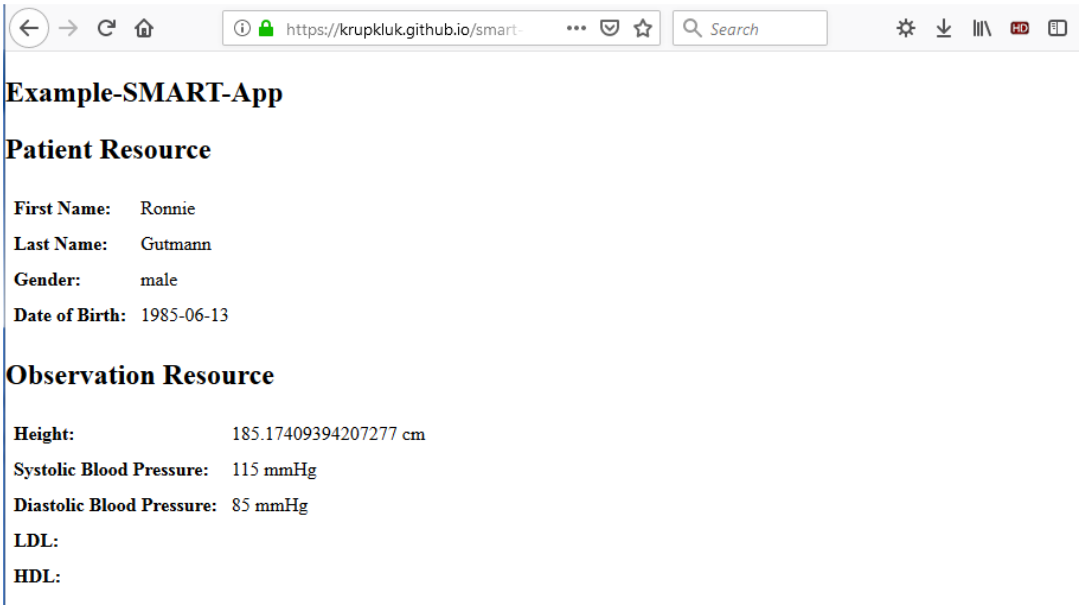
V této implementaci je aplikace provozována na cloudu GitHub, ke kterému které se přistupuje vzdáleně. V reálné implementaci by webová aplikace s FHIR knihovnami mohla být nahrána v daném zařízení a přistupovalo by se na ni přímo na zařízení. Pro skutečnou realizaci je také vhodnější využití správce balíčků jako npm pro instalaci nejnovějších verzí FHIR klienta *fhir-client.js*.

Tento experiment ukazuje funkčnost přenosového standardu FHIR pro přenos zdravotnické informace, při kterém je zajištěna zejména bezpečnost dat, o kterou u zdravotnické aplikace jde především. V tomto experimentu je vidět zejména principy autorizace. To je pro jakoukoliv službu zásadní a bezpodmínečně nutné. Na základech tohoto FHIR standardu na vícero úrovních lze tak dosáhnout komplexní zdravotnické služby.

Funkčnost takto demonstrované implementace byla provedena i na serveru organizace SMART Health IT [47] na obrázku 8.H s obdobným výsledkem viditelným na obrázku 8.I. To navíc ukazuje, že takto sestavená aplikace může fungovat na vícero serverech pouze s minimálními změnami. Hlavní změnou je odlišný přístupový bod serveru pod parametrem „iss“ a rozdílný Client ID, které je nutné změnit v aplikaci smart-on-fhir-tutorial pro úspěšnou identifikaci aplikace. Navíc u toho serveru bylo pole Client ID ignorováno, pro možnosti snazšího testování, tak nebylo nezbytností ho měnit.



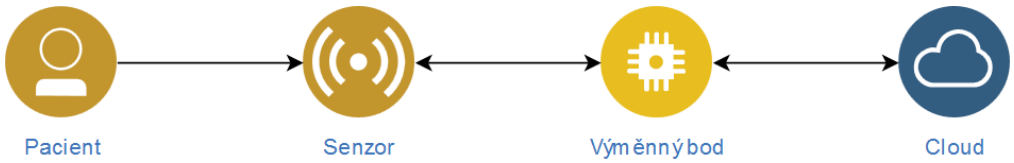
Obrázek 8.H Úvodní stránka testovací registrace pro testování SMART on FHIR aplikací



Obrázek 8.I Zobrazená stránka index.html s obdrženými PHI ze serveru SMART Health IT

9. Shrnutí do praxe

Tato práce se zaměřuje na způsoby implementace cloudové služby k zařízení na detekci mikro pohybů kosterního svalstva. Zobecněně by se mohlo jedna o libovolnou zdravotnickou IoT aplikaci pracující s lidskými údaji a měřením člověka tedy určitou formou PHI. Základní zobecněný komunikační model celé aplikace je vidět na obrázku 9.A. Tato práce uvádí 2 způsoby, jak provádět zpracování a přenos dat z výměnného bodu do cloudového úložiště. Obě implementace vychází ze situace, kdy ve výměnném bodě, které představuje zařízení Raspberry Pi, dochází k přebrání informace od partnerského projektu. Tyto data mohou být ve vícero datových interpretacích v závislosti na přenosových parametrech partnerského projektu. Před použitím těchto dat je ovšem nutné je uvést do formátu JSON či XML, pokud v nich už nejsou. To může řešit skript v rámci aplikace (Node-RED či FHIR klient) či samostatný. Zmíněné aplikace již dále data zpracovávají a posílají dále komunikačním standardem.



Obrázek 9.A Zobecněný komunikační model

Pro implementaci takové cloudové služby je vhodné si nejdříve položit několik otázek a rozhodnout, co od takové celé aplikace očekáváme. Je tato aplikace určena vícero pacientům najednou například v rehabilitačním centru? Očekávám ji rozšířit pro mnoho pacientů? Kdy a jak rychle budu potřebovat tuto aplikaci? Bude spolupracovat s některým centrálním systémem zdravotnických informací? Je takový pacient v tomto centrálním systému? Chtěl bych, aby k získaným údajům mělo přístup větší množství lidí? Budu vytvářet vlastní přístupový portál k údajům?

Takové otázky je důležité si položit, jelikož poté je možné se teprve rozhodnout, jakou cestou implementace takové aplikace se dát. Je nutné vědět, co od ní vy či vaši zákazníci očekávají. Existují již dříve zmíněné 2 základní cesty, jakými se při implementaci takové zdravotnické služby dá jít.

První cesta pro zpracování a přenos dat z výměnného bodu do cloudového úložiště je formou již existujících plně podporovaných standardů v oblasti IoT. Experimentální implementace s protokolem MQTT byla detailněji popsána výše. U ní není možná žádná přímá integrace se zdravotními informačními systémy a je vhodná spíše pro proprietární řešení u výjimečných aplikací vyžadující i například rychlou a jednoduchou implementaci. U této aplikace je pro případ nutnosti rychlé implementace vhodné i použití časově méně náročné platformy Node-RED, která je ovšem na datové i energetické prostředky náročnější než jiné programovací platformy. Ty je vhodné použít v případě, kdy nejde tolik o čas, ale především o co nejméně náročnou aplikaci především pro zařízení ve výměnném bodě. Toto zařízení může být napájené z baterie, a tak s tím souvisí i výdrž takového zařízení. Na straně cloudu je pak vhodné využít nástrojů v rámci platforem IoT (například AWS IoT, Azure IoT Suite atd.), které zahrnují i zde použitý Node-RED, a podporují MQTT protokol.

Hlavními pozitivy této varianty je open-source řešení, běžně využívané standardy jako MQTT, nižší energetická i výpočetní náročnost, kratší doba implementace a žádná závislost na zdravotnických systémech s podporou FHIR standardu, které jsou ve většině teprve ve vývoji či implementaci. Zároveň správa cloudové platformy bez podpory FHIR je finančně méně náročná. Při výběru konkrétní cloudové platformy je také možné vybírat z velkého množství, jelikož de facto jediná podmínka je podpora MQTT protokolu. Proto je možné se dívat zejména na cenu mezi poskytovateli

a podporu dalších přídavných funkcí služby k vizualizaci a prezentaci dat pro vytvoření uživatelsky přívětivého prostředí.

Z pohledu bezpečnosti je tento způsob implementace méně robustní než s FHIR, ale i tak splňuje základní podmínky bezpečnosti při použití doporučených opatření, jako jsou bezpečná a periodicky měněná hesla na zařízeních, fyzické zabezpečení, šifrování a autorizace uživatele při přenosu skrze MQTT. Bezpečnost na cloudu v tomto případě je přenesena na třetí stranu, která za to zodpovídá.

Druhá cesta k implementaci takové služby je za pomoci především zdravotnických standardů, jako je FHIR. Ty jsou zpravidla více energeticky a datově náročné, jelikož zde je dáván důraz především na zvýšenou bezpečnost. Tyto standardy přímo navazují na technologie ke zdravotním informačním systémům EHR. Implementace těchto standardů tak není možná bez FHIR serveru, který je komplikovaný a časově náročný k implementaci. Je tak vhodné využít již stávajících či teprve vyvíjejících se systémů u cloudových poskytovatelů, které mají či budou mít celý systém s FHIR serverem i databázemi připravený. Tento způsob zároveň napomáhá k celkové integraci zdravotnických služeb, které mohou pro pacienta být na jednom místě. Společnost Cerner je jedna z mála, která by byla schopna již nyní takovou službu provozovat.

Doporučený postup celé implementace cloudové služby s FHIR se dělí na 3 části. Jsou jimi část aplikace FHIR klienta ve výměnném bodě, registrované instance aplikace a platforma pacienta. Doporučené požadavky k implementaci prvních 2 částí jsou:

- Zařízení výměnného bodu s podporou JavaScript, Python či iOS (například Raspberry Pi)
- FHIR klient se SMART nadstavbou
- Cloudový poskytovatel s fungujícím SMART on FHIR serverem

První část je implementace aplikace klienta, sloužící jako autorizační a přenosová autorita. Klienta je možné stáhnout zpravidla přímo od poskytovatele, u kterého budete využívat jeho server. Klienty je možné také získat ze stránek organizace SMART Health IT [49] a dalších. Typ jazyka, ve kterým jsou knihovny klienta napsány, musíte zvolit dle podpory zařízení výměnného bodu. Aplikaci klienta nahrajete na zařízení výměnného bodu, ale doporučuje se, pokud je to možné, využití správce balíčků jako npm pro instalaci nejnovějších verzí FHIR klienta.

Následně je nutné zaregistrovat aplikaci na serveru poskytovatele serveru FHIR, jakým je nyní například společnost Cerner. U zmíněné společnosti registrace zahrnuje následující kroky:

- Registrace svého účtu
- Vytvoření nové instance aplikace s parametry:
    - Název aplikace – volitelné
    - Typ aplikace – Provider
    - Autorizace – ano
    - Standardní rámce (odpovídá FHIR zdrojům) – podle druhu posílaných dat, v tomto případě patient/Observation.write, patient/Patient.write a další již definované v základu při registraci

Ve vytvořené instanci aplikace získáte Client ID a standardní rámce, které je nutné promítnout do klienta ve výměnném bodě. Client ID tak jasně identifikuje, že aplikace patří k registrované instanci na serveru FHIR. Standardní rámce nám zase udávají, k čemu chcete na serveru FHIR přistupovat. Client ID i standardní rámce se využívají zde jako paramenty při autorizaci pomocí volání *FHIR.oauth2.authorize* a bez nich by nebylo možné autorizaci klienta provést. Potřeba je zde i konkrétní přihlašovací údaje k pacientovi v databázi FHIR serveru, se kterými pracuje autorizační server. Skrze takto sestavenou aplikaci je možné zasílat z klienta

zabezpečeně data v definovaných rámcích/zdrojích ve formátu JSON či XML na FHIR server s jeho přidruženými databázemi.

Třetí částí je platforma pacienta, skrze kterou pacient či jiná osoba chce přistupovat k údajům pacienta z FHIR serveru a databází přes web. Jedná se o cloudovou aplikaci obsahující opět klienta FHIR, sloužící jako autorizační a přenosová autorita, a další části. Těmi jsou webové aplikace zpravidla v HTML. Ty jsou zodpovědné už za samotné zobrazení přijatých dat. Kvalita výstupu pak přímo závisí na kvalitě této HTML stránky. Tyto stránky ke klientovi si je nutné doprogramovat v HTML nebo existují testovací aplikace [50], jako byla použita v ukázce v této práci výše. Doporučuje se cloudovou aplikaci i s klientem FHIR nahrát na libovolné cloudové úložiště, kde bude aplikace dostupná. To nemusí být nutně u stejného poskytovatele jako FHIR server, ale i to je možné. V ukázce s FHIR byla takto použit server GitHub. Správu takové cloudové aplikace tak přenesete na třetí stranu, čím předáte velkou část zodpovědnosti za hladký chod. Někteří poskytovatelé FHIR serveru mohou mít časem i k dispozici celou vlastní platformu pacienta, čímž tato celá činnost může odpadnout úplně.

Postup k platformě pacienta je založen na těchto doporučujících požadavcích:

- Cloudová aplikace s FHIR klientem s nadstavbou SMART a webovou HTML stránkou pro zobrazení výsledků
- Cloudový poskytovatel pro provoz cloudové aplikace
- Cloudový poskytovatel s fungujícím SMART on FHIR serverem

Po instalaci cloudové aplikace pro platformu pacienta na některé cloudové úložiště například od společnosti IBM či Cerner (pro ukázku fungování byl použit server GitHub), následuje registrace aplikace na webu poskytovatele FHIR serveru, stejného jako v kroku u klienta ve výměnném bodě tedy u společnosti Cerner. Postup registrace je obdobný, liší se pouze jinými parametry při vytváření nové instance aplikace. Nové parametry jsou zde:

- Vytvoření nové instance aplikace s parametry pro platformu pacienta
  - Název aplikace – volitelné
  - Typ aplikace – Pacient
  - Autorizace – ano
  - Standardní rámce (odpovídá FHIR zdrojům) – podle druhu požadovaných dat, v tomto případě patient/Observation.read, patient/Patient.read a další již definované v základu při registraci

V takto vytvořené aplikaci není díky odlišným rámcům tak možné zapisovat, ale pouze číst, a proto se jedná o platformu pacienta. Ve vytvořené cloudové aplikaci je potřebná stejná operace s Client ID a standardními rámci, jako u FHIR klienta ve výměnném bodě pro korektní autorizaci aplikace a jasnou identifikaci cloudové aplikace k registrované instanci aplikace. Takto vytvořená aplikace může už složit jako platforma pacienta pro přístup k údajům na FHIR serveru. Přistupuje se k ní pomocí url adresy na umístění HTML stránky platformy pacienta. Stránka si dle vlastní potřeby volá další funkce jako *FHIR.oauth2.authorize*. Případné další parametry závisí na konkrétní funkci HTML stránky. Například u testovací aplikace společnosti Cerner bylo nutné doplnit k url platformy také parametr „iss“ s konkrétní adresou testovacího serveru. Přístupové údaje ke konkrétnímu pacientovi se v tomto případě zadávají přes webový formulář autorizačního serveru Cerner, na který jste přesměrování z FHIR serveru.

Způsob implementace s technologií FHIR se doporučuje zejména v situacích, kdy se předpokládá dlouhodobé využití takové služby i s předpokladem budoucí integrace do některého z centrálních zdravotnických informačních systémů, který v této době v České republice ani v mnoha dalších zemích není zatím k dispozici. Služba může být snadno rozšířena na vícero zařízení, kdy

centrální systém a klient na zařízení můžou zůstat téměř stejné. Zároveň je možnost připojení i k jiným serverům bez velkých změn, jelikož FHIR sever funguje stejně. Změny, které by bylo nutné provést, by byly změny Client ID v klientovi a nová registrace aplikace na serveru poskytovatele. Hlavní pozitiva tohoto způsobu implementace cloudové služby je open-source řešení, vyšší bezpečnost i díky klasifikaci dat do zdrojů a integrace do centrální zdravotních systémů.

Vzhledem k rychlému vývoji v této oblasti se dá předpokládat, že tento model fungování, by mohl být často využíván. Při implementaci je doporučeno využít správce balíčků jako npm pro instalaci nejnovějších verzí FHIR klienta (například *fhir-client.js*) na zařízení výměnného bodu. Dále by takový klient neměl obsahovat další funkcionality či skripty, které nebude využívat, aby byla zachována čistota a funkčnost aplikace. Někteří klienti, upravené provozovateli FHIR serverů, totiž obsahují nadbytečné funkce, aby pokryly vícero možností využití. Dále někteří klienti využívají autorizaci uživatele skrze webový portál autorizačního serveru. To není úplně vhodné pro využití v zařízení výměnného bodu, kde zpravidla není přístup ke grafickému rozhraní. Ačkoliv pří použití klienta jako pacientské platformy pro čtení dat vhodný je, ovšem ten se nepředpokládá v této aplikaci ve výměnném bodě nýbrž v cloudovém úložišti, kam člověk přistupuje z počítače či mobilu. Autorizace je tak vhodné provést bez nutnosti lidské interakce přímým zasláním identifikačních údajů na autorizační server.

Pro výsledné fungování celé aplikace je možné použití obou variant jak s MQTT, tak s FHIR, ačkoliv každá má svá specifika a omezení. Vždy je důležité při implementaci mít na paměti, že se pracuje se zdravotnickými daty lidí, a je tak na nejvýš důležité používat nejnovějších a bezpečných postupů k zabezpečení těchto dat.

10. Závěr

Tato práce se zabývala rozsáhlejší problematikou zdravotnických cloudových služeb v IoT a eHealth oblasti. Hlavním cílem bylo porovnání možností technologií a poskytovatelů cloudových služeb v těchto oblastech za účelem nalezení vhodného řešení zdravotnické služby pro zdravotnické zařízení. V tomto případě se jednalo o zařízení na detekci mikro pohybů kosterního svalstva.

Práce nejprve mapuje základní terminologii zdravotnických dat a služeb. Popisuje právní rámec, který se týká zdravotnických služeb. Jedná se především o americký zákon HIPAA, ze kterého mnoho velký nadnárodních telekomunikačních firem vychází. Vychází z něj, přestože tyto firmy operují na celém světě, jelikož mají často sídlo právě v USA. Tento zákon popisuje způsoby a postupy, kterých se telekomunikační firmy i poskytovatelé zdravotnické péče při nakládání se zdravotnickými daty musí řídit. Popisuje jak technické záruky, tak i případné sankce při jejich neplnění.

Evropská legislativa, která je založena na jednotlivých národních zákonech v každé členské zemi EU, je v oblasti služeb eHealth o něco pozadu. Velký pokrok k legislativním úpravám a rozvoji je program Evropské komise eHealth European Interoperability Framework a doporučení Evropské komise o evropském formátu pro výměnu elektronických zdravotních záznamů z února 2019. Ty napomáhají rozvoji elektronického zdravotnictví ve členských státech EU. V České republice zatím není elektronické zdravotnictví rozvinuté. Změnu by mohla přinést Národní strategie elektronického zdravotnictví pod hlavičkou Ministerstva zdravotnictví. Tato strategie určuje směr rozvoje eHealth v České republice s horizontem alespoň 5 let do roku 2021.

Práce dále ukazuje a porovnává poskytovatele cloudových služeb s ohledem na jejich vybavenost v oblasti IoT a eHealth služeb. Zkoumané subjekty zahrnují společnosti Amazon, IBM, Microsoft, Google a Cerner. Speciální důraz byl zde kladen na bezpečnost a podporu specifických standardů jako MQTT a FHIR. Srovnání ukazuje, že všechny společnosti si jsou vědomi důležitosti bezpečnosti u jejich platforem. Tomu odpovídá i využití podobných standardů a procesů, které zaručují bezpečnost pro zpracovávaná data. Většina probíraných poskytovatelů je také velmi dobře připravena na služby založené na protokolech využívaných v oblasti IoT včetně MQTT protokolu. Je to dáno již dlouhodobým vývojem v této oblasti s celou řadou implementací. Výjimkou je společnost Cerner, která se soustředí především na zdravotnické standardy. U těch ovšem poskytuje plnou podporu i pro standard FHIR. Platformy ostatních firem nejsou u tohoto standardu zatím tolik rozvinuté a mnoho z nich se stále ještě nalézá ve fázi vývoje. Jedním z důvodů je, že se jedná o relativně nový standard vzešlý z organizace Health Level 7 a také doposud malým množstvím implementací. To se ale předpokládá, že se časem změní. Souvisí to totiž úzce i s rozvojem elektronického zdravotnictví.

Tyto společnosti mají vysoký potenciál i v dalším rozvoji služeb ve zdravotnictví. Mají kapacity na tento rozvoj díky své velikosti a globálnímu dosahu a významně se touto oblastí včetně standardu FHIR zabývají. Svědčí o tom i konference CMS Blue Button 2.0 Developer Conference, kde se vedoucí pracovníci v oblasti zdravotnických informačních technologií ze zmíněných firem shodli na společných základních bodech rozvoje eHealth [42].

Hlavní náplní této práce je volba a implementace vhodného řešení cloudové služby pro zařízení na detekci mikro pohybů ve svalech. Služba má za úkol převzít data ve výměnném bodě a bezpečným způsobem přenést do cloudové platformy k dalšímu zpracování. Data jsou získány od partnerského práce Lukáše Gregory, která se zabývá detekcí mikro pohybů. Byly vybrány 2 způsoby řešení k realizaci takové služby, které se od sebe výrazně liší. Prvním je způsob za využití standardů a protokolů z oblasti Internetu věcí, která má specifika jako malá datová i energetická náročnost na zařízeních. Hlavní přenosový protokol byl zvolen MQTT a byl implementován do

experimentální cloudové služby za pomocí platformy Node-RED a serverů společnosti IBM. Platforma sloužila i jako nástroj ke zpracování, transportu i vizualizaci dat. Protokol MQTT byl také detailněji rozebrán pro pochopení celé problematiky.

Tento způsob ukazuje, jak je možné za pomoci standardů IoT, implementovat takovou zdravotnickou službu. Přestože tyto standardy nebyly nikdy určeny k práci se zdravotnickými daty, plní tuto funkci dobře. Pokud implementátor zvolí tuto cestu, je důležité, aby aplikoval všechny možné bezpečnostní prvky protokolu MQTT. Poté je možné splnit základní požadavky na bezpečnost dat za pomoci procesů šifrování a autorizace, které jsou u zdravotnické služby nepostradatelné. Hlavními pozitivy této varianty je open-source řešení, běžně využívané standardy, nižší energetická i výpočetní náročnost a žádná závislost na zdravotnických systémech s podporou FHIR standardu.

Druhým způsobem je využití standardů a protokolů z oblasti zdravotních informačních systémů, která jsou složitější, komplexnější a dávají zvýšený důraz na bezpečnost. Hlavní přenosový protokol byl zvolen FHIR, který byl také detailněji rozebrán pro pochopení jeho fungování a celé problematiky. Byl k němu vytvořen model fungování cloudové služby ke zdravotnickému zařízení, který demonstruje možnosti implementace cloudové služby za pomoci přímo standardu FHIR. Byly zde doporučeny postupy, které by měly být v takovém modelu dodrženy. Kompletní implementace služby popsaného modelu nebyla z časových a technologických důvodů možná, a proto na základě tohoto modelu byly demonstrovány ukázky fungování na testovacích serverech. Ty ukazují zejména procesy autorizace, která je jednou z hlavních částí standardu FHIR. Práce také více rozebrala doporučený způsob reálné implementace cloudové služby s FHIR technologií v sekci Shrnutí do praxe.

Hlavní pozitiva tohoto způsobu implementace cloudové služby je open-source řešení, vyšší bezpečnost i díky klasifikaci dat do zdrojů a integrace vícero zdravotnických aplikací do centrálních zdravotních systémů. U těch se předpokládá velký rozvoj v následujících letech, ačkoliv nyní jsou v mnoha zemích včetně České republiky teprve ve fázi příprav. Zde se pak předpokládá, že technologie FHIR bude hrát důležitou roli, a že pronikne také do platforem velkých cloudových poskytovatelů. Ty stále ve většině nejsou připraveni na implementaci tohoto standardů a jedná se tak také o vývoj následujících let. Tím je i dáno doposud malé množství reálných implementací.

Obě použité varianty k dané problematice přistupují rozdílně a každá má jisté limity. Společného mají zejména open-source řešení a vysoký potenciál k vyššímu využití u obou zmíněných přenosových technologií. Hlavní rozdíl se vyskytuje u většího množství přenášených dat u technologie FHIR, možnosti integrace se zdravotnickými informačními systémy a implementační připravenost stávajících systémů cloudových poskytovatelů. Zatímco FHIR standard se bude používat jako univerzální protokol pro výměnu zdravotnických informací, tak MQTT se v této oblasti vyskytuje pouze zřídka, ale to nevylučuje vhodnost využití u některých případů, jako může být i tento.

V rámci bezpečnosti jsou obě varianty dostačující při dodržení doporučených postupů a technologií včetně šifrování atd. Zdravotnická varianta navíc klasifikuje data do zdrojů, čím jasně definuje, o jaký druh dat se jedná a server s nimi podle toho může nakládat.

Tuto práci lze považovat za ukázku možností a určitý návod pro implementaci cloudové služby ke zdravotnickým zařízením. Práce tak mapuje rozsáhlou problematiku využití MQTT a FHIR protokolů pro zdravotnickou službu, která nemusí být napojena pouze na zařízení na detekci svalové aktivity kosterního svalstva, ale i na jiné zdravotnické zařízení či zdravotnickou aplikaci.

Seznam obrázků

Seznam tabulek

Reference

[1] M. Rouse, „personally identifiable information (PII),“ TechTarget, [Online]. Available: https://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information. [Přístup získán 2. 11. 2018].

[2] R. Sharma, „What is PII and PHI? Why is it Important?,“ File Cloud, [Online]. Available: https://www.getfilecloud.com/blog/2015/03/what-is-pii-and-phi-why-is-it-important/. [Přístup získán 2. 11. 2018].

[3] TechTarget, „HIPAA (Health Insurance Portability and Accountability Act),“ TechTarget, [Online]. Available: https://searchhealthit.techtarget.com/definition/HIPAA. [Přístup získán 1. 11. 2018].

[4] TechTarget, „protected health information (PHI) or personal health information,“ TechTarget, [Online]. Available: https://searchhealthit.techtarget.com/definition/personal-health-information. [Přístup získán 1. 11. 2018].

[5] Ministerstvo zdravotnictví ČR, „Narodní strategie elektronického zdravotnictví,“ [Online]. Available: http://nsez.mzcr.cz/. [Přístup získán 8. 11. 2018].

[6] F. H. Wesam, S. M. Raed a L. T. Leszek, „PHeDHA: Protecting Healthcare Data in Health,“ 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, New York, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00164.

[7] HIMSS Interoperability & Standards Committee, Technology Information Exchange Work Group, „Foundations for Healthcare Interoperability,“ Healthcare Information and Management Systems Society (HIMSS), 2014.

[8] National Rural Health Resource Center, „Privacy and Security Overview and Resource List,“ 2012.

[9] P. van Langenhove, K. Decreus, A. Rogala a T. Olyslaegers, „eHealth - European Interoperability Framework,“ European Commission – ISA Work Programme, Luxembourg, 2013, doi: 10.2759/15839.

[10] Evropská komise, „Recommendation on a European Electronic Health Record exchange format,“ 6. 2. 2019. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format. [Přístup získán 1. 5. 2019].

[11] J. Kopal, „Overview of national legislation on EHR in the Czech Republic,“ Milieu Ltd., Brussel, 2014.

[12] Q. Chen, J. Lambright a S. Abdelwahed, „Towards Autonomic Security Management of Healthcare Information Systems,“ IEEE First Conference on Connected Health: Applications, Systems and Engineering Technologies, Washington, 2016, doi: 10.1109/CHASE.2016.58.

[13] MuleSoft, „What is a REST API?,“ [Online]. Available: https://www.mulesoft.com/resources/api/what-is-rest-api-design. [Přístup získán 11. 3. 2019].

[14] JS Foundation, „Node-RED,“ [Online]. Available: https://nodered.org/. [Přístup získán 11. 3. 2019].

[15] Postscapes, „IoT Standards and Protocols,“ 5. 1. 2019. [Online]. Available: https://www.postscapes.com/internet-of-things-protocols/. [Přístup získán 11. 3. 2019].

[16] Y. Ding, B. Fan, X. Kong a Q. Ma, „Design and implementation of mobile health monitoring system based on MQTT protocol," 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Shenzhen, 2016, doi: 10.1109/IMCEC.2016.7867503.

[17] B. S. Sarjerao a A. Prakasarao, „Smart Healthcare Monitoring System Using MQTT Protocol," 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, 2018, doi: 10.1109/I2CT.2018.8529764.

[18] T. Jaffey, „MQTT and CoAP, IoT Protocols," Eclipse Foundation, Inc., [Online]. Available: https://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php. [Přístup získán 12. 3. 2019].

[19] National Institute of Standards and Technology, „Healthcare - Standards & Testing," 1. 3. 2017. [Online]. Available: https://www.nist.gov/itl/ssd/systems-interoperability-group/healthcare-standards-testing. [Přístup získán 25. 11. 2018].

[20] J. Aerts, „Towards a Single Data Exchange Standard for Use in Healthcare and in Clinical Research," University of Applied Sciences FH Joanneum, Institute of eHealth, Graz, 2018, doi: 10.3233/978-1-61499-858-7-55.

[21] M. Olschesky, „Inroduction to FHIR," Datica Health, Inc., 5. 2018. [Online]. Available: https://datica.com/academy/introduction-to-fhir/. [Přístup získán 6. 2. 2019].

[22] HL7 International, „FHIR," HL7.org, [Online]. Available: http://www.hl7.org/fhir/. [Přístup získán 14. 3. 2019].

[23] D. Bender a K. Sartipi, „HL7 FHIR: An Agile and RESTful Approach to Healthcare Information Exchange," CBMS, Hamilton, 2013, doi: 10.1109/CBMS.2013.6627810.

[24] M. Olschesky, „The FHIR Resource Object: The Core Building Block," Datica Health, Inc., 17. 5. 2018. [Online]. Available: https://datica.com/academy/the-fhir-resource-object-the-core-building-block/. [Přístup získán 16. 3. 2019].

[25] RESTfulAPI.net, „REST API Tutorial," [Online]. Available: https://restfulapi.net/. [Přístup získán 22. 3. 2019].

[26] T. Straka, „Bakalářská práce: Cloudové služby v prostředí technologické firmy," České vysoké učení technické v Praze, Praha, 2017.

[27] M. Ammar, G. Russello a B. Crispo, „Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications 38, Belgium, 2017, doi: 10.1016/j.jisa.2017.11.002.

[28] Amazon Web Services, Inc., „AWS IoT - Protocols," [Online]. Available: https://docs.aws.amazon.com/iot/latest/developerguide/protocols.html. [Přístup získán 1. 2. 2019].

[29] Amazon Web Services, Inc., „Roundup of AWS HIPAA Eligible Service Announcements," [Online]. Available: https://aws.amazon.com/blogs/aws/roundup-of-aws-hipaa-eligible-service-announcements/. [Přístup získán 1. 2. 2019].

[30] Amazon Web Services, Inc., „Amazon API Gateway," [Online]. Available: https://aws.amazon.com/api-gateway/. [Přístup získán 1. 2. 2019].

[31] Amazon Web Services, Inc., „InterSystems IRIS for Health Community," [Online]. Available: https://aws.amazon.com/marketplace/pp/B07N87JLMW/. [Přístup získán 1. 2. 2019].

[32] H. J. Cartwright, „FHIR Server for Azure: An open source project for cloud-based health solutions," Microsoft , 12. 11. 2018. [Online]. Available:

https://cloudblogs.microsoft.com/industry-blog/health/2018/11/12/fhir-server-for-azure-an-open-source-project-for-cloud-based-health-solutions/. [Přístup získán 1. 2. 2019].

[33] C. von See, „Getting to know the Google Cloud Healthcare API: Part 1," 31. 10. 2018. [Online]. Available: https://cloud.google.com/blog/topics/healthcare-life-sciences/getting-to-know-the-google-cloud-healthcare-api-part-1. [Přístup získán 3. 2. 2019].

[34] IBM Corporation, „IBM Watson IoT Platform," [Online]. Available: https://www.ibm.com/cz-en/marketplace/internet-of-things-cloud. [Přístup získán 16. 2. 2019].

[35] IBM Corporation, „IoT reference architecture," [Online]. Available: https://www.ibm.com/cloud/garage/architectures/iotArchitecture/reference-architecture. [Přístup získán 16. 2. 2019].

[36] IBM Cloud, „IBM Cloud platform service CLIs and APIs," [Online]. Available: https://console.bluemix.net/docs/overview/platform-cli-api.html#cli_api. [Přístup získán 5. 2. 2019].

[37] T. Hahn a J. Rao, „IoT security: An IBM position paper," IBM Corporation, Somers, 2016.

[38] IBM Corporation, „Watson Platform for Health GxP," [Online]. Available: https://www.ibm.com/support/knowledgecenter/SSSMS8/content/wp4h_gxp_kc_product_overview.html. [Přístup získán 5. 2. 2019].

[39] Cerner Corporation, „Cerner | code," [Online]. Available: https://code.cerner.com/. [Přístup získán 27. 3. 2019].

[40] Cerner Corporation, „Cerner Security Program," [Online]. Available: https://www.cerner.com/security. [Přístup získán 3. 4. 2019].

[41] Cerner Corporation, „SMART," [Online]. Available: https://fhir.cerner.com/smart/. [Přístup získán 27. 3. 2019].

[42] J. Mandel, „Microsoft, Amazon, Google, IBM, Oracle, and Salesforce issue joint statement for healthcare interoperability," Microsoft, 13. 8. 2018. [Online]. Available: https://cloudblogs.microsoft.com/industry-blog/health/2018/08/13/microsoft-amazon-google-and-ibm-issue-joint-statement-for-healthcare-interoperability/. [Přístup získán 11. 5. 2019].

[43] Nasuni Corporation, „NASUNI," [Online]. Available: https://www.nasuni.com/partner/ibm/. [Přístup získán 16 květen 2018].

[44] CloudMQTT, „Hosted message broker for the Internet of Things," [Online]. Available: https://www.cloudmqtt.com/. [Přístup získán 16 květen 2018].

[45] CloudMQTT, „Plans & Pricing," [Online]. Available: https://www.cloudmqtt.com/plans.html. [Přístup získán 16 květen 2018].

[46] IBM, „IBM Cloud," [Online]. Available: https://console.bluemix.net/. [Přístup získán 22. 4. 2018].

[47] SMART Health IT Project, „SMART," [Online]. Available: https://smarthealthit.org/. [Přístup získán 27. 3. 2019].

[48] J. C. Mandel, D. A. Kreda, K. D. Mandl, I. S. Kohane a R. B. Ramoni, „SMART on FHIR: a standards-based, interoperable apps platform for electronic health records," Journal of the American Medical Informatics Association, 2016, doi: 10.1093/jamia/ocv189.

[49] SMART Health IT, „SMART on FHIR," [Online]. Available: http://docs.smarthealthit.org/. [Přístup získán 10. 4. 2019].

[50] Cerner Corporation, „SMART on FHIR developer tutorial,“ GitHub repository, [Online]. Available: https://github.com/cerner/smart-on-fhir-tutorial. [Přístup získán 12. 4. 2019].

[51] Cerner Corporation, „Developer Portal,“ [Online]. Available: https://code.cerner.com/developer/smart-on-fhir/ . [Přístup získán 12. 4. 2019].