

UNIVERZITA HRADEC KRÁLOVÉ
FAKULTA INFORMATIKY A MANAGEMENTU
KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

System pro automatické vyhodnocení vitálních funkcí zvířat

DISERTAČNÍ PRÁCE

Autor: Ing. David Šec

Studijní program: P1802 Aplikovaná Informatika

Studijní obor: Aplikovaná informatika

Školitel: prof. RNDr. Peter Mikulecký, PhD.

Katedra/pracoviště školitele: Katedra informačních technologií

V Hradci Králové

duben 2024

PROHLÁŠENÍ

Prohlašuji, že jsem pojednání k doktorské zkoušce zpracoval/a samostatně a s použitím uvedené literatury a pramenů. Všechny zdroje, prameny a literaturu, které jsem při vypracování používal nebo z nich čerpal, v práci řádně cituji s uvedením úplného odkazu na příslušný zdroj.



Ing. David Šec

V Hradci Králové

dne 6. dubna 2024

ANOTACE

Moderní technologie se pomalu začínají postupně pronikat i do oblastí veterinárního zdravotnictví. Cílem práce je navrhnout a implementovat nový systém pro monitoring vitálních dat u zvířat, který dokáže autonomně monitorovat vybrané vitální funkce zvířat a zároveň dokázal reagovat na vybrané nestandardní situace. Základní požadavky na návrh systému byly definovány ve spolupráci s veterinárními zdravotníky. Následně bylo navrženo řešení celého systému založeného na technologii edge computing. Výhodou nově navrženého systému je jeho bezpečnost, vysoká škálovatelnost, propustnost dat a odolnost proti výpadkům internetového připojení.

ANNOTATION

Modern technologies are gradually making their way into the field of veterinary healthcare as well. The aim of this work is to design and implement a new system for monitoring vital data in animals, which can autonomously monitor selected vital functions of animals and also respond to specific non-standard situations. The basic requirements for the system design have been defined in collaboration with veterinary professionals. Subsequently, a solution for the entire system based on edge computing technology has been proposed. The newly designed system offers advantages in terms of security, high scalability, data throughput, and resistance to internet connection failures.

OBSAH

ÚVOD	1
1 CÍLE PRÁCE	1
2 METODIKA A STRUKTURA PRÁCE	7
3 LITERÁRNÍ REŠERŠE, EXISTUJÍCÍ ŘEŠENÍ PRO SBĚR VITÁLNÍCH FUNKCÍ	10
3.1 ZAŘÍZENÍ PRO MONITORING FITNESS AKTIVITY ZVÍŘAT	13
3.2 NOSITELNÁ ZAŘÍZENÍ PRO MONITORING SRDEČNÍ AKTIVITY.	14
3.3 MĚŘENÍ SRDEČNÍHO TEPU U ZVÍŘAT	16
3.3.1 <i>Přímá metoda měření tepu pomocí elektrických veličin na kůži zvířete</i>	17
3.3.2 <i>Nepřímé metody měření srdeční aktivity</i>	18
4 SPECIFIKACE SYSTÉMU	21
4.1 POŽADAVKY NA SYSTÉM	21
4.2 EXISTUJÍCÍ SYSTÉMY PRO SBĚR A VYHODNOCENÍ VITÁLNÍCH DAT	21
4.2.1 <i>Historie a vývoj telemedicíny</i>	21
4.2.2 <i>Zdravotní systémy pro vzdálený monitoring</i>	22
4.2.3 <i>Vědecké studie</i>	23
4.2.4 <i>Smart fitness zařízení pro sběr vitálních dat</i>	25
5 EDGE COMPUTING	28
5.1 EDGE COMPUTING – VYMEZENÍ ZÁKLADNÍCH POJMŮ	28
5.2 FOG COMPUTING.....	31
5.3 VÝHODY EC.....	32
5.4 PŘÍKLADY VYUŽITÍ EDGE COMPUTINGU	35
5.4.1 <i>Edge computing ve zdravotnictví</i>	35
5.5 PŘEDSTAVENÍ SYSTÉMU.....	38
5.6 TECHNICKÉ VÝZVY V IMPLEMENTACI SYSTÉMU	41
5.6.1 <i>Komunikace</i>	41
5.6.2 <i>Různorodost dat a standardizace obsahu zpráv</i>	42

5.6.3	<i>Zabezpečení – Obecné principy</i>	43
5.6.4	<i>Správa systému</i>	45
6	NÁVRH SYSTÉMU – IDENTIFIKACE JEDNOTLIVÝCH VRSTEV	46
6.1	SENZORY A EDGE GATEWAYS.....	46
6.2	EDGE NODE	46
6.3	CLOUD	54
7	IMPLEMENTACE SYSTÉMU, TECHNICKÉ VÝZVY	56
7.1	PROPUSTNOST SYSTÉMU	56
7.2	ZABEZPEČENÍ KOMUNIKACE	59
7.2.1	<i>Testování zranitelností</i>	61
7.3	KOMPONENTOVÝ PŘÍSTUP – VIZUALIZAČNÍ ŘETĚZEC	68
7.4	MAPOVÁNÍ NAMĚŘENÝCH DAT	71
8	MOŽNOSTI VYUŽITÍ NAMĚŘENÝCH DAT	74
8.1	VYHODNOCENÍ HR, BR, HRV	74
8.2	DETEKCE EMOCÍ	82
8.2.1	<i>Způsoby detekce emocí</i>	84
8.2.2	<i>Statistické analýzy HRV</i>	86
8.2.3	<i>Frekvenční analýza HRV</i>	90
8.2.4	<i>Potenciál dalšího využití dat</i>	92
8.3	DETEKCE ZÁCHVATŮ	93
9	ZHODNOCENÍ CÍLŮ DISERTAČNÍ PRÁCE	99
10	ZÁVĚR	102
11	POUŽITÁ LITERATURA	103
12	SEZNAM PUBLIKACÍ AUTORA	131
13	SEZNAM PROJEKTŮ A PODÍL AUTORA NA JEDNOTLIVÝCH PROJEKTECH	135
14	PŘÍLOHY	138

Seznam obrázků

<i>Obrázek 1: Přehled vyhledávání klíčových slov pomocí vyhledání Google; (autor).....</i>	<i>32</i>
<i>Obrázek 2: Návrh systému; (autor).....</i>	<i>38</i>
<i>Obrázek 3: Edge node – Schéma propojení jednotlivých modulů; (autor)</i>	<i>47</i>
<i>Obrázek 4: Ukázka definice metadat; (autor).....</i>	<i>48</i>
<i>Obrázek 5: Notifikace Ontologie systému; převzato z (Bunch et al. 2005) upraveno</i>	<i>52</i>
<i>Obrázek 6: Cloudová aplikace – Proces uložení a získávání dat; (autor).....</i>	<i>54</i>
<i>Obrázek 7: Ukázka základních metrik – Grafana; (autor).....</i>	<i>57</i>
<i>Obrázek 8: Graf závislosti délky výpočtu na počtu paralelních vláken; (autor).....</i>	<i>58</i>
<i>Obrázek 9: Nmap výstup dostupných zpráv; (autor).....</i>	<i>63</i>
<i>Obrázek 10: Wireshark – Analýza CONNECT paketu; (autor)</i>	<i>64</i>
<i>Obrázek 11: Přehled poskytovaných protokolů; (autor).....</i>	<i>66</i>
<i>Obrázek 12: Seznam kategorií podporovaných šifer; (autor).....</i>	<i>67</i>
<i>Obrázek 13: Test známých zranitelností TLS/SSL; (autor)</i>	<i>67</i>
<i>Obrázek 14: Výsledné hodnocení bezpečnosti; (autor)</i>	<i>67</i>
<i>Obrázek 15: Vizualizační řetězec – ukázka vybraných modulů a možností jejich nastavení; (autor) 69</i>	
<i>Obrázek 16: UML diagram implementace vizualizačního řetězce; (autor)</i>	<i>71</i>
<i>Obrázek 17: Mapování dat na konkrétní zvíře – seznam dostupných zařízení; (autor)</i>	<i>73</i>
<i>Obrázek 18: Znázornění průběhu ECG křivky a jednotlivých intervalů; (převzato z Jordans et al. 2013).....</i>	<i>75</i>
<i>Obrázek 19: Definování minimální snímkovací frekvence ECG signálů; ; (převzato z Jordans et al. 2013) upraveno.....</i>	<i>79</i>
<i>Obrázek 20: Ukázka spektrogramu měřeného signálu; (autor)</i>	<i>79</i>
<i>Obrázek 21: Vizualizace naměřeného signálu; (autor).....</i>	<i>80</i>
<i>Obrázek 22: Křivka dýchání; převzato z (Sec et al. 2018b).....</i>	<i>81</i>

<i>Obrázek 23: Graf znázornění RR intervalů pro výpočet HRV; (autor).....</i>	<i>85</i>
<i>Obrázek 24: Detekce RR intervalů v měřeném signálu (autor)</i>	<i>86</i>
<i>Obrázek 25: Graf délek RR intervalů; (autor)</i>	<i>87</i>
<i>Obrázek 26: Histogram porovnání četností délek intervalů dvou signálů; (autor).....</i>	<i>88</i>
<i>Obrázek 27: Poincarého graf – porovnání vzorků; (autor).....</i>	<i>89</i>
<i>Obrázek 29: Prototyp zařízení pro detekci záchvatů (vlevo) Detail display s přehledem o aktuálním stavu baterie a průběhu měření (vpravo); (autor)</i>	<i>96</i>

Seznam zkratek

A-D	Analog to Digital převod analogového signálu na digitální.
ACL	Access Controll List List pro kontrolu přístupů
AEAD	Authenticated encryption with associated data,
AED	Antiepileptic drugs Anitepileptika
AES	Advanced Encryption Standard standard pokročilého šifrování
ANS	Autonomic nervous systém Autonomní nrevový systém
BCG	Ballistocardiography Balistokardiaografie
BLE	Bluetooth Low Energy
BPM	Beats Per Minute Počet úderů za minutu
BR	Breath rate Dechová frekvence
CDI	Code Dependency Injection - Návrhový vzor pro vkládání závislostí
CoAP	Constrained Application Protocol Protokol navržený pro komunikaci zařízení s omezenými prostředky
COVID 19	Coronavirus disease 2019 Koronavirové onemocnění 2019
CSV	Comma Separated Values IETF RFC4180 Čárkou oddělené hodnoty

CT	Computed tomography - výpočetní tomografie, někdy také nazývaná také jako počítačová tomografie
DDoS	Distributed Denial of Service
ECC	Elliptic-curve cryptography Kryptografie eliptických křivek
ECG	Electrocardiogram, nebo také EKG jakožto jedna za základních vyšetřovacích metod v kardiologii.
EE	Enterprise Edition
EJB	Entity Java Bean - základní komponenta reprezentující perzistentní data v databázi
GATT	Generic Attribute profile
GCG	Giro Cardiology Gyrokardiografie
HF	High frequency Vysoká frekvence
HR	Heart rate hodnota seděcího rytmu udávaná v počtu úderů srdce za minutu
HRV	Heart rate variance Variabilita srdečního rytmu
HW	Hardware Fyzické zařízení
I-O	Input-output Vstupně-výstupní (například zařízení)
ID	Zkratka pro identifikaci - unikátní označení konkrétní položky.
IE	Idiopathic Epilepsy Idiopatická (primární) epilepsie
IoT	Internet of Things Internet věcí

JPQL	Java Persistence Query Language
JTA	Java Transaction API, Java API pro provádění Distribuovaných transakcí
LF	Low frequency Nízká frekvence
M2M	Machine to Machine Způsob komunikace mezi dvěma zařízeními
MQTT	Message Queuing Telemetry Transport
MRE	Magnetic Resonance Enterography, Magnetická rezonance
OLED	Organic Light-Emitting Diode
OOP	Object oriented programing Objektově orientované programování
ORM	Object–relational mapping, Objektově-relační mapování
PDF	Portable Document Format
PNS	Parasympathetic nervous system Parasympatikum
PPG	Photoplethysmography Photoplethysmografie
PSD	Power spectral density Výkonová spektrální hustota
QoS	Quality of service - Kvalita (dostupnosti) poskytovaných služeb
RHR	Resting Heart Rate, klidová tepová frekvence
RMSSD	Root Mean Square of Successive Differences Střední kvadrát kořenů rozdílů dvou následujících RR intervalů

RSA	(iniciály autorů Rivest, Shamir, Adleman) - šifrovací metoda se symetrickým klíčem
RTG	Röntgen radiation Rentgenové záření, nebo také zkratka pro označení vyšetření pomocí rentgenového záření
SCG	Seismocardiography Seismokardiografie
SDK	Software Development Kit
SDNN	Standard deviation of NN intervals – Standardní odchylka dvou následujících NN intervalů
SNS	Sympathetic nervous system Sympatikum
SQL	Structured query language, Standardizovaný strukturovaný dotazovací jazyk
SSL	Secure Sockets Layer
StE	Structural Epilepsy Strukturální epilepsie
SVM	Support Vector Machine
SW	Software Programové vybavení počítače
TCP	Transmission Control Protocol - nejpoužívanější protokol na transportní vrstvě
TLS	Transport Layer Security Šifrování na Transportní vrstvě
TLS-PSK	Transport Layer Security pre-shared key ciphersuites
UZV	Ultrazvuk - základní technika pro provádění neinvazivních vyšetření pro zobrazení tkání a měkkých orgánů

VLf	Very low frequency Velmi nízká frekvence.
VPN	Virtual Private network Virtuální Privátní Síť
WS	Web Socket - obousměrný komunikační protokol na jednom TCP spojení
WSS	Web Socket Secured - Web socket zabezpečený pomocí TLS šifrování

“My fashion philosophy is, if you’re not covered in dog hair, your life is empty.”

Elayne Boosler



1 ÚVOD

Převážná většina veterinárních zařízení se při výkonu práce spoléhá na nejmodernější přístupy a diagnostické přístroje. Proto při své práci uvítají jakékoliv řešení, které by usnadnilo monitoring životních funkcí zvířat bez zásahu lékaře, nebo v době jeho nepřítomnosti. S ohledem na tyto potřeby jsou otevřeni jakýmkoli inovacím umožňující veterinářům vykonávat svou práci mnohem efektivněji nebo alespoň přinést menší administrativní zátěž při vykonávání rutinních operací a během výkonu pravidelné lékařské péče u zvířat, která jsou čerstvě po podstoupení operativního zákroku, nebo naopak u pacientů s dlouhodobými chronickými obtížemi, kdy je pravidelný dohled naprosto nezbytný.

V posledním desetiletí se s rozvojem internetu věcí (Internet of Things - IoT) objevila celá řada řešení integrujících všemožné senzory a umožňujících vzdálené vyčítání dat přes internet. I když je samotný koncept IoT znám mnohem déle, údajně první kdo s myšlenkou připojení běžných zařízení k internetu přišel, byl (Kazar et al. 1982), avšak k jeho masivnímu rozšíření došlo až s příchodem cenově dostupných senzorů a mikročipů. Postupně tak vznikala celá řada systémů umožňujících sběr dat z nejrůznějších senzorů včetně nositelné elektroniky v podobě fitness trackerů, monitorujících fyzickou aktivitu sportovců. Ve veterinárním sektoru však stále neexistují obdobná zařízení, která by dokázala autonomně monitorovat životní funkce zvířat. Vzhledem k vysoké specializaci daného odvětví navíc nelze použít existující řešení, která často poskytují pouze velice základní informace, případně vyžadují přítomnost mobilního telefonu pro komunikaci se zařízením, nebo stabilní internetové připojení pro vyhodnocování dat.

Z tohoto důvodu bylo přistoupeno k tvorbě nového řešení využívajícího nejnovější přístupy a poznatky z oblastí IoT, cloud computingu a edge computingu a přinášejícího výhody obou přístupů, dokáže efektivně plnit požadované funkce a bude rovněž splňovat požadavky na bezpečnost systému a zabezpečení osobních dat, která se k takovému systému vážou.

Samotný pojem Edge computingu však není nijak exaktně vymezen a reprezentuje nejrůznější množství technologií, služeb a rozdílných přístupů. Samotný koncept vychází

z původního návrhu cloud computingu, pouze přináší některé výpočty dat blíže jejich zdroji, čímž jsou nejen zachovány některé výhody cloudových služeb jako vysoká elasticita, škálovatelnost a vzdálený přístup (Martens et al. 2012), ale navíc umožňuje snížit nároky na síť a výrazně tak zvýšit rychlost odezvy celého řešení. Dalšími benefity jsou rovněž vyšší odolnost systému vůči výpadkům internetového připojení, ale stejně tak i lepší škálovatelnost, nebo vyšší bezpečnost.

2 Cíle práce

Cílem práce je výzkum přístupů a technologií pro sběr a monitoring vitálních funkcí zvířat s následným návrhem a implementací systému s využitím moderních postupů a technologií. Celý proces měření by měl probíhat neinvazivně s důrazem na minimalizaci negativních dopadů na aktuální zdravotní i psychický stav zvířete. Za tímto účelem bude v disertační práci navržen, podrobně představen a následně implementován zcela nový systém, který si klade za cíl poskytovat detailní informace o aktuálním zdravotním stavu monitorovaných zvířat a zpracovávat tato data pro jejich pozdější zobrazení lékařem, ale také poskytovat automatické notifikace lékaři v případě výskytu nenadálé události. Systém rovněž musí být navržen tak, aby jej bylo možné využít v běžné zdravotnické praxi i pro následný pooperační monitoring hospitalizovaných zvířat a částečně tak nahradit nezbytný pravidelný lékařský dohled nad hospitalizovaným zvířetem. Systém musí být zároveň dostatečně mobilní za účelem přenosu (nezbytných částí systému) pro účely měření životních funkcí i mimo zdravotní ordinaci, např. pro zajištění nezbytné pooperační péče, nebo pro zajištění dlouhodobého dohledu nad zvířetem v domácích podmínkách.

Veškeré informace ze systému musí být k dispozici pro případný zdravotnický dohled nad pacienty, vyhodnocení rizikových situací pro pacienta a následné informování ošetřujícího lékaře. To vše musí být dostupné i pro léčbu dlouhodobě či chronicky nemocných zvířat.

Výsledný systém si klade za cíl usnadnit práci lékařům při vykonávání běžné zdravotnické praxe, zejména pak zajištěním nepřetržitého zdravotního dohledu nad zvířetem, ale i chovatelům zejména při zajištění asistence a domácí rekonvalescence zvířete. Dále by měl přispět k co efektivnějšímu sběru a vyhodnocování naměřených dat a poskytnout nejen informace o aktuálním zdravotním stavu, ale také dlouhodobé přehledy a statistiky umožňující zhodnocení efektivity poskytované péče a odrážející vývoj zdravotního stavu v dlouhodobém horizontu.

Základním předpokladem pro zajištění úspěšnosti navrženého řešení představuje efektivní sběr informací na základě požadavků jednotlivých zdravotních zařízení spolu s následným ověřením použitelnosti celého systému jeho dlouhodobým provozem přímo ve reálných podmínkách ve spolupráci s vybranými zdravotními zařízeními.

Naplnění cíle práce vyžaduje splnění jednotlivých dílčích cílů, které formují obsah práce a zároveň otevírají nové otázky pro jejich další výzkum:

1. Vymežit základní terminologii a provést analýzu současného stavu spolu s porovnáním existujících řešení dostupných v dané vědecké oblasti ať už v komerční řešení, nebo řešení zaměřené na vědu a výzkum.
2. Nalézt a stanovit klíčové funkce systému pro vyhodnocování dat a definovat jednotlivé pohledy na problematiku. Součástí zhodnocení bude detailní analýza jednotlivých komponent, jejich role v rámci systému a zhodnocení rizik vyplývající z použití konkrétní metody, nebo technologií.
3. Na základě provedené analýzy představit vybrané problémy a aplikovaná řešení vycházející z dostupné literatury a vlastních zkušeností autora nabytých v průběhu studia a participace na vědecko-výzkumných projektech s firemním sektorem v dané oblasti.
4. Nasadit a provozovat systém v reálném provozu a ověřit tak schopnost fungování systému v reálných podmínkách běžné veterinární praxe s cílem ověření robustnosti a použitelnosti navržené platformy a sběru dat pro další vědecké výzkumy i případný další rozvoj.

Jedním z prvotních cílů práce je tedy vymezení základních terminologií a provedení důkladné rešerše současného stavu spolu s detailním porovnáním všech dostupných řešení pokrývajících stejnou nebo příbuznou vědeckou oblast. Práce tak zahrnuje kompletní přehled literatury zabývající se danou oblastí včetně důkladného zhodnocení současného stavu výzkumu ale také zhodnocení technických a technologických aspektů jako jsou v současnosti dostupné nástroje a zařízení, která mohou být využita pro snímání, nebo zpracování dat v dané oblasti výzkumu, případně pro ověření správné funkce a zhodnocení bezpečnosti navrženého řešení.

Dalším z důležitých faktorů je porovnání aktuálně dostupných řešení a technologií s cílem zahrnutí komerčních i vědeckých projektů v dané oblasti. Jejich celkové zhodnocení a důkladná analýza současného stavu tak tvoří jeden ze základních pilířů samotného výzkumu a poskytují základní představu o směrech jakými by se měl ubírat budoucí vývoj a zároveň poskytnout nezbytný základ pro úspěšné naplnění dalších cílů výzkumu

a celkové objektivní zhodnocení výsledků výzkumu v porovnání s konkurenčními postupy.

Dalším z cílů je popis klíčových funkcí systému a identifikace klíčových funkcí nezbytných pro správné fungování celého systému je identifikace základních komponent systému a detailní popis jednotlivých částí nezbytný pro správné porozumění systému jako celku včetně popisu jakým způsobem systém pracuje a jak může být využit v praxi. Rovněž v práci nechybí stanovení různých pohledů na danou problematiku umožňující uživatelům systému definovat rozdílné pohledy na danou problematiku spolu s možností přizpůsobit si aktuální výstup svým potřebám a získat tak maximálně relevantní informace z vyhodnocovaných dat. Součástí zhodnocení systému bude rovněž detailní analýza jednotlivých komponent, jejich klíčové role v rámci celého systému, ale také definice jednotlivých funkcí v systému, včetně analýzy a posouzení rizik spojených s použitím konkrétních metod, nebo technologií.

Na základě uvedené analýzy představit vybrané problémy a aplikovaná řešení vycházející nejen z aktuálně dostupné literatury, ale také vlastních zkušeností autora nabytých v průběhu studia, participace na vědecko-výzkumných projektech, nebo v rámci spolupráce s firemním sektorem v dané oblasti.

Posledním z dílčích cílů práce je podrobení výsledného systému dlouhodobému testování v reálných podmínkách veterinární praxe v minimálně jedné lokalitě tak aby bylo možné objektivně zhodnotit nejen fungování systému jako celku, ale také jako nástroj pro včasnou identifikaci případných nedostatků v návrhu a implementaci systému a jejich následné odstranění v nadcházejících iteracích vývoje. Dlouhodobé testování si tak klade za cíl nejen ověření správné funkce všech navržených komponent ale také demonstrovat schopnost systému obstát v nejrůznějších situacích každodenního provozu v reálných podmínkách přímo u zákazníka.

Úzká spolupráce se zdravotníky již od raných fází vývoje rovněž poskytuje ideální příležitost pro zhodnocení výsledných částí a případnou konzultaci následného vývoje přímo se zdravotním personálem s cílem poskytnutí efektivní zpětné vazby i sběr podnětů pro budoucí vývoj systému pro zajištění maximální efektivity všech částí systému, případně zlepšení uživatelské zkušenosti.

Dlouhodobý provoz tedy neslouží pouze jako testovací prostředek, ale také jako aktivní nástroj pro dlouhodobý sběr dat z veterinární praxe. Tyto data mohou být následně využita jako základ pro další rozvoj jednotlivých výpočetních algoritmů, ale také pro další zpracování a případných budoucí výzkum zahrnující zkoumání nových možností vyhodnocení a detekce vitálních funkcí, emočních stavů, nebo výzkumu rozvoje onemocnění u zvířat, čímž dokáže přinést tak nové poznatky do oblasti veterinární medicíny a péče o zvířecí pacienty a přispět tak ke zkvalitnění veterinární péče.

3 Metodika a struktura práce

Teoretická část Disertační práce byla převážně zpracována kombinací metod systematického přehledu literatury, kde byla provedena detailní analýza současné literatury včetně aktuálně dostupných vědeckovýzkumných studií zabývajících se tématy bezprostředně související s tématem disertační práce, jakým je způsob snímání elektrických i neelektrických veličin, způsoby záznamu a vyhodnocení vitálních funkcí, případně aktuální metody zpracování a ochrany dat při přenosu. Cílem této metodiky bylo identifikovat klíčové trendy v existující literatuře, shrnout dosavadní poznatky a identifikovat případné mezery v existující literatuře, díky čemuž bylo možné vymezit základní rámec pro navrhovaný výzkum a předurčit tak směr pro následné směřování disertační práce.

Po vymezení základních oblastí výzkumu následuje detailní kvalitativní analýza s cílem hlubšího porozumění konkrétních výzkumných oblastí následovaná detailní analýzou vybraného problému a získání objektivních výsledků s cílem zohlednit získané poznatky a přístupy v praktické části práce včetně propojení informací z několika informačních zdrojů.

V části práce věnované zhodnocení existujících řešení je použita celá řada analytických metod, zejména pak klasifikační, datová, funkční a srovnávací analýza za účelem rozboru dané problematiky a identifikaci klíčových prvků systému. V případech, kdy je známa i konkrétní architektura systému, nebo dostupná implementace daného řešení jsou rovněž zhodnoceny použité výpočetní metody a případné nedostatky vyplývající z daného řešení, nebo použité architektury. Výsledný systém je posléze navržen tak, aby splňoval definované požadavky na systém, ale zároveň omezil, případně úplně eliminoval některé nedostatky již existujících řešení.

Architektura použitá při vývoji software vychází ze základních principů Edge computingu. Její vlastnosti a výhody daného řešení jsou detailně popsány v Kapitole 6. Při vývoji byly použity programovací jazyky Java, konkrétně byla použita platforma Jakarta Enterprise Edition (EE) ve verzi 10. Při vývoji systému byly následně využity metodiky agilního přístupu k vývoji software. Na vybrané části systému pak byly aplikovány metodiky prototypového přístupu s využitím poznatků z přechozího vývoje, nebo na základě poskytnuté zpětné vazby z reálného provozu.

Pro databázi byla na základě identifikovaných požadavků a následném zhodnocení dostupných řešení zvolena databáze PostgreSQL v kombinaci s NoSQL databází InfluxDB pro uchování naměřených časových řad představujících jednotlivá měření. V práci je rovněž kladen zvýšený důraz na bezpečnost dat. Za tímto účelem byly použity dostupné techniky pro zabezpečení komunikace mezi jednotlivými částmi systému, ale také vybrané postupy a nástroje zajišťující bezpečnost dat na úrovni lokálních uzlů. Vybrané Frameworky a podpůrné knihovny použité při vývoji software slouží pro maximální zajištění bezpečnosti celého řešení, ale také jako nástroje využívající vybrané návrhové vzory a usnadňující vývoj celého systému, případně obsahující mechanismy pro zajištění zvýšení propustnosti a celkové odezvy systému. Namátkou mohou být jmenovány například FlyWay, který zajišťuje snadné verzování databázové struktury a její automatickou správu napříč rozdílnými prostředími, Apache Delkatspike využívající výhody jazyka Java Persistence Query Language (JPQL) pro uložení rozsáhlých databázových struktur a převodu objektové struktury do podoby relační databáze. Dále byl v systému použitý Framework MyBatis, který rovněž poskytuje efektivní nástroj pro persistenci dat, ale na rozdíl od Apache Deltaispice je ale založený na vytváření jednodušších dotazů ve formě nativních SQL a XML schémat spolu pokročilými technikami ORM mapování a poskytuje tedy vhodnější řešení pro ukládání velkého množství dat. Stejně tak umožňuje lepší kontrolku nad SQL dotazy a jejich optimalizací. Další integrovanou knihovnou třetích stran je Retrofit, který slouží pro zajištění volání externích služeb prostřednictvím HTTP REST API a automatické mapování příchozích dat ve formátech JSON a XML do objektové struktury. Posledním významným použitým aplikačním frameworkem je PrimeFaces umožňující správu UI komponent a zajišťující efektivní mapování proměnných mezi frontendovými a backendovými částmi aplikace.

Celá práce je členěna do patnácti kapitol včetně úvodu, závěru, seznamu použitých informačních zdrojů, vědecko-publikační činnosti autora a seznamem projektů na kterých se autor práce podílel stručný popis projektu a způsob zapojení autora do projektu. V úvodní kapitole jsou vymezeny základní požadavky na navržený systém, podmínky a zaměření práce. Druhá kapitola definuje základní cíle práce. Následuje Kapitola 4 obsahující motivaci, identifikaci základní metodiky a stejně tak i zdůvodnění struktury práce. Kapitola 4 popisuje současný stav a literární rešerši aktuálně dostupných zařízení pro monitoring základních vitálních funkcí. Tato kapitola má za cíl informovat čtenáře

nejen o základních technikách měření těchto funkcí, ale také o základní povaze a struktuře naměřených dat prostřednictvím jednotlivých senzorů. Přinést základní představu o způsobech snímání vitálních funkcí, použitých technikách a orientačních snímkovacích frekvencích. Tato kapitola tak čtenáři poskytuje základní obrázek o celkovém množství dat produkovaných jednotlivými senzory. Následující kapitola představuje základní požadavky na systém na jejichž základech byly identifikovány a představeny jednotlivé technologie a postupy měření. Kapitola je zakončena představením komerčně dostupných řešení a vědeckých studií na téma sběru přenosu a vyhodnocení vitálních funkcí. V kapitole 6 následuje představení výhod navrženého řešení a srovnání s tradičními technikami cloud computingu, představení možností využití dané platformy v jednotlivých odvětvích a představení základní struktury systému spolu s identifikací klíčových funkcí pro zajištění správné funkce a zabezpečení systému. Následují kapitoly 8 a 9 zabývající se samotnou implementací navrženého řešení spolu s identifikací jednotlivých modulů a představením funkce každého modulu spolu s testováním zabezpečení a propustnosti systému. Kapitola 10 následně představuje další postup směřování disertační práce. Shrnuje aktuální stav systému, způsoby naplnění vytyčených cílů a představuje možnosti využití navržené architektury pro možnosti budoucího rozšíření systému a oblasti využití naměřených dat ze systému pro další výzkum.

Zhodnocení vytyčených cílů se stává klíčovým prvkem závěru této práce následovaný seznamy použité literatury, seznamu publikací autora práce a stručné představení projektů, na kterých se autor práce podílel v průběhu studia.

Jednotlivé kapitoly integrují vybrané myšlenky vycházející z dosavadní vědecko-výzkumné a publikační činnosti autora, které jsou průběžně podpořeny a případně dále doplněny prostřednictvím referencí z uvedeného seznamu použité literatury.

V práci je použita citační norma vychází ze standardní normy ČSN ISO 690:2011 s využitím harvardského citačního stylu, uvádějící autora a rok publikace.

Práce rovněž obsahuje celou řadu cizích slov a anglicismů, které jsou v určitých případech velmi těžko přeložitelné a jsou tedy v práci ponechány v jejich původní podobě. Tyto pojmy jsou následně vysvětleny v textu a případně doplněny o referenci odkazující na doplňující literaturu. Přímé citace a vybrané diagramy jsou rovněž v převážné většině ponechány v jejich původním znění.

4 Literární rešerše, existující řešení pro sběr vitálních funkcí

V současnosti je na našem trhu dostupná celá řada nejrůznějších zařízení spadající do kategorie nositelné elektroniky se zaměřením na snímání a vyhodnocení základních vitálních funkcí. Zařízení určená pro měření fitness funkcí u zvířat pak nejsou výjimkou. Některé aktuálně dostupné modely budou stručně představeny v následujících sekcích, kde bude rovněž popsána jejich funkce, použité technologie pro snímání jednotlivých veličin, nebo způsob komunikace s dalšími zařízeními pro vyhodnocení dat, případně prosté ukládání a následné poskytování naměřených dat uživateli. Tato zařízení jsou z velké části určena převážně nadšencům z řad chovatelů a kynologů a poskytují spíše základní soubor informací o aktuální fyzické kondici daného zvířete, než aby dokázali odhalit možné anomálie ve zdravotním stavu, nebo mohli posloužit jako diagnostický nástroj pro monitoring vitálních funkcí.

Pokud se zaměříme čistě na profesionální zdravotní sféru, tak zde prozatím neexistuje žádné řešení, které by umožňovalo vzdáleně monitorovat, byť jen základní vitální funkce u zvířat a zdravotní personál zde spoléhá spíše na pravidelné vizuální kontroly aktuálního zdravotního stavu zvířete v kombinaci s konvenčními metodami měření srdeční aktivity, které jsou v případě potřeby dále doplněné o stacionární nebo přenosné měřicí přístroje jako elektrokardiogram (ECG), případně ultrazvuk (UZV). V případě orientačního měření srdeční odezvy a dechové frekvence se však jedná zejména o prostý poslech jednotlivých srdečních ozvů.

Orientační měření srdeční odezvy a dechové frekvence představují poměrně jednoduchou ale zároveň efektivní metodu pro poskytnutí informací o aktuálním zdravotním stavu daného zvířete. Při poslechu srdečních tepů a dechových cyklů může lékař nebo jiný zdravotnický pracovník získat základní představu o tom, jak rychle a pravidelně tělo pracuje, ale také může odhalit abnormality srdečního rytmu, jako je například srdeční arytmie. Dechová frekvence pak poskytuje informaci o tom, s jakou frekvencí a jak účinně plíce pracují. Některé vnější vlivy jako je stres, nebo zvýšená fyzická aktivita, mohou způsobit zrychlení srdečního tepu a zvýšení dechové frekvence jako přirozená reakce těla na danou situaci, ale v některých případech může být rovněž příznakem potenciálních zdravotních problémů.

Existuje celá řada studií zaměřených na vztah majitele s jeho zvířecím mazlíčkem a jakým způsobem tato vzájemná vazba ovlivňuje fyziologii zvířat. Většina dostupných studií je zaměřená na psy, kde zkoumají dopady odloučení psa od majitele.

Jednou z těchto studií je (Maros et al. 2008), která provedla měření variability srdečního rytmu (HRV - Heart rate variability) u psů během období, kdy byli odděleni od svých majitelů, a porovnála je s měřeními, která byla provedena za shodných podmínek pouze za přítomnosti majitele. Výsledky ukázaly až 70% nárůst HRV u psů, kteří byli odděleni od svých majitelů. Tento nárůst HRV může být interpretován jako projev stresu a úzkosti, kterou psi cítí, když jsou odděleni od svých majitelů. Podobné studie také ukázaly, že pobyty ve zdravotních zařízeních, nebo útulcích mohou mít na psy podobné účinky, vlivem vystavení neznámému prostředí a oddělení od svých rodin a majitelů.

Stejně nepříznivě mohou zvířata rovněž reagovat na přítomnost neznámé osoby, nebo zdravotního personálu, což se rovněž může negativně podepsat na výsledcích měření. Pokud bychom tyto nepříznivé vlivy dokázali efektivně eliminovat například měřením bez trvalé přítomnosti lékaře, nebo přímo prováděním měření v domácích podmínkách a následně naměřená data poskytnout k posouzení lékaři, mohli bychom získat objektivní obrázek o aktuálním zdravotním stavu bez zbytečného stresování zvířat. Další nespornou výhodou pro použití autonomních měřících zařízení je možnost monitorovat paralelně i několik desítek různých zvířat najednou.

Je však důležité si uvědomit, že tyto základní diagnostické techniky pro měření srdeční odezvy a dechové frekvence nazývané též souhrnným názvem screeningová vyšetření jsou pouze prvotní a orientační metody poskytující pouze omezené a v mnoha případech i částečně zkreslené možnosti provedení základní diagnostiky zdravotního stavu. Pokud jsou v průběhu vyšetření zjištěny některé anomálie, následují další vyšetření a testy pro přesné určení původce daného problému a následné stanovení postupu další léčby. Výsledky však mohou být značně zkreslené právě vlivem zvýšené míry stresu během vyšetření.

Pro detailní záznam průběhu srdeční aktivity v čase se v současnosti spoléhá převážně na měření ECG. Možnostem měření ECG bude věnována samostatná kapitola, kde budou představeny základní principy snímání, měřené veličiny i obvyklé rozsahy snímkovacích frekvencí. Pro tento okamžik se však spokojíme pouze velice obecnou definicí, kdy se

jedná o podrobnou techniku měření spočívající ve snímání elektrických impulzů v čase vyvolaných funkcí srdečního svalu.

I když jsou obě poslechové metody i metody měření ECG spolehlivé a relativně rychlé, vyžadují trvalou přítomnost lékaře po celou dobu měření. Cílem tohoto výzkumu je vyvinout takové zařízení, které by umožnilo nepřetržitě monitorovat aktuální zdravotní stav zvířete a reagovat na nestandardní situace upozorněním zdravotního personálu, případně vykonáním jiné, předem zadané akce. Cílem systému není zcela nahradit profesionální zdravotnické vybavení, ani kompletně nahradit profesionální práci lékaře, ale naopak reagovat na aktuální potřeby zdravotního personálu na poskytnutí měřicího zařízení, které dokáže dlouhodobě monitorovat aktuální zdravotní stav bez nutnosti nepřetržitého dohledu lékařem, nebo poslouží jako dlouhodobý monitoring životních funkcí.

S využitím dlouhodobého monitoringu a s ním spojeným větším množstvím naměřených vzorků dat mohou rovněž přispět k utvoření celkového obrazu o zdravotním stavu zvířete v dlouhodobém horizontu. Cílem tohoto dlouhodobého monitoringu je nejen diagnostika aktuálního zdravotního stavu ale také monitoring dlouhodobých trendů s velmi dlouhou periodou opakování v řádu dnů, případně i (několika) měsíců. Dlouhodobým měřením konkrétní veličiny v čase může lékařům poskytnout cenné informace o dlouhodobém vývoji a trendech ve zdravotním stavu pacientů, což může vést k objevení skrytých vzorců, identifikaci potenciálních zdravotních problémů, nebo optimalizaci léčebných postupů. V neposlední řadě tato data mohou posloužit pro účely dlouhodobé statistiky která může hrát klíčovou roli při stanovení účinnosti a vývoje léčby u dlouhodobě nemocných zvířat, případně při léčbě chronických onemocnění.

Při hledání existujících řešení byly zohledněny jak hotová komerční řešení, tak některé studie v podobě vědeckých publikací. Jednotlivé výsledky byly následně rozděleny do kategorií, podle množství měřených funkcí a technologie použité pro snímání měřených veličin. U každé technologie je stručně popsán princip snímání, typické vzorkovací frekvence, ale stejně tak i její výhody a případná negativa spojené s využitím této techniky pro měření vitálních funkcí.

4.1 Zařízení pro monitoring fitness aktivity zvířat

První kategorií zařízení jsou zařízení, která mají za úkol monitorovat aktivní pohyb zvířete a poskytovat tak chovateli aktuální obraz o fyzické kondici zvířete. V současnosti probíhá na trhu velký boom v oblasti nositelné elektroniky nejen pro lidi, ale také pro zvířata a výrobci se předhánějí v představení nejrůznějších variant zařízení pro snímání základních vitálních funkcí. Nejčastěji je tato elektronika zaměřena primárně na psy, a to nejen z důvodu celkové vyšší váhy zařízení ve stovkách gramů ale také povahou nabízených funkcí jako je například detekce štěkání. I když někteří výrobci uvádějí, že je zařízení vhodné i pro kočky, dá se předpokládat, že jednotlivé výpočetní algoritmy budou rovněž zaměřeny primárně na měření fyzické aktivity u psů.

Instalace probíhá vždy připečením zařízení na obojek zvířete a následné spárování zařízení s mobilním telefonem, nebo speciální stanicí. Mezi nejznámější komerčně dostupná zařízení můžeme zařadit FitBark (FitBark Inc. 2019), PitPat (Pitpatpet Ltd 2019), WonderWoof (Wondermento Inc. 2017), případně celou řadu dalších zařízení. Funkce všech těchto zařízení je však velice obdobná a z hlediska měření vždy spočívá na jednoduchém principu snímání zrychlení pomocí akcelerometru a výpočtu jednotlivých kroků jako výsledný vektor zrychlení každého vzorku měřeného signálu. Následně jsou aplikovány lineární filtry tak, aby se ze signálu odstranil nežádoucí šum. Jedná se zpravidla o dolní propust eliminující frekvence nad 4,5Hz, což po přepočtu odpovídá odfiltrování všech hodnot přesahujících hodnotu 270 kroků za minutu. Na takto vyfiltrované hodnoty mohou být následně aplikovány další korekční mechanismy, jako například detekce chyby prvního druhu (*false-positive*), nebo doplněním výpočtu o hladinu významnosti alfa s cílem zajištění vyšší spolehlivosti výpočtů a zvýšení důvěryhodnosti poskytovaných dat.

Detailní princip snímání chůze za pomoci akcelerometrů, nebo gyroskopů ať už zabudovaných přímo v mobilním telefonu, nebo s pomocí přídavných nositelných zařízení včetně dalších technik pro zpřesnění vyhodnocení měřeného signálu popisují například publikace (Mladenov a Mock 2009; Zhao 2010; Muset a Emerich 2012; Abadleh et al. 2017). Základní algoritmy pro výpočet detekce chůze a následného celkového počtu kroků za dané období jsou poměrně nenáročné na implementaci. Samotný vyhodnocovací algoritmus rovněž nevyžaduje vysoké výpočetní ani paměťové

nároky a může tak být snadno implementován přímo jako součást měřicí elektroniky na jednoduchém čipu uvnitř těchto nositelných zařízení. Jednotlivá data mohou být uchována uvnitř zařízení a synchronizována v pravidelných dávkách např. jednou denně. Měření je u některých modelů dopěno o data z gyroskopu, případně GPS polohu zařízení získanou přímo ze zařízení, nebo doplněnou na základě časové známky z dat o poloze poskytovaných mobilním telefonem.

Data jsou následně odesílána nejčastěji pomocí technologie Bluetooth do mobilního telefonu, případně dále do cloudových služeb výrobce zařízení. Z dat o počtu kroků spolu s časovou známkou lze následným zpracováním časových známek rozlišit chůzi od běhu, odhadnout celkovou překonanou vzdálenost a pomocí kalorických tabulek a zadané váhy zvířete určit množství spálených kalorií za den. Z naměřených dat lze rovněž vypočítat další hodnoty jako celková doba spánku, koeficient spánku, nebo health index.

4.2 Nositelná zařízení pro monitoring srdeční aktivity.

Jediné z komerčně nabízených zařízení na trhu pro monitoring dechu a srdeční aktivity poskytuje společnost PetPace (PetPace 2018). Stejně jako předchozí zařízení využívá i tento systém senzoru připevněného na obojek psa. Obojek monitoruje a vyhodnocuje sedm základních údajů o zdravotním stavu psa, jakými jsou teplota na povrchu kůže, dech, pulz a hodnoty jako množství spálených kalorií, polohu a úroveň aktivity. Poslední funkcí, kterou výrobce nabízí, je vyhodnocování a predikce stresu, bolesti a nemoci. Toto zařízení se rovněž jako jediné z nabízených pyšní algoritmy pro detekci epileptických záchvatů u psů.

Sám výrobce však uvádí, že tato funkce je stále ve fázi vývoje a spočívá na poměrně jednoduchém principu porovnávání naměřených dat s historickými záznamy. V případě, že je u psa identifikován záchvat, je uživatel vyzván k zanesení přesného času výskytu záchvatu do systému. Do systému se následně uloží hodnoty vitálních funkcí, které předcházeli vyvolání záchvatu a systém v následně za pomoci technik strojového učení porovnává aktuálně naměřená data s podmínkami, které byli příčinou vyvolání záchvatu. Kdykoliv aktuální kombinace hodnot přesáhne definovanou mez, je zaslána informace majiteli psa prostřednictvím emailu, nebo telefonátu o možném budoucím výskytu

záchvatu. Podrobnější informace o způsobu vyhodnocení, ani jakým způsobem jsou signály korelovány však již výrobce bohužel neuvádí.

Samotná konstrukce měřicího zařízení je složena ze dvou částí, z obojku, na kterém jsou umístěny měřicí akcelerometry snímající pohyb ve třech nezávislých osách, a základnové stanice, která je umístěna v blízkosti psa. Ta slouží pro příjem dat ze senzorů na obojku. Snímkovací frekvence je pouze 1 Hz, tedy jeden měřený vzorek za vteřinu. Akcelerometry rovněž slouží pro určení orientace polohy obojku, a tedy i určení polohy měřeného zvířete. Poloha zvířete může být měřena pouze v klidu, proto je snímání polohy aktivováno pouze pokud nebyla u zvířete detekována aktivita po dobu alespoň šesti vteřin. Obojek rovněž detekuje dechovou a tepovou frekvenci pomocí vestavěného akustického senzoru na vnitřní straně obojku. Akustická detekce však může být velice snadno rušena okolním hlukem, nebo přímo pohybem měřeného zvířete, nebo jinak negativně ovlivněna nedostatečným přilehnutím senzoru ke krku zvířete, což potvrzují také výzkumy (Belda et al. 2018) a (Ortmeyer et al. 2018), který uvádí že měření probíhá vždy ve dvou minutových intervalech, přičemž za úspěšné vyhodnocení je považováno takové měření, během kterého bylo rozpoznáno alespoň 40 úderů srdce. Naměřená data jsou bezdrátově přenášena do základnové stanice. Technologii použitou pro přenos však výrobce bohužel neuvádí. Efektivní dosah okolo deseti metrů však naznačuje použití technologie Bluetooth.

(Ortmeyer et al. 2018) Posledním článkem systému je cloudová aplikace sloužící pro agregaci a vyhodnocení naměřených dat. Synchronizace dat z obojku probíhá v pravidelných intervalech od 2 do 120 minut v závislosti druhu dat, ale liší se také dle typu a výše předplatného. V těchto intervalech jsou však data pouze synchronizována nikoliv vyhodnocována. Samotné vyhodnocení pak probíhá v patnáctiminutových až dvouhodinových intervalech a výsledkem je vždy pouze jedna hodnota za daný časový úsek.

V posledních třech letech se rovněž objevila spousta vědeckých studií využívající zařízení PetPace jako zařízení pro sběr dat ze psů a koček a jejich následné vyhodnocení. Namátkou lze uvést například (Ortmeyer et al. 2018) který zkoumal vyhodnocení záchvatů u jedenácti psů přičemž pro vyhodnocení používal zařízení PetPace a Actigraph GT9X s vestavěným akcelerometrem. Zatímco u slabších záchvatů autor naměřil silnou

korelaci s r-hodnotou přesahující 0,7 mezi oběma zařízeními, u silných záchvatů již korelace obou hodnot prokázána nebyla. Sám autor to vysvětluje omezeným množstvím naměřených vzorků, kdy se silný záchvat projevil pouze u jednoho psa, ale osobně bych se rovněž přikláněl k omezeným možnostem snímkovací frekvence zařízení PetPace, která je řádově nižší než u zařízení Actigraph. U něj byla v průběhu experimentu snímána data s mnohem vyšší frekvencí 30 Hz a měl tak vyšší potenciál na odhalení případných záchvatů.

4.3 Měření srdečního tepu u zvířat

Nejčastěji používanou metodou pro měření detailního průběhu srdečního tepu je Elektrokardiograf (ECG). Jedná se o základní neinvazivní metodu vyšetření v kardiologii, která měří elektrickou aktivitu srdce pomocí elektrod, které jsou u lidí umístěny na kůži v oblastech hrudníku, rukou a nohou. V případě psů se elektrody umísťují na přední tlapy a spodní část břicha. Tato srdeční aktivita je pak zaznamenána v podobě ECG křivky, která ukazuje změny elektrického potenciálu během jednotlivých fází srdečního cyklu.

Výsledkem měření je ECG křivka, která velmi podrobně znázorňuje informace o jednotlivých fázích srdečního cyklu. Jednomu stahu srdce odpovídá vždy jeden pulz měřeného signálu. Detailní princip a funkce ECG a význam jednotlivých fází měřeného signálu popisuje například (Hampton 2013). Cílem našeho výzkumu není vyvinout systém, který by dokázal plně nahradit měření ECG, ale poskytnout řešení, které poskytne srovnatelné výsledky bez dodatečné obsluhy. I když je ECG považováno za zlatý standard v oblasti monitoringu srdeční odezvy, jedná se o poměrně drahý způsob měření, který navíc vyžaduje nepřetržitou pozornost lékaře a pro dlouhodobý monitoring několika desítek zvířat se proto tato technika stává značně nepraktickou a finančně náročnou. Dále je tu nutnost aplikace měřících elektrod, která s sebou často přináší lokální odstranění srsti.

Z výše popsaných důvodů budou v následujících sekcích představeny alternativní postupy a vědecko-výzkumné projekty zabývající se měřením srdeční aktivity zvířat. Budou popsány použité technologie pro snímání srdečního tepu spolu s metodikou a postupy vyhodnocení měřených veličin, ale také množství produkovaných dat, které

je nutné posléze vyhodnotit. To zpravidla probíhá až po dokončení měření individuálním posouzením lékařem, nebo specializovanými matematickými softwarovými nástroji.

4.3.1 Přímá metoda měření tepu pomocí elektrických veličin na kůži zvířete

První z možností měření je snímání elektrických veličin přímo na kůži zvířete. Tato technika funguje na stejném principu jako zmíněné ECG. Na kůži zvířete jsou nalepeny, nebo přiloženy elektrody, které snímají rozdíly napětí vznikající šířením akčního potenciálu myokardem. Dle (Škraňková 2017) je hodnota akčního napětí měřitelná přímo na povrchu srdce až +20mV. Toto napětí se však vlivem vnitřního odporu těla podstatně snižuje, přičemž největší podíl na tomto úbytku napětí má právě samotná kůže zvířete. Proto je zcela nezbytné zajistit co možná nejlepší kontakt měřících elektrod právě s povrchem těla a minimalizovat tak další přechodový odpor mezi kůží a měřící elektrodou. Proto se většina dostupných publikací spoléhá na větší množství paralelně uložených elektrod, které pomáhají tento přechodový odpor minimalizovat. (Brugarolas et al. 2016) podrobně zkoumá závislost množství použitých elektrod na velikosti přechodového odporu. Množství použitých elektrod se tak běžně pohybuje mezi jedním až deseti kusy, (Virtanen et al. 2018) používá dokonce až 30 paralelně uložených elektrod. Vlivem měření střídavých napětí se však kromě přechodového odporu projeví rovněž kapacita, která má za následek impedanci, silně závislou právě na periodě měřeného signálu. Tato impedance se projeví převážně při nižších frekvencích snížením amplitudy měřeného signálu. (Brugarolas et al. 2016) uvádí útlum v nízkých frekvencích v řádu jednotek až desítek kilo Ohmů. Pro minimalizaci impedance však musí být elektrody dokonale čisté, což se zejména z dlouhodobého hlediska jeví jako velký problém. Autor dále doporučuje odstranění srsti zvířete v oblasti, kde dochází ke kontaktu elektrod s kůží a použití vodivého gelu, což se velmi často setkává s nelibostí chovatelů a majitelů zvířat. Výsledné napětí měřitelné na povrchu kůže se tak reálně pohybuje v řádu jednotek mV. (Eckenfels 1986) uvádí maximální amplitudu R-vlny rozmezí od 0,5-2,7 mV.

Na trhu existuje celá řada nejrůznějších zařízení pracujících na principu snímání elektrických veličin vyvolaných srdeční aktivitou na povrchu těla. Jednotlivé modely se však mohou ve své funkci značně lišit, a to především v tom, zda umožňují zaznamenat pouze počet pulzů, tedy počet úderů srdce v čase, nebo i jejich přesný tvar. Od toho jsou

následně odvozeny nejen konstrukční parametry daného přístroje, zejména pak jeho snímkovací frekvence a s tím související velikost interní paměti pro uchování záznamů, ale i využití daného přístroje.

Zatímco prostý čítač impulzů dokáže spolehlivě určit tepovou frekvenci (Heart rate – HR) a její variabilitu v čase (Heart rate variance – HRV) a postačí frekvence v jednotkách až desítkách snímků za sekundu, pro vizualizaci detailního průběhu jsou již nezbytné řádově vyšší snímkovací frekvence. V případě zachycení detailního průběhu lze určit například pravidelnost srdečního rytmu, z čehož lze následně identifikovat nejruznější srdeční vady, ať už vrozené, nebo způsobené dalšími vlivy například s přibývajícím věkem zvířete (Sec et al. 2018b).

Možnosti monitoringu HR a HRV pomocí snímání elektrických veličin přímo z povrchu těla domácích i hospodářských zvířat se v minulosti věnovala řada projektů. Některé z nich využívají vlastní konstrukci pro měření například (Eckenfels 1986; Mohr et al. 2002; Lahdenoja et al. 2019), jiná naopak spoléhají na již existující řešení (Quintana et al. 2012; Essner et al. 2015; Brugarolas et al. 2016). Zde se nejčastěji se jednalo o hrudní pásy určené pro sportovce od společnosti Polar. Snímkovací frekvence se u jednotlivých metod značně liší a je závislá primárně na požadovaném průběhu měření. Pro zachycení základní tepové frekvence se snímkovací frekvence pohybují v rozmezí od 300 Hz až 600 Hz. Pro zachycení detailního tvaru křivky ECG jsou však třeba frekvence vyšší. V takových případech se nejčastěji používaly frekvence okolo 1000 Hz.

4.3.2 Nepřímé metody měření srdeční aktivity

Oproti přímým metodám měření srdečního tepu existují i jiné metody snímání srdeční aktivity založené na nepřímém měření mechanických pohybů způsobených změnou tlaku krve ve velkých tepnách vyvolanou srdeční kontrakcí (Gordon 1877; Frederick a Eddleman 1958). Mezi dostupné techniky měření patří Seismokardiografie (Seismocardiography – SCG), Balistokardiaografie (Ballistocardiography – BCG), Gyrokardiografie (Giro Cardiography – GCG), případně Photoplethysmografie (Photoplethysmography – PPG).

SCG je metoda založená na snímání vibrací hrudníku vyvolaných stahováním a opětovným rozpínáním srdeční komory při pumpování krve do krevního řečiště. Poprvé na tento jev upozornil (Gordon 1877), když pozoroval, jak člověk stojící na váze dokáže rozkmitat ručičku vah pouze tlukotem svého srdce. V současné době lze snímání provádět akcelerometrem na hrudi zvířete. K tomuto účelu se nejčastěji používají tříosé akcelerometry s nízkou hladinou šumu, jako například (Di Rienzo et al. 2011), který používá tříosé akcelerometry pro monitoring vitálních funkcí u kardiaků. Akcelerometr měří zrychlení vyvolané pohyby hrudníku a výsledný signál je dále filtrován a zpracováván. Způsoby zpracování se však mohou velice lišit již od samého začátku, kdy některé metody používají pro zpracování pouze jednu (dominantní) osu (Zanetti a Tavakolian 2013; Anon. [b.r.]), jiné naopak zpracovávají signál ze všech os (Sec et al. 2018b; Cimr a Studnička 2020). Detailní přehled o metodě SCG a jejích výhodách i nevýhodách, ale i způsobech využití popisuje např. (Zanetti a Tavakolian 2013; Castiglioni et al. 2007). Výzkum automatické detekce fibrilací srdečních síní za pomoci SCG dat pak (Hurnanen et al. 2017).

BCG je metoda založená na snímání nikoliv přímo srdeční aktivity samotné, ale měří mechanickou reakci srdce na elektrické podněty a další jevy související s pohybem krve. (Pinheiro et al. 2010; Cimr a Studnička 2020). Konkrétně se jedná o měření sil způsobených srdeční kontrakcí a zrychlením pohybu krve uvnitř velkých cév. Výsledný signál lze snímat pomocí piezoelektrických senzorů (Zink et al. 2017), soustavou akcelerometrů a gyroskopů (Wiens a Inan 2015;), nebo tenzometrů (Cimr a Studnička 2020). Vzorkovací frekvence se v závislosti na použitých senzorech pohybují od 100 do 1000 Hz. Srovnání BCG a SCG spolu s dostupnými metodami měření a použitými senzory, stejně jako výhody každého z řešení popisuje například (Inan et al. 2015).

GCG je neinvazivní metoda snímání srdeční aktivity založená na snímání změny polohy a uhlové rychlosti hrudníku vyvolané mechanickými pohyby srdce, konkrétně levou srdeční komorou. Sensor je umístěn ve středu hrudníku a mikro pohyby hrudníku vyvolávají změnu polohy otáčení jednotlivých os gyroskopu. Ty jsou následně zaznamenány jako gyrokardiogram, který odpovídá jednotlivým stahům srdce. Výhodou této metody je nižší náchylnost gyroskopů na vnější vibrace a vnější magnetické pole Země, stejně tak jejich nízká pořizovací cena a dostupnost tohoto senzoru v převážné většině mobilních telefonů a nositelných zařízení. Snímkovací frekvence se pohybují

v rozsahu od 400 do 800 Hz. (Marcelli et al. 2007; Inan et al. 2015; Tadi et al. 2016; Yang a Tavassolian 2018).

Poslední z představených metod je **PPG**, která je založena na optickém měření průchodu krve drobnými cévami pod povrchem kůže. Princip spočívá v prosvětlení povrchu kůže nejčastěji červeným nebo infračerveným zdrojem světla o vlnové délce 600 – 940 nm (Kamal et al., 1989; Gotter, 2017) a následném a snímání změn v množství pohlcovaného světla krví protékající těmito cévami (Hayes a Smith 1998; Alian a Shelley 2014). Touto metodou tak lze nejen měřit srdeční tep, ale i množství hemoglobinu, resp. množství kyslíku v těle. I přes to, že tato metoda vyžaduje těsný kontakt zdroje světla i detektoru s kůží, byla úspěšně provozována pro měření srdeční frekvence u zvířat bez nutnosti odstranění srsti, což dokazuje například publikace (Brugarolas et al. 2016) využívající pro průchod srstí optická vlákna. Naproti tomu (Cugmas et al. 2019) měří srdeční tep a množství kyslíku v těle na povrchu jazyka, na tlapách, uších, nebo ocasu. Sám autor však tuto techniku uvádí jako použitelnou pouze v případech, kdy je zvíře znehybněno, nebo v celkové anestezii.

Velkou výhodou všech výše popsaných metod je, že je lze provozovat zcela neinvazivně a veškeré měřené senzory mohou být umístěny ať už přímo na těle zvířete jako malá nositelná zařízení. Zde se úspěšně využívají metody SCG, GCG, MCG, případně PPG. U určitých metod však není nutné na zvíře umisťovat žádné senzory, ale veškeré měřící zařízení mohou být integrovány jako součást podložky na kterou je možné zvíře dočasně, nebo dlouhodobě umístit. Zde se jedná převážně o metodu BCG. Existují rovněž případy, kdy jsou jednotlivé metody zkombinovány, Typickým příkladem může být kombinace SCG a GCG (Yang a Tavassolian 2018; Kaisti et al. 2019). Nevýhodou těchto nepřímých metod měření je však fakt, že měřený signál je ve většině případů založen na snímání velice drobných mechanických výchylek, který však může být nepříznivě ovlivněn dalšími vlivy jako jsou pohyby zvířete, případně vnějšími vibracemi přenášenými z okolí a mít tak za následek zkreslení, nebo v některých případech úplně znemožnění detekce srdečního tepu. Proto je nezbytné do výpočtu zahrnout metody pro redukci těchto nežádoucích vlivů. Jednou z možností jsou již zmíněné filtry pro odstranění nežádoucích frekvencí. V případě PPG může být výsledný signál ovlivněn množstvím ambientního světla z okolí. Redukcí nežádoucích vlivů v PPG se věnuje například (Hayes a Smith 1998).

5 Specifikace systému

Na základě požadavků zdravotního personálu a požadavků na informační bezpečnost shromažďovaných dat a další vývoj systému byly identifikovány následující systémové požadavky.

5.1 Požadavky na systém

- Aktuální informace o vitálních funkcích zvířete musí být k dispozici i v případě výpadku internetového připojení.
- Veškerá data z lokálních senzorů musí být vyhodnocována lokálně a takřka v reálném čase.
- Surová data ze senzorů musí být dostupná v centrálním úložišti, a to ze všech lokalit a po celou dobu měření. Tato data poslouží pro účely dalšího vývoje a ladění algoritmů.
- Systém musí být schopný upozornit lékaře na náhlou změnu zdravotního stavu pacienta, a to i v případě ztráty spojení.
- Data v lokálním i centrálním úložišti musí být dostatečně chráněna proti zneužití citlivých údajů. Soukromá data musí být uložena pouze lokálně.

5.2 Existující systémy pro sběr a vyhodnocení vitálních dat

5.2.1 Historie a vývoj telemedicíny

Pojem Telemedicíny poprvé definoval Kenneth T. Bird v roce 1971 jako lékařskou praxi bez nutnosti obvyklé fyzické konfrontace mezi lékařem a pacientem za použití interaktivního audio video komunikačního systému, ale první snahy o diagnostiku zdravotního stavu na dálku se objevují již s rozvojem prvních telekomunikačních sítí jako byly telefonní, nebo telegrafní sítě. Například (Duplaga a Zieliński 2006) uvádí jako období začátku rozvoje Telemedicíny na konci 40. let 20. století, konkrétně v roce 1948, kdy byly první radiologické snímky pořízené v nemocnici West Chester přeneseny pomocí běžné telefonní linky do cca 60 km vzdáleného pracoviště ve Filadelfii ve státě Pensylvánie. V roce 1959 byl v USA zřízen uzavřený televizní vysílací okruh umožňující

přenos neurologického vyšetření pro edukativní účely na vzdálená pracoviště a používání televizního přenosu se později stalo běžnou praxí (Bashshur et al. 1975; Perednia a Allen 1995).

O tři roky později dokonce vznikl vyhrazený krátkovlnný kanál mezi Nebraským psychiatrickým ústavem a Státní nemocnicí Norfolk sloužící pro účely diagnostiky onemocnění v oblastech dermatologie, radiologie, kardiologie a psychiatrie.

Jak již bylo z výše uvedených příkladů naznačeno, Telemedicína poskytuje užitečný nástroj pro vzdálenou diagnostiku, nebo konzultaci zdravotního stavu pacienta s využitím audio-video vizuální techniky a přináší benefity jako je efektivnější a rychlejší dostupnost zdravotní péče ve vzdálených lokalitách. Později své uplatnění našly také jako efektivní a cenově dostupný přístup k odborné zdravotní péči ve velmi vzdálených lokalitách jakými jsou například odlehlé oblasti a výzkumné stanice za polárním kruhem, pracoviště umístěná na širém moři, případně v těžko přístupných vysokohorských oblastech. Dokáží tak poskytovat rychlejší zdravotní péči bez nutnosti zdlouhavého cestování a v neposlední řadě také umožňuje úsporu nákladů na cestování i léčbu samotnou.

Telemedicína rovněž sehrála svou nezastupitelnou roli v dobách pandemie COVID-19, kdy se právě telemedicína stala jedním z mála dostupných prostředků základní diagnostiky pacientů v izolaci a lze říci, že právě pandemie COVID-19 přispěla k masivnímu rozšíření telemedicíny i do povědomí široké veřejnosti a stala se tak nepostradatelným zdrojem pro zlepšení dohledu na pacienty v izolaci, jako dostupný nástroj pro včasnou identifikaci nákazy a následnou péči během nákazy, ale především pro prvotní diagnostiku momentálního zdravotního stavu, nebo jako nástroj pro zajištění kontinuity zdravotní péče o chronicky nemocné pacienty v průběhu pandemie.

5.2.2 Zdravotní systémy pro vzdálený monitoring

V následující kapitole budou zmíněna některá komerčně dostupná řešení pro měření libovolných vitálních funkcí u lidí.

Quardio (Qardio, Inc, 2020) je jediné z komerčně dostupných služeb pro monitoring vitálních funkcí zahrnující nejrůznější zařízení v podobě vah, ale také tlakoměrů, nebo

zařízení pro měření ECG. Data z těchto zařízení jsou následně synchronizována s mobilní aplikací a odesílána do cloudu, kde probíhají jejich další statistické analýzy v podobě trendů a korelací, případně vyhodnocení rizikových situací. Konkrétní metodiku výpočtu, ani přehled vstupních parametrů výrobce bohužel neuvádí. Výsledkem je však pouze zatřídění rizikových pacientů do tří skupin podle míry rizika. Takto naměřená data mohou být následně nasdílena k nahlédnutí lékaři. Systém rovněž umí z naměřených dat vytvořit report za dané období v podobě PDF souboru, který lze později lékaři předložit. Jedná se tak spíše o systém pro pasivní sběr dat bez možnosti jejich vyhodnocování v reálném čase. Přístup k datům je prostřednictvím již zmíněné mobilní aplikace, odkud lze hodnoty vyexportovat ve formě CSV a PDF souborů. Jakýkoliv další způsob přístupu k naměřeným datům však výrobce neuvádí.

5.2.3 Vědecké studie

Vzhledem k akutnímu nedostatku komerčně dostupných řešení bylo přistoupeno k vyhledávání dalších dostupných řešení v oblasti vědecko-výzkumných publikací. Na základě toho byly v dostupných vědeckých databázích identifikovány publikace obsahující klíčová slova jako Medical support system, Decision support system, Medical sensor system, IoT medical, Edge computing medical system. Vybrané výsledky zabývající se sběrem a zpracováním dat, jejich přenosem, nebo nejrůznějšími technikami automatického vyhodnocování, jsou shrnuty a zhodnoceny v následující kapitole.

S myšlenkou aplikace sloužící pro ukládání dat z oblasti medicíny a jejich sdílení mezi jednotlivými zdravotními zařízeními přišel (Seto et al. 2000), který si tuto techniku nechal později také patentovat. Jedná se o myšlenku centrální elektronické kartotéky pacienta, kam budou vkládány veškeré zdravotní údaje. Tato evidence se měla nacházet v jednotlivých zdravotnických zařízeních rozdělená dle trvalého bydliště pacienta a v případě, že se pacient dostavil do jiného zdravotnického zařízení, měla být tato data přenesena do daného zdravotního zařízení a po ukončení léčby případné změny v záznamech promítnuty zpět do původní lokality pacienta. Na tuto myšlenku dále navazuje publikace (Seto et al. 2000) představující konkrétní implementaci v podobě lokální webové aplikace a značkovacího jazyka XML použitého pro výměnu informací mezi serverem a klientskými aplikacemi. Publikace (Lu a Liu 2011) shrnuje možnosti využití senzorů připojených do IoT k monitoringu základních vitálních funkcí pacientů,

případně jako nástroj umožňující rozvoj telemedicíny a poskytující přehled veškerých záznamů pacienta na jenom místě.

Publikace (Xu et al. 2014) dále přináší způsob v označování jednotlivých senzorů sémantickými značkami pro jejich snazší identifikaci. Jedná se však pouze o studie bez konkrétní implementace.

(Rathore et al. 2016) představuje cloudovou platformu pro vyhodnocení dat z nositelných senzorů. Sběr a odesílání dat probíhá opět prostřednictvím mobilního telefonu. Data jsou odesílána do centrálního uložště, kde jsou v pravidelných intervalech vyhodnocována. Konkrétní metodika však opět v práci chybí. Autor pouze popisuje použití nástroje Hadoop a technik Map Reduce pro agregace dat a využití technik strojového učení a soft computing při jejich vyhodnocování.

Autor (Elhoseny et al. 2018) se zabývá způsobem šifrovaného přenosu dat mezi jednotlivými zdravotnickými zařízeními, konkrétně hybridním šifrováním obrazových medicínských dat pro zajištění bezpečnosti přenášených dat prostřednictvím IoT zařízení. Tato data pocházela z rozdílných zdravotnických zařízení například z přístrojů fungujících na principu vyzařování rentgenového záření (RTG) případně CT (Computed tomography), ale také dalších přístrojů využívajících rozdílných způsobů snímání jako je UZV, nebo snímků pořízených za pomoci magnetické rezonance (MRE - Magnetic Resonance Enterography). K dosažení cíle autor kombinuje prvky steganografie a šifrovacích algoritmů s cílem zvýšit bezpečnost přenášených informací kombinací steganografických a hybridních šifrovacích schémat. Princip šifrování spočívá v rozdělení přenášeného obrazu na sudou a lichou složku, které jsou před přenosem do vzdálené lokality rozděleny na sudou a lichou složku a každá ze složek je následně v šifrována s využitím rozdílného algoritmu a různé sady šifrovacích klíčů. V tomto konkrétním případě autor použil šifry AES a RSA.

Výsledky měření mohou být dále automaticky vyhodnocovány pomocí neuronových sítí jako v případě (Yan et al. 2006; Tuli et al. 2020) kdy jsou data o HR a HRV analyzována a následně použita pro predikci onemocnění. Podobné systémy jsou rovněž s úspěchem využívány pro predikce virových onemocnění. Příkladem mohou být studie využívající data z chytrých náramků Fitbit k predikci šíření virových onemocnění. Studie (Radin et al. 2020) se zabývá predikcí šíření virové nákazy na území USA v době chřipkových

epidemií. K tomu využívá data z 50 000 náramků Fitbit, která jednotliví uživatelé sdílí spolu s přibližnou polohou zařízení. Jako vstupní data pro výpočet slouží hodnota klidové tepové frekvence (Resting Heart Rate – RHR), která je poskytována přímo ze serverů společnosti Fitbit prostřednictvím vlastního REST API. Studie využívá pozitivní korelace mezi onemocněním a rostoucí RHR. Podobná studie založená na této myšlence byla představena jako nástroj pro identifikaci šíření nákazy COVID-19 v jednotlivých regionech Německa (Hegemann 2020). Do studie se může zapojit každý s vlastním nositelným fitness zařízením Fitbit, Withings nebo chytrými hodinkami Apple Watch.

5.2.4 Smart fitness zařízení pro sběr vitálních dat

Mezi nejznámější systémy pro sběr vitálních dat patří nejrůznější smart fitness náramky měřící denní aktivitu. Mezi nejrozšířenější řešení patří výrobky značek Fitbit, Xiaomi, Apple, Polar, Garmin a případně celá řada dalších společností. Veškerá tato řešení mají obdobný způsob snímání dat a odlišují se především v množství nabízených funkcí a případném způsobu poskytování naměřených dat, proto budou v práci posuzována jako celek a budou pouze zdůrazněny případné odlišnosti jednotlivých řešení. Jednotlivá zařízení monitorují množství funkcí jako počet kroků za den, nebo rozpoznání různých typů aktivity. Snímání těchto veličin je u převážné většiny zařízení založeno na technologii GCG popsané v kapitole 4.3.2. Některá zařízení obsahují další optické senzory pro měření srdečního rytmu, případně krevního tlaku využívající PPG senzoru. Z nasbíraných dat lze následně na základě kalorických tabulek dopočítávat množství spálených kalorií, absolvovanou vzdálenost, případně rozpoznání pohybové aktivity, nebo délku a kvalitu spánku. Způsob výpočtů i umístění výpočtů jednotlivých algoritmů se může u jednotlivých zařízení lišit, ale obecně lze říci, že jednodušší algoritmy jako detekce aktivity, překonaná vzdálenost a množství kalorií bývají umístěny přímo v hodinkách a ostatní výpočty jsou prováděny prostřednictvím aplikace na mobilním telefonu, nebo prostřednictvím cloudu vždy až po dokončení synchronizace dat ze zařízení. Synchronizace s hodinkami probíhá bezdrátově prostřednictvím technologie bluetooth, je iniciována vždy z mobilního zařízení a je prováděna manuálně uživatelem, případně může být vnucena automaticky v pravidelných intervalech prostřednictvím mobilní aplikace běžící na pozadí. Synchronizace dat trvá od několika desítek vteřin

až po jednotky minut, v závislosti na množství přenášených dat. Získané hodnoty se vyhodnocují v mobilním zařízení, kde mohou být výpočty obohaceny o další údaje například o fyzické skladbě jedince. Nejčastěji jsou to údaje o váze, věku, nebo výšce používané pro výpočet spálených kalorií, výpočet klidové tepové frekvence (resting heart rate) případně pro určení délky jednotlivých kroků používaných při výpočtu vzdálenosti.

Výsledná data jsou následně odesílána cloudovým službám, odkud jsou dostupné výsledky zobrazovány uživateli formou grafů a pravidelných reportů. Zde se funkce jednotlivých systémů příliš neliší a drobné rozdíly můžeme spatřovat převážně v množství poskytovaných funkcí a možnostech nastavení parametrů pro vyhodnocení, případně možnostech zasílání notifikací a sdílení dat.

V čem se však jednotlivé služby výrazně liší je způsob poskytování dat pro účely výzkumu, vývojářům a aplikacím třetích stran. Některé služby, jako například Xiaomi, jakékoliv sdílení dat ze zařízení zásadně odmítají a neposkytují žádná data ze svých Smart zařízení. Jiné služby (Google, Fitbit, Polar, Garmin a celá řada dalších) využívají vlastní komunikační platformu, nejčastěji prostřednictvím REST API, kde jsou jednotlivé výsledky a agregovaná data poskytovány ve formátu JSON, nebo XML. Mezi jednotlivými službami však můžeme nalézt velké rozdíly nejen v množství poskytovaných informací, ale především v jejich formě, kde si každý výrobce zařízení sám definuje strukturu obsahu zpráv i formu poskytovaných informací a je tak prakticky nemožné integrovat několik rozdílných zařízení do jednoho systému, případně hromadně analyzovat tato data bez ohledu na zařízení ze kterého pocházejí.

Poslední skupinou zařízení jsou zařízení umožňující komunikaci s libovolnou mobilní aplikací na základě výrobcem vydaného SDK, nebo za použití univerzálního protokolu Bluetooth GATT (Generic Attribute profile). Podrobná specifikace protokolu je dostupná z (Bluetooth SIG 2020). Ve zkratce se jedná o specifikaci komunikačního protokolu definující, jakým způsobem mohou komunikovat zařízení na platformě BLE (Bluetooth Low Energy) a vzájemně sdílet data. Komunikaci se zařízením tak lze navázat z libovolné aplikace implementující dané SDK, nebo podporující tento univerzální protokol. Jednou z takových platform je například Google Fit, umožňující komunikaci se zařízeními na platformě Android Wear, ale také s produkty značky Apple, případně dalšími

kompatibilními zařízeními. Kompletní seznam podporovaných zařízení lze nalézt na stránkách výrobce.

Jedná se tak o způsob, jakým lze integrovat rozdílná zařízení do jednoho systému, ovšem nedílným předpokladem pro tuto integraci je již zmíněné zajištění podpory komunikačního protokolu GATT výrobcem samotného zařízení. Výsledná data lze v případě vlastní aplikace odesílat na vlastní cloudovou službu, případně pouze ukládat do mobilního zařízení. Google Fit pak data vystavuje přes vlastní REST API rozhraní.

Samotná integrace protokolu GATT je jedním z předpokladů pro integraci různých zařízení, avšak tento komunikační standard sám o sobě nijak nezaručuje možnost ekvivalentního zpracování dat z rozdílných senzorů, nebo zařízení. Interval zasílání informací mohou být například libovolně konfigurovány podle potřeb konkrétní aplikace nebo způsobu použití. Tyto intervaly mohou mít podobu intervalů s pevně definovanou délkou (například každých 5 sekund) nebo může být frekvence zasílaných informací dynamicky měněna v závislosti na podmínkách, nebo povaze zasílaných dat jako například změny stavu senzoru, nebo změna naměřené hodnoty. Některé senzory rovněž mohou interpretovat změnu hodnoty v její absolutní hodnotě, zatímco jiní výrobci mohou využívat relativní odchylku vzhledem k předchozí naměřené hodnotě například za účelem snížení množství přenášených informací nebo zjednodušení interpretace dat pro uživatele.

Aby mohla být data z různých senzorů zpracovávána jednotným způsobem, je nutné před samotným zpracováním zajistit jednotnou interpretaci dat například jejich normalizací. Příkladem může být prosté převedení veličin na stejné jednotky nebo průměrování případně interpolace dat v čase tak aby byla zajištěna stejná frekvence vzorků dat. Těmto technikám normalizace dat se podrobně věnuje například (Padmaja a Marutheswar 2018).

6 Edge computing

Edge computing představuje distribuovaný výpočetní model umožňující zpracování dat a provádění všech nezbytných výpočetních úkonů s důrazem na lokalitu zdroje těchto dat tak aby byly veškeré výpočty a agregace prováděny co nejbližší k místu, kde byla data vytvořena nebo spotřebována, tedy na okraji sítě (tzv. edge). Model EC je navržen tak, aby řešil určité nedostatky nezbytně spojenými s tradičními cloudovými výpočetními paradigmaty, jako jsou latence, šířka pásma, zajištění spolehlivosti spojení a ochrany dat při přenosu. Díky vysoké míře lokálního zpracování dat umožňuje provádět výpočty v reálném čase, což je klíčové pro aplikace v oblastech průmyslové automatizace, řízení autonomních vozidel, nebo právě zdravotní péče. Tento přístup umožňuje využívat výhody cloudových služeb, ale zároveň minimalizuje některé jejich nedostatky tím, že kombinuje distribuované i lokální zpracování dat díky čemuž lze dosáhnout vyšší propustnosti, robustnosti, případně škálovatelnosti navrženého systému (Shi et al. 2016a; Wang et al. 2020). Publikace (Grover a Garimella 2019) navíc zmiňuje právě zdravotnická zařízení jako optimálního kandidáta pro zavádění Edge computingu pro jejich vysoké požadavky na nízkou latenci, zajištění kvality služeb (QoS - Quality of service), nebo snadnou škálovatelnost zdrojů dle aktuální potřeby.

6.1 Edge computing – Vymezení základních pojmů

V minulosti jsme byli několikrát svědky toho, jak docházelo ke změnám v oblasti zpracování dat od striktně lokální firemní infrastruktury spoléhající na uzavřené systémy uvnitř organizací, až po vyspělá cloudová řešení, kde mohou být datové i výpočetní zdroje přidělovány dle aktuální potřeby uživatele, nebo umístěny v různých geograficky vzdálených lokalitách za účelem jejich replikace, nebo zajištění optimální dostupnosti. Ne vždy je však nezbytně nutné, nebo žádoucí přenášet veškerá data do cloudu. Důvody přitom mohou být různé, od legislativních požadavků na ochranu osobních dat, požadavky na rychlost zpracování, snaha o minimalizaci nákladů za cloudovou infrastrukturu a internetové připojení, nebo zvýšení dostupnosti. Takovou alternativu poskytuje právě edge computing, který je určen pro systémy produkující velké množství dat a jejich zpracování přímo v místě jejich vzniku s ohledem na minimální odezvu.

Následující sekce definuje základní pojmy edge a fog computingu, uvede příklady jejího využití a nastíní možnosti využití edge computingu coby alternativu k tradiční metodě cloud computing.

Edge computing je přístup ve zpracování distribuovaných výpočtů spočívající v decentralizaci výpočetních uzlů na okraj sítě (to the Edge) tak aby byly situovány co nejblíže koncovým zařízením. (Singh 2019) definuje Edge computing jako službu pro maximální využití stávajících cloudových služeb tak že, data jsou zpracovávána již na samotném okraji sítě poblíž zdroje těchto dat. Na rozdíl od cloud computingu tak přináší výpočetní výkon a úložnou kapacitu blíže k místu, kde jsou tato data produkována, to znamená tam, kde je skutečně potřeba. Umístěním klíčových služeb již na samém okraji sítě má výhodu nejen ve snížení objemu dat přenášených do centrálního cloudu, ale také minimální latenci způsobenou jejich přenosem, a s tím spojenou rychlejší reakci na události a v neposlední řadě je to rovněž výrazně nižší režie samotného cloudu.

Ruku v ruce s technologií edge computing jde rovněž také technologie fog computingu. Jedná se v podstatě o rozšíření edge computingu o novou vrstvu, která se stará o výměnu a agregaci dat z jednotlivých edge nodů na vyšší úrovni, například na úrovni poskytovatele internetu a jejím účelem je další redukce přenášeného objemu dat směrem do Internetu, případně další snižování latence při komunikaci mimo edge lokalitu. Tato technologie bude rovněž podrobně představena v následující kapitole.

V dostupné literatuře lze najít celou řadu definic pojmu edge computing. Namátkou byli vybrány následující tři:

Edge computing encompasses the generation, collection, and analysis of data where the data is generated.

(Sanders 2020)

„Edge, it’s anything that’s not a “data center cloud.“

(Reznik 2018)

Edge computing is part of a distributed computing topology where information processing is located close to the edge, where things and people produce or consume that information.

(Gartner, Inc. 2019).

Důvodem k zavádění edge computingu je masivní rozvoj IoT technologií v posledních letech. Ta umožnila připojení stovek milionů malých a často jednoúčelových zařízení do internetu věcí a jejich sdílení s ostatními zařízeními ať už v rámci jedné domácnosti, nebo kdekoli po světě skrze cloudovou službu (Ashton 2009). Původní vize IoT směřovala k tomu, že každé zařízení bude mít svou vlastní IP adresu, ze které bude možné získávat aktuální data. Tato představa se však záhy ukázala jako mylná, nejčastěji z důvodu příliš vysoké energetické náročnosti. Většina zařízení tak komunikuje s internetem prostřednictvím speciální brány, která zprostředkovává veškerou komunikaci mezi jednotlivými zařízeními a cloudem. Veškerá data jsou pak veřejným internetem odesílána do cloudu výrobce, kde jsou vyhodnocena a výsledek je následně odesílán zpět do daného zařízení, což může mít za následek vykonání určité předem definované akce.

Příkladem takového zpracování může být například hlasový asistent (Google home), který poslouchá veškerou komunikaci a zazní-li klíčové slovo, začne danou konverzaci nahrávat. Tuto nahrávku posléze odešle ke zpracování do cloudu, odkud obdrží patřičné instrukce a následně vykoná definovanou akci.

S rostoucím počtem těchto zařízení navíc rostou přirozeně rovněž nároky na cloudové služby, na což upozorňují například (Kaisler et al. 2013; Katal et al. 2013). Tento způsob zpracování dat se tak z dlouhodobého hlediska stává neudržitelným (Big Data problém). Na vině jsou nejen omezené výpočetní prostředky cloudových služeb, ale také způsob, jakým takto rozsáhlé množství dat ukládat, stejně tak i chybějící infrastruktura, která by takové množství dat dokázala vůbec přenést. Ne v každé situaci je navíc možné či žádoucí přenášet objemná, nebo soukromá data do internetu pouze za účelem jejich vyhodnocení. A právě v těchto případech je mnohem výhodnější využít edge computingu.

6.2 Fog computing

Pojmy edge computing a fog computing spolu velice úzce souvisí. Přesná definice fog computing však není zcela jasně vymezena. Napříč odbornou literaturou tak můžeme najít celou řadu nejrůznějších definic. Níže jsou uvedeny některé definice z vybraných zdrojů:

“In essence, fog is the standard, and edge is the concept.” This means that the fog “defines how edge computing should work,”

(Alvarez 2019)

„A fog environment places intelligence at the local area network (LAN) and edge computing places intelligence and processing power in devices such as embedded automation controllers.“

(WINSYSTEMS Inc. Company 2017)

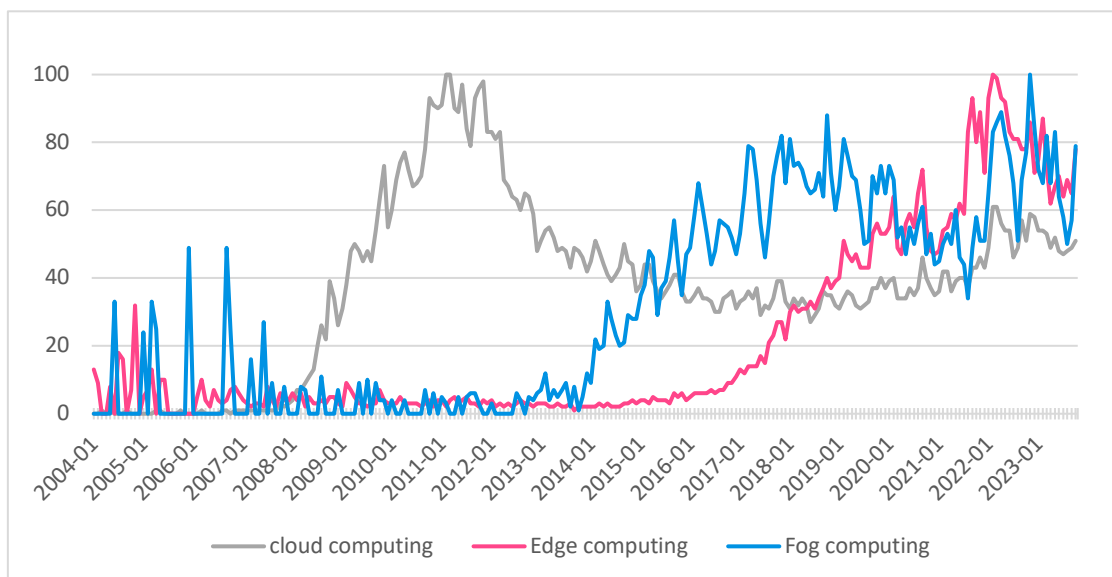
„Fog computing is a horizontal, physical or virtual resource paradigm that resides between smart end-devices and traditional cloud computing or data center.“

(Chan 2017)

V obecné literatuře se rovněž objevují názory, že pojmy fog computing a edge computing jsou vlastně to samé. Do jisté míry je to pravda. Oba pojmy se prolínají a mají stejnou funkci, ovšem pracují na rozdílných vrstvách. Zatímco fog computing přináší ideu přidat další distribuční a agregační vrstvu například na úrovni poskytovatelů internetu a optimalizovat tak distribuci a zpracování dat ze senzorů (edge nodů) do sběrných míst, čímž lze snížit jejich latenci, edge computing se primárně zaměřuje na poskytování výpočtů se zaměřením na danou lokalitu. Existují však i další varianty přístupů založené na principech distribuovaných systémů, peer to peer sítí, případně blockchain. Namátkou mohou uvedeny některé projekty zabývající se danou problematikou (Stanciu 2017; Liu et al. 2018; Xiong et al. 2018; Chen et al. 2018a; 2018a; Casado-Vara et al. 2018).

O rostoucí popularitě obou technologií svědčí rovněž statistiky vyhledávání Google, kde se klíčová slova edge computing, fog computing a cloudcomputing v posledních letech těší vysoké popularitě. Vypovídajícím měřítkem o popularitě daných technologií může být rovněž přehled vyhledávání těchto termínů prostřednictvím služby Google Trends. Obrázek 1 zobrazuje statistiky vyhledávání klíčových slov edge computing, fog

computing a cloud computing. Od roku 2013 je zde patrný přetrvávající zájem o dané technologie a můžeme rovněž předpokládat, že s pokračujícím rozvojem IoT, autonomní dopravy, Smart Cities a Průmyslu 4.0 se v následujících letech zájem o toto téma ještě více prohloubí. Naopak u cloud computingu lze oproti předchozím letům pozorovat mírný pokles zájmu veřejnosti o tuto technologii.



Obrázek 1: Přehled vyhledávání klíčových slov pomocí vyhledání Google; (autor)

6.3 Výhody EC

V předchozím odstavci byly stručně shrnuty definice edge a fog computingu spolu se základními vlastnostmi jednotlivých technologií. V následující kapitole budou tyto vlastnosti rozvedeny a podrobně představeny výhody využití edge computingu ve srovnání s cloudovými službami. Rozhodně však nelze říci, že by edge computing poskytoval univerzální a za každé situace ideální způsob nakládání s daty a vždy tak záleží na konkrétním zhodnocení navrhované aplikace, zda je Edge computing vhodným nástrojem pro dané využití, případně zda dokážou výhody EC převážit případná negativa spojená zejména s vyšší náročností implementace, vyššími nároky zejména na fyzickou bezpečnost jednotlivých prvků, případně i horší centrální správy systému. Nicméně i přes tato negativa existuje celá řada aplikací, kde je edge computing pro své vlastnosti ideální a v určitých případech dokonce jediným možným řešením, jak zpracovávat data efektivně a udržitelným způsobem. Edge computing poskytuje ve srovnání s cloud computingem následující výhody:

- **Rychlost a odezva** – Nejcitelnější a také nejčastěji zmiňovaným důvodem pro nasazení edge computngu je již zmíněná rychlost odezvy. Přiblížením výpočetních prostředků k místu vzniku dat lze minimalizovat počet přeskoků sítí nutných pro překonání vzdálenosti od producenta dat k jejich zpracování a výrazně tak snížit rychlost odezvy celého systému. Přitom právě snížením odezvy sítě lze zásadním způsobem zvýšit rychlost celého systému bez nutnosti jakéhokoliv dalšího zásahu do existující infrastruktury, nebo funkce programu. Zároveň zde také odpadá tzv. „problém poslední míle“, tedy nutnost využití méně kvalitního internetového připojení lokálních poskytovatelů internetu spojující páteřní síť s koncovými zákazníky, kde se často mísí několik rozdílných přenosových technologií, a právě tato poslední míle se zpravidla největší měrou podílí na výsledné celkové odezvě sítě. Využitím pouze lokální sítě tak lze dosáhnout odezvy v řádu mikrosekund až jednotek milisekund. V případě cloudových služeb jsou to pak desítky až stovky milisekund.
- **Bezpečnost dat** – U cloud computingu dochází k soustřeďování veškerých dat do jednoho bodu. Pomineme-li geografické rozmístění jednotlivých data center a replikaci dat mezi nimi, jsou veškerá data ze všech zařízení odesílána do jednoho prvku, čímž se tyto cíle stávají pro případného útočníka daleko lákavějšími. (Gyarmathy 2019) a (LaBrie Greg 2019) rovněž uvádějí architekturu cloud computingu jako náchylnější k případným útokům typu DDoS. Distribucí výpočetních prostředků do různých okrajových částí sítě dochází rovněž k rozprostření rizik případného útoku. Organizace si navíc sama může zvolit, případně vynutit, jakým způsobem a technologií zajistí zabezpečení svých dat (Al-Turjman 2018). V neposlední řadě je důležitý i fakt, že přenosem menšího množství dat dochází rovněž ke snížení rizika jejich zneužití při zachycení případným útočníkem, protože tato data již prošla zpracováním a každá organizace má možnost ovlivnit, jaký druh dat bude odesílán do cloudu, případně jakým technikami zajistit anonymizaci dat před jejich odesláním do cloudu.
- **Škálovatelnost** – Ačkoliv by se mohlo zdát, že škálovatelnost výpočetních zdrojů je hlavní doménou v oblasti cloud computingu, práce (LaBrie Greg 2019; Gyarmathy 2019; O'Brien 2019) ji popisují jako výhodu právě v oblasti edge computingu. Přesunutím výpočetních prostředků na okraje sítě může organizace

sama efektivně přizpůsobovat množství výpočetních prostředků jejich aktuální poptávce a v případě potřeby rychle a levně tyto prostředky rozšířit. (LaBrie Greg 2019) dále poukazuje na snazší koordinaci personálu při nasazování zařízení na okraji jedné sítě. (Shi et al. 2016b) naopak upozorňuje na některé problémy v oblasti škálovatelnosti, které mohou být spojené s rozdílným výkonem, architekturou i energetickými nároky a spolehlivostí připojení jednotlivých prvků ve srovnání s infrastrukturou datových center jako jeden z důležitých faktorů, které mohou negativně ovlivnit proces škálování výpočetních zdrojů.

- **Snížení nákladů** – Snížením množství přenášených informací do vnější sítě lze přirozeně ušetřit množství nákladů za kvalitu a šířku přenosového pásma internetové konektivity. Předzpracováním některých výpočtů mimo cloud lze rovněž ušetřit výpočetní a diskové prostředky samotné cloudové služby, což se rovněž projeví úsporou nákladů za jeho následný provoz. (LaBrie Greg 2019) popisuje edge computing jako nástroj, který si neklade za cíl zcela eliminovat cloudové služby, ale optimalizovat tok dat ve firemním prostředí tak, aby docházelo k minimalizaci provozních nákladů. (O'Brien 2019) dokonce popisuje edge computing jako nástroj pro vytváření dalšího zisku tím, že umožní rozvoj nových technologií v oblastech automatizace a autonomního řízení, kterých by za použití cloud computingu nebylo vůbec možné dosáhnout.
- **Autonomní provoz** – Výpočty a lokální řízení lze provádět i v případech kdy dojde k výpadku internetového připojení mezi lokálním systémem a cloudovou službou. V takovém případě sice nemusí být některá data zcela aktuální, ale lokální systém zůstává i nadále funkční a je schopen samostatně obsluhovat a řídit lokální zařízení.
- **Legislativní požadavky** – V silně regulovaných průmyslových odvětvích a regionech (například v Evropě, kde platí Obecné nařízení o ochraně osobních údajů GDPR) jsou velice striktně nařízeny postupy při nakládání s osobními údaji a jejich zpracování, včetně specifikace místa a způsobu jejich ukládání i možnosti jejich přenosu na vzdálená místa, čímž se jen zvyšuje potřeba lokálních datových center pro ukládání těchto citlivých dat (APC 2016).

6.4 Příklady využití Edge Computingu

Následující kapitoly shrnují možnosti využití edge computingu, jeho výhody ale i možná rizika a překážky spojené s jeho zavedením. Tato kapitola si neklade za cíl detailně představit každé řešení, pouze identifikovat klíčové oblasti využití EC a přínosy pro jednotlivá odvětví, stejně tak i budoucí vývoj a vize EC v následujících letech. Speciální sekce je pak věnována možnostem využití edge computingu ve zdravotnictví.

Tabulka 1: Seznam odvětví s potenciálem využití EC

Průmysl	(Sittón-Candanedo et al. 2020), (Liu et al. 2017)
Obchod	(Hu et al. 2018), (Chen et al. 2018a)
IoT	(Sittón-Candanedo et al. 2019), (Liu et al. 2019), (Xu et al. 2019), (Ai et al. 2018), (Bonomi et al. 2012)
Smart Cities	(Sittón-Candanedo et al. 2019), (Kanwal et al. 2019), (Khan et al. 2019), (Din et al. 2017), (Shi et al. 2016b)
Autonomní doprava	(Liu et al. 2018), (Liu et al. 2017), (Datta et al. 2016), (Bonomi et al. 2012), (Bonomi 2011)
Zdravotnictví	(Tuli et al. 2020), (Djelouat et al. 2020), (Han et al. 2019) (Felter 2019), (Tynan 2019), (Abdel-Basset et al. 2019), (Conboy 2019), (Namee et al. 2019), (Keary 2018), (Dubey et al. 2017), (Howbert et al. 2014), (Seto et al. 2000),
Vize EC	(Khan et al. 2019), (Zhang et al. 2019), (Loven et al. 2019), (Xiong et al. 2018), (Shi et al. 2016b), (Varghese et al. 2016)

6.4.1 Edge computing ve zdravotnictví

Následující sekce je zaměřena na potenciální využití edge computingu ve zdravotnictví a veterinární péči. Budou zde představeny jednotlivé potenciály technologie Edge computingu v oblastech veterinárního zdravotnictví a její konkrétní přínosy pro organizace, nebo zdravotní personál. Z důvodu nedostatku relevantních zdrojů

z problematiky využití edge computingu ve veterinární péči, však byly v následující kapitole rovněž zohledněny i některé materiály a studie zahrnující klasické humánní zdravotnictví medicíny zabývající se zlepšením zdravotní péče u lidí.

Články (Conboy 2019; Tynan 2019) popisují využití edge computingu ve zdravotnictví jakožto nástroj, který umožní rapidní rozvoj IoT technologií ve zdravotním sektoru. Autor (Tynan 2019) dále vyzdvihuje přínosy EC, jakými jsou nižší nároky na personál při provádění rutinních prohlídek a dohledem nad pacienty, stejně tak nižší administrativa spojená se správou dat o pacientech nebo automatizaci některých základních rutinních úloh. Druhou nespornou výhodou Edge computingu je zvýšení úrovně zdravotní péče v odlehlých oblastech bez kvalitního internetového připojení. (Conboy 2019; Tynan 2019) zdůrazňují, že použitím přístrojů s okamžitou možností analýzy dat bez nutnosti použití internetového připojení přispěje ke zrychlení a zkvalitnění poskytované péče, ať už v menších obcích, nebo přímo v terénu prostřednictvím mobilních ambulantních pracovišť.

Dle (Tynan 2019) přispěje využití edge computingu k rozvoji vědy tím, že přinese jednotnou formu ve struktuře dat, čímž umožní aplikovat zcela nové přístupy v procesu získávání skrytých informací v datech, např. metodami strojového učení, nebo pomocí technik data mining. (Tynan 2019) rovněž poukazuje na to, že jednotlivá zdravotní zařízení často provozují stovky různých systémů generující obrovské množství dat ve zcela rozdílných formátech. K roztržičnosti jednotlivých informací přispívá rovněž fakt, že různí lékaři často používají rozdílné způsoby pro označování dat a mohou tak vznikat komplikace při jejich pozdějším slučování a zpracování.

Edge computing může rovněž pomoci při léčbě chronicky a dlouhodobě nemocných pacientů. (Felter 2019) uvádí, že poskytnutí malých přenosných zařízení pacientům umožní jejich nepřetržitý zdravotní dohled. Lze tak prodloužit intervaly mezi pravidelnými zdravotními prohlídkami a zároveň poskytnout lékaři lepší přehled o celkovém zdravotním stavu pacienta. Systém rovněž může na základě naměřených dat s pacientem interagovat, například doporučeními v závislosti na aktuálních podmínkách prostředí, nebo aktuálním zdravotním stavu pacienta, čímž lze nepochybně přispět k eliminaci nepříznivých vlivů, a naopak ke zlepšení jeho dlouhodobého zdravotního stavu. Zároveň systém může sám upozornit lékaře v případech, kdy se zdravotní stav

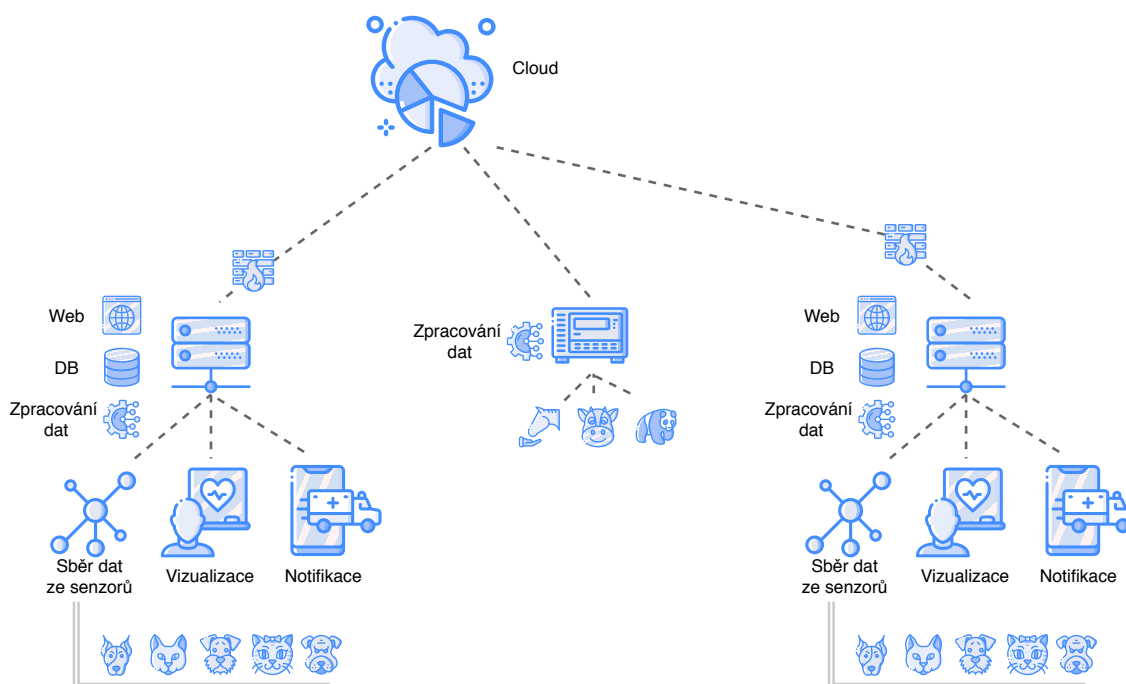
pacienta výrazně zhorší. Lékaři tak mohou díky dostupnosti aktuálních i historických dat tuto informaci snadno ověřit a posoudit možná rizika a odhadnou případný budoucí vývoj zdravotního stavu pacienta a včas učinit patřičná protipatření. Edge computing rovněž může pomoci při dohledu nad pacientem v režimu intenzivního dohledu, tedy tam, kde je požadována okamžitá reakce systému na událost a není čas na odesílání dat do cloudu k jejich zpracování. Jako příklad takového zařízení uvádí (Tynan 2019) přístroj pro monitoring hladiny inzulínu v těle, zařízení pro včasnou detekci a predikci epileptických záchvatů (Strong et al. 1999), (Howbert et al. 2014), (Sec et al. 2018b), případně přístroje pro měření poruchy dýchání, nebo neurologické a srdeční aktivity. V neposlední řadě se může jednat o přenos aktuálního obrazu životních funkcí při přepravě pacienta do nemocnice, kdy lze rovněž veškerá data zpracovat již na palubě vozidla a na centrální stanoviště přenášet pouze výsledné hodnoty čímž lze ušetřit velkou část přenosové kapacity. To je opět neocenitelné v oblastech s nekvalitním internetovým připojením, jako jsou odlehlé komunikace, nebo lesy, kde tato vozidla často zasahují. V případě domácích a hospodářských zvířat pak mohou podobné přístroje přispět k monitorování nemocných, nebo čerstvě narozených zvířat bez nutnosti jejich transportu do veterinárních zařízení a jejich vystavení dodatečnému stresu způsobeným jejich převozem.

Součástí práce je rovněž samostatná sekce věnovaná dlouhodobému monitoringu psů postižených epilepsií s představením návrhu a využitím v práci představné platformy pro dlouhodobý sběr, automatické vyhodnocení a zpřístupnění dat pro zdravotní personál pro dlouhodobý monitoring a predikci jednotlivých záchvatů u psů.

7 Představení systému

Na základě požadavků na systém uvedených v sekci 5.1 byly definovány základní požadavky na systém a představena architektura systému. Stručný náhled na strukturu systému poskytuje Obrázek 2. Jedná se však pouze o základní dělení systému do jednotlivých vrstev a identifikaci jednotlivých funkčních celků. V této sekci tak nebudou uvedeny konkrétní způsoby implementace ani technologie použité pro vývoj systému, ale pouze představení jednotlivých modulů systému spolu s vysvětlením jejich funkce, souborem dat, se kterými daná vrstva disponuje a případné návaznosti modulu na ostatní komponenty v systému s cílem představit architekturu a princip fungování systému jako celku.

Konkrétní způsob implementace, stejně tak použité technologie a zdůvodnění jejich použití je následně uveden v samostatné Kapitole 8 věnované právě návrhu systému.



Obrázek 2: Návrh systému; (autor)

Navržený systém je rozdělen do tří základních vrstev. Nejnižší senzorní vrstva senzorů se stará o získávání naměřených dat, obsluhu jednotlivých měřících senzorů a zaslání těchto dat vyšším vrstvám systému k jejich vyhodnocení a zpracování. Tato vrstva zahrnuje samotné senzory pro detekci dechové a tepové frekvence zvířat, monitoring

pohybu, a aktuální váhy zvířete. Výsledkem měření této vrstvy je digitální signál o konstantní frekvenci, který je bez jakéhokoliv dalšího zpracování odeslán do střední edge vrstvy. Stručný popis, jakým lze jednotlivá sensorická data vyhodnocovat je uveden v následujících sekcích. Samotná sensorická zařízení pro měření veličin však nejsou dílem autora této práce a nebudou tedy detailně popisována. Původní naměřená data jsou odesílána do vyšších vrstev systému, kde dochází k jejich zpracování.

Ve druhé edge vrstvě jsou tyto původní naměřené hodnoty obohaceny o metadata obsahující nezbytné informace o druhu monitorovaného zvířete a v případě některých algoritmů rovněž o data z dalších sensorů, která jsou následně jsou následně zpracována. Výsledkem je soubor hodnot vypovídající o aktuální zdravotním stavu zvířete, na něž je možné reagovat například při překročení hranice některé z definovaných hodnot. Tato reakce na událost může spočívat ve zobrazení varování na monitoru obsluhujícímu personálu, zaslání zprávy na telefon zdravotníka, nebo majitele zvířete, případně vykonání jiné předem definované akce zasláním příkazu nižší vrstvě. Architektura systému předpokládá umístění vždy nejméně jednoho výpočetního nodu (uzlu) do každé veterinární ordinace. Účelem této vrstvy je poskytnout kompletní řízení a obsluhu sensorů připojených do této lokální sítě a umožnit tak jejich plnohodnotnou správu i v případě úplného výpadku internetového připojení. V takovém případě sice nebude možné získávat veškeré informace z okolních systémů nebo jiných veterinárních pracovišť, ani monitorovat systémy umístěné v domácnostech například u dlouhodobě, nebo chronicky nemocných zvířat, ale lokální funkce systému zůstane vždy plně zachována. I přes absenci internetového připojení budou systémy pro vyhodnocování vitálních dat a dohledového centra i veškeré notifikace nadále plně funkční. Přerušování spojení s vyššími vrstvami systému tak neohrozí zdravotní stav hospitalizovaných zvířat. Umístěním vyhodnocovacího modulu na úroveň jednotlivých zdravotních zařízení se zároveň projeví veškeré výše popsané výhody edge computingu, jakými jsou výrazně rychlejší odezva systému, úspora přenosového pásma a v neposlední řadě při dodržení požadavků na zabezpečení a pravidelné zálohy systému i vyšší bezpečnost dat.

Jednotlivá hardwarová podoba i funkce výpočetních edge nodů se může lišit v závislosti na požadavcích ale i na počtu zpracovávaných sensorů. Například pro menší veterinární zařízení lze využít malé osobní počítače, nebo mini PC s připojeným monitorem a dohledovou aplikací, Velké veterinární zařízení mohou naopak využít pro zpracování

dat servery umístěné ve vnitřní síti organizace a pro následnou obsluhu systému a vizualizaci dat pak použít běžné pracovní stanice obsluhujícího personálu. Pro domácí použití lze pak zcela odstranit některé moduly jako je notifikace a vizualizace dat a přenechat tak jejich správu plně na zdravotním personálu. Omezením některých funkcí u jednotlivých edge nodů lze rovněž uspořit výpočetní i hardwarové nároky a výsledná zařízení obsluhující jen několik senzorů tak mohou získat podobu malých krabiček typu Raspberry Pi, nebo hardwarově podobných zařízení. Výhodou pro uživatele je velice snadná instalace, ale i příznivé náklady za jejich následný provoz.

Veškerá naměřená data mohou být ukládána do lokální databáze. Množství dat i jejich podoba se může značně lišit v závislosti na funkci jednotlivého nodu. Data jsou následně odesílána do cloudové aplikace, odkud může zdravotní personál získávat a zpracovávat dlouhodobá data z různých míst systému.

Cílem cloudové aplikace je tedy dlouhodobý sběr a zpracování dat o vitálních funkcích zvířat a umožnit tak propojení dat jednotlivých veterinárních zařízení připojených do tohoto systému při zachování výhod spojenými s využitím cloud computingu jako je vysoká flexibilita, škálovatelnost, nebo rozložení zátěže mezi lokalitami (Varghese et al. 2016). Funkcí cloudové aplikace je tak dlouhodobé shromažďování dat za účelem jejich přístupu z libovolného zdravotního zařízení, případně jejich pozdějšího zpracování za účelem tvorby dlouhodobých analýz. Sémantickým propojením dat z rozdílných senzorů tak vznikne unikátní databáze dat umožňující využití širokého spektra analytických a statistických funkcí jako jsou data mining, strojové učení, umělá inteligence, nebo neuronové sítě. Zároveň umožní tyto výsledky později zpětně aplikovat v oblasti navazujícího vývoje a možnostech dalšího zpracování senzorických dat.

Největší výhodou navrženého řešení je poskytování služeb i v případě, kdy jsou jednotlivé nody v offline stavu bez spojení s cloudovou částí systému. Tuto možnost zatím nenabízí žádné z představených řešení, dokonce ani v oblasti chytrých nositelných zařízení, kde by stačilo vyřešit uložení a vyhodnocení dat na lokální úrovni. Použitím techniky edge computingu tak může zpracování dat probíhat čistě na lokální úrovni. Využití edge computingu rovněž umožnilo takřka v reálném čase vyhodnocovat velké množství původních dat v řádech několika stovek záznamů za sekundu z jednoho senzoru bez vysokých nároků na cloudovou službu a s minimální latencí. Veškeré jmenované

konkurenční systémy pro zpracování vitálních funkcí spoléhají výhradně na cloudovou architekturu a pracují s řádově nižšími objemy dat. Unikátní je rovněž systém automatického vyhodnocení rizikových situací, který může probíhat nepřetržitě a takřka v reálném čase, nikoliv pouze v pravidelných intervalech v řádu několika desítek minut po předchozí synchronizaci dat jako je tomu u výše představených systémů. Velkým přínosem pro lékaře je rovněž možnost přizpůsobit výpočet přesně na míru konkrétnímu zvířeti, stejně tak možnosti nastavení notifikací podle jejich závažnosti. Některé ze služeb poskytují zpracovaná data pro použití aplikacemi třetích stran. Za tímto účelem společnosti vystavují data prostřednictvím REST API. Struktura správ ale i způsob komunikace se však u jednotlivých systémů poměrně liší. Nově navržený systém vystavuje data prostřednictvím standardizovaných open schémat a umožňuje je tak snadněji propojit s dalšími systémy, nebo využít pro hromadné zpracování. Zabezpečení a komprese veškeré komunikace pak tvoří spíše standard pro zajištění bezpečnosti a spoléhá na tradiční dostupné způsoby a techniky zabezpečení dat. I přes mnohé výhody přináší navržená architektura také některé výzvy v oblastech komunikace a správy systému, které jsou představeny v následující kapitole.

7.1 Technické výzvy v implementaci systému

V předchozí kapitole byla stručně představena struktura systému a popis funkcí jednotlivých vrstev systému. Následující kapitola uvede technické výzvy zejména z oblastí IoT, edge computing a zabezpečení dat, kterým je nutné při následném vývoji systému čelit.

7.1.1 Komunikace

Nejčastější výzvou v oblasti sběru dat z IoT je integrace několika rozdílných technologií a definování jednotného způsobu komunikace tak, aby spolu mohly jednotlivé části systému komunikovat. Zároveň je nutné komunikaci definovat dostatečně univerzálně tak, aby v budoucnu umožnila integraci nových systémů a senzorů.

Největším problémem je komunikace s koncovými senzory na samotném okraji sítě. Důvodem je, že v IoT existuje nepřehledná škála rozdílných implementací, komunikačních technologií a protokolů jednotlivých koncových zařízení. Toto je naprosto v pořádku, protože každá z technologií je navržena pro jiný způsob komunikace a uzpůsobená právě

k tomuto druhu přenosu s ohledem na množství dostupných zdrojů, množství a četnost přenášených informací a energetickou náročnost přenosu. Každá z technologií je vhodná na specifický případ použití a není tak možné vytvořit univerzální komunikační technologii, která by byla ideální pro jakékoliv použití v IoT. Problém je rovněž v definici komunikačních standardů, které si často definují samotní výrobci těchto zařízení. Komunikace tak často probíhá výhradně s vlastní proprietární bránou výrobce, který integruje pouze vlastní hardwarové zařízení, a to často pouze v rámci jedné definované generace zařízení. Z hlediska integrace je tak prakticky nemožné vytvořit takový systém který by dokázal komunikovat se všemi zařízeními. K tomu by výrazně přispělo definování jednotných komunikačních standardů pro každou přenosovou technologii, ale tento úkol se zdá být v dohledné době nerealizovatelný a veškerá snaha o vytvoření jednotné implementace ze strany výrobců a soukromých menších společností by vedla jen k vytvoření dalšího proprietárního komunikačního protokolu. V praxi tak často dochází k integraci jednoho, nebo několika výrobců a standardů na úrovni lokální infrastruktury do jedné brány (edge gateway), která zároveň zprostředkovává komunikaci s okolím. Zde je však nutné vybírat obezřetně taková zařízení, která umožňují získávání dat lokálně bez použití cloudové služby. Z hlediska edge computingu je tak důležité, aby každý uzel v síti podporoval komunikaci se zařízeními na úrovni lokální sítě a zároveň integroval dostatečně univerzální protokoly pro komunikaci s vnější sítí. Vyšší možnosti integrace rovněž přispěje jednotná struktura zpráv.

7.1.2 Různorodost dat a standardizace obsahu zpráv

Spolu s komunikací systémů je spojena i různorodost obsahu produkováných zpráv. Systémy zpracovávající data z různých míst musí často čelit rozdílné struktuře obsahu v závislosti na zdroji těchto dat. V případě zpracování dat (nebo i pouze jejich slučování z různých zdrojů) je tak naprosto nezbytné správnému porozumění jejich kontextu tak aby nemohlo dojít k chybné interpretaci a zkreslení výsledků zpracování. Standardizovaný formát zpráv rovněž značně přispěje k pozdější integraci dat, bez ohledu na to, z jaké části systému data pocházejí. V případě zdravotnictví je správná sémantická struktura dat, pro svou složitost a komplexnost jednotlivých údajů ještě důležitější, na což upozorňují například i (Chen et al. 2018b; Tynan 2019).

Správné pochopení významu jednotlivých dat a rozdílnost struktury dat z různých zdrojů je tak stále zásadní překážkou při jejich klasifikaci a hromadném zpracování. Kromě struktury samotné se však může lišit i význam jednotlivých atributů uvnitř zpráv. Jako příklad lze uvést váhu, nebo teplotu zvířete, která bude uváděna v různých jednotkách napříč státy. Ale stejně tak se může jednat o časový údaj, s přihlédnutím k časovému pásmu, letnímu času atd. Veškeré tyto údaje by měli být ve schématu specifikovány a veřejně přístupné. Naštěstí je zde snaha o definování jednotného obsahu zpráv o čemž svědčí i řada databází tzv. Open Schémat jako Open mHealth (mHealth, Inc. 2011), Microsoft Common Data Model (Palmer a Owen 2020), případně další. Tyto projekty si kladou za cíl poskytnout jednotnou strukturu dat a usnadnit tak jejich zpracování, ale i přístup k těmto datům široké veřejnosti.

7.1.3 Zabezpečení – Obecné principy

Z důvodu enormní variability a roztržitosti výpočetních zdrojů se stává otázka zabezpečení jednotlivých zařízení jednou z klíčových úloh při tvorbě systému. Mnoho různých IoT zařízení se navíc v minulosti ukázalo jako nedostatečně zabezpečených a zranitelných vůči nejrůznějším útokům zneužívající zranitelnosti bezdrátových technologií ZigBee (Khanji et al. 2019), Z-Wave (Hoskins 2016; Unwala et al. 2018), LoRa (Aras et al. 2017), případně další (Andrea et al. 2015; Ling et al. 2017) k manipulaci s koncovým zařízením, nebo přímo získání přístupu útočníka do lokální sítě. Mohou tak snadno posloužit jako potenciální vstupní brána pro nejrůznější útoky.

(Kerner 2019) rozlišuje pět základních pravidel pro zabezpečení jednotlivých edge zařízení na okrajích sítě:

- **Zabezpečení okraje sítě** (*Perimeter security*) – Implementovat dostatečné zabezpečení okraje sítě a výpočetních zdrojů tak, aby nemohlo dojít k jejímu narušení vnějším útočníkem. Zde se jedná zejména o tradiční techniky řízení přístupu k jednotlivým zdrojům, jako firewally coby nástroje pro analýzu a filtrování síťové komunikace okraje sítě s jejím okolím, nebo zabezpečení přístupu do vnitřní sítě v například formou VPN tunelů. (Identity Management Institute 2019) rovněž upozorňuje na riziko, kdy jsou jednotlivá zařízení často navrhována jen s minimálním důrazem na jejich zabezpečení, kdy jsou použity

zastaralé techniky zabezpečení, případně jakákoliv ochrana zařízení a zabezpečení komunikace s ním zcela chybí (Zhang et al. 2018; Sha et al. 2019). Další možné bezpečnostní hrozby spočívají i v laxním přístupu výrobců při vydávání bezpečnostních aktualizací. Důvodem může být i levnější, méně výkonná hardwarová architektura těchto zařízení a omezené možnosti autentizace a zabezpečení přenosu, než je tomu u tradičních serverů. Jednou z dalších úloh je vyřešení otázky fyzické bezpečnosti jednotlivých zařízení ať už z hlediska jejich odcizení, neoprávněné manipulace s jednotlivými zařízeními, nebo ověření identity jednotlivých zařízení.

- **Zabezpečení aplikací** (*Application security*) – Mimo samotné síťové infrastruktury musí být bezpečné i koncové aplikace, které se starají o zpracování a uchovávání dat tak, aby nemohlo dojít k narušení interní komunikace mezi jednotlivými moduly, interními systémy, nebo zcizení citlivých dat z těchto systémů.
- **Identifikace hrozeb** (*Threat detection*) – Protože je edge computing z principu založen na decentralizaci, je tak velmi obtížné monitorovat veškerý provoz v síti z jednoho centrálního místa. (Kerner 2019) doporučuje použití systémů proaktivní bezpečnosti. Tyto systémy nepřetržitě monitorují veškerou aktivitu v síti a využívají statistickou analýzu, strojové učení, nebo neuronové sítě pro včasnou detekci jakékoliv podezřelé aktivity na hranách sítě.
- **Správa zranitelností** (*Vulnerability management*) – Má za cíl identifikovat a eliminovat slabá místa v síti organizace. Jejím úkolem je monitorovat průběh odstraňování všech nalezených zranitelností, ale také identifikovat příčinu jejich vzniku. Jednotlivé zranitelnosti jsou často hodnoceny určitým stupněm rizika, podle míry ohrožení systému a následků v případě útoku na takto zranitelné místo. Správa zranitelností rovněž obsahuje různé kontrolní, penetrační a zátěžové testy s cílem ověření funkčnosti a stability dané architektury v reálném provozu.
- **Správa aktualizací** (*Patching cycles*) – Automatická aktualizace jednotlivých zařízení a automatické aplikování bezpečnostních záplat jsou důležitou součástí pro udržení aktuálnosti systému a minimalizaci rizik případného útoku. V současné době se i v edge computingu prosazují metody kontejnerizace a orchestrace kontejnerů. Kromě dalších výhod, které tato technologie nabízí,

může využití tzv. light-weight virtualizačních technik velice usnadnit proces automatického nasazování jednotlivých aplikací, a stejně tak i jejich následnou aktualizaci, nebo vzdálenou správu.

Celkově se tak jedná o poměrně široký proces kombinující techniky detekce bezpečnostních hrozeb v kombinaci s monitoringem v reálném čase, analýzu a proaktivní bezpečnostní opatření k ochraně okrajové infrastruktury a dat zpracovávaných na okraji sítě. Avšak tento bezpečnostní obor se stále vyvíjí spolu s tím, jak edge computing čím dál více získává na významu v souvislosti s jeho postupným zaváděním v nejrůznějších průmyslových odvětvích.

7.1.4 Správa systému

Dalším zásadním krokem pro správnou funkci systému je vyřešit možnost jeho vzdálené správy. To znamená, jakým způsobem lze v budoucnu řešit nasazení nových verzí systému, jakým způsobem vzdáleně přistupovat k tomuto zařízení za účelem správy systému, případně jak provádět vzdálenou diagnostiku tohoto zařízení. Určitou možností je již zmíněná orchestrace virtuálních kontejnerů, spolu s dalšími technikami zabezpečeného přístupu, jako jsou VPN tunely. Tato metoda se velmi osvědčila v oblasti cloud computingu a umožňuje distribuovat aktuální obrazy mezi jednotlivé systémy, ale stejně tak řídit kompletní životní cyklus těchto kontejnerů a napomáhat tak při výměně jednotlivých verzí, nebo se základní diagnostikou systému. Rovněž je třeba vyřešit způsob jakým lze spravovat zařízení bez veřejné IP adresy. Zde lze proces aktualizací vyřešit například automatickým stažením a instalací aktualizací z cloudové služby, případnou správu zařízení pak již zmíněnou službou VPN. V případě přenosných zařízení je však nutné proces aktualizace uzpůsobit tak, aby nenarušoval samotnou funkci zařízení, například nestahoval aktualizace přes mobilní připojení. Zároveň se zde z důvodu absence jakéhokoliv výstupu předpokládá velice omezená, nebo vůbec žádná možnost interakce s uživatelem.

8 Návrh systému – Identifikace jednotlivých vrstev

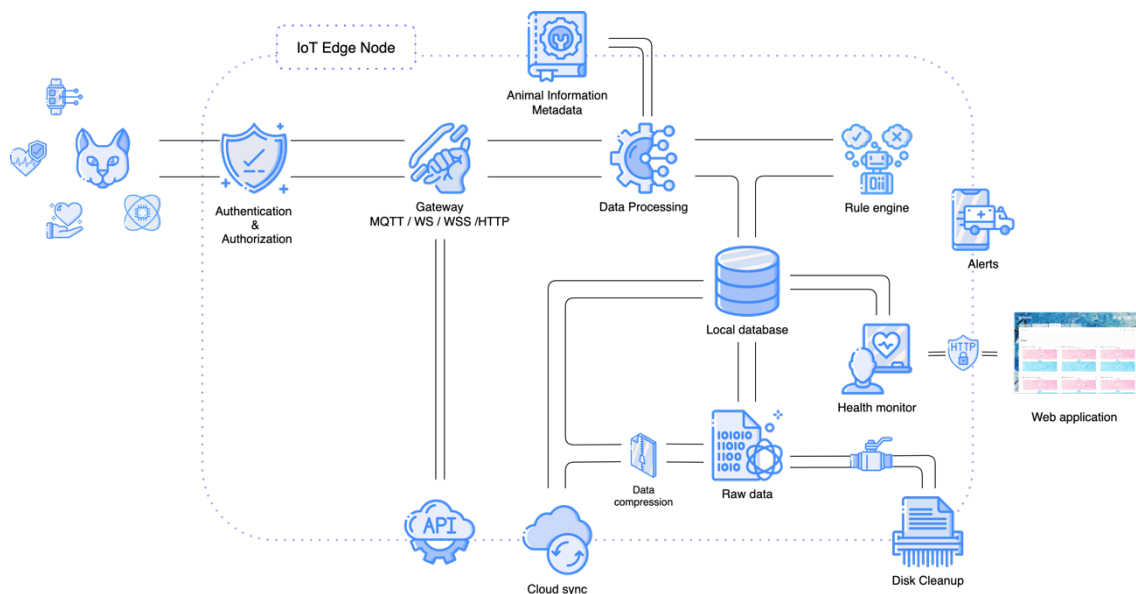
V následující kapitole bude představena funkce jednotlivých vrstev systému od nejnižší senzorické vrstvy po cloudovou aplikaci vycházející z konstrukce uvedené na Obrázek 2, která je dále rozšířena o konkrétní funkční bloky v podobě jednotlivých modulů. V každé vrstvě budou identifikovány klíčové moduly a představena jejich funkce včetně významu jednotlivých vazeb na ostatní komponenty v systému.

8.1 Senzory a Edge gateways

Jedná se o jednotlivé koncové senzory měřící základní veličiny uvnitř prostředí a případné brány (Edge gateways). Tyto brány na okraji sítě se starají o bezprostřední komunikaci s jednotlivými senzory bez ohledu na druh přenosu, použitou technologii nebo způsob komunikace. Zde lze využít buď originální hardware jednotlivých výrobců, ale i vlastní implementace, nebo libovolný hardware a software řešení třetích stran. Jedinou podmínkou pro připojení do systému je alespoň jeden z podporovaných komunikačních protokolů a komunikace brány na lokální úrovni, nikoliv výhradně s využitím cloudové služby výrobce tohoto zařízení. Výhodou je pak samozřejmě podpora zabezpečené komunikace. Účelem těchto bran je obsluhovat jednotlivé senzory, případně provádět dílčí výpočty, nebo agregace ve smyslu přepočtu výstupní hodnoty z A-D převodníku na konkrétní veličinu, nebo pravidelné vyčítání hodnot ve smyčce a zasílání pouze hodnot, které se od předchozího stavu změnilo. Tímto lze nejen ušetřit značnou část přenosového pásma, ale také snížit zátěž jednotlivých edge nodů. Jak již bylo zmíněno v kapitole 5.1, konstrukce ani obsluha jednotlivých senzorů a bran však není oborem autora práce a nebude tedy detailně popisována. Více informací lze získat z jednotlivých publikací (Stepan et al. 2017a; Sec et al. 2018c; Vojtas et al. 2018; Sec et al. 2018b; 2018a).

8.2 Edge node

Edge node tvoří nejdůležitější část každého lokálního uzlu. Veškerá komunikace s jednotlivými bránami probíhá pomocí gateways, odkud jsou po prvotním procesu párování a ověření zařízení data odesílána k jejich zpracování. **Chyba! Nenalezen zdroj odkazů.** znázorňuje výčet aktuálně používaných modulů.



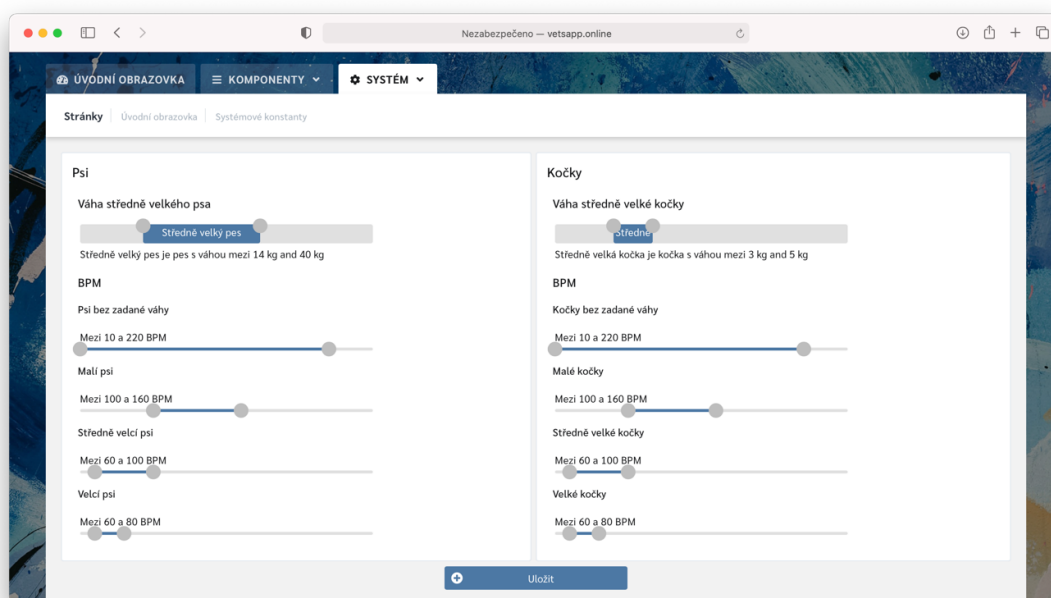
Obrázek 3: Edge node – Schéma propojení jednotlivých modulů; (autor)

Komunikace edge nodu s nižší vrstvou je obstarávána prostřednictvím jednoho z dostupných komunikačních rozhraní (gateway). Aktuálně podporované technologie jsou MQTT, Web Socket (WS) / Web Socket Secured (WSS) a HTTP /HTTPS.

Pro ověření identity jednotlivých zařízení lze použít například TLS (*Transport Layer Security*) spolu s certifikátem pro ověření identity edge nodu, ale také unikátní certifikáty pro každé jednotlivé zařízení. Tím je zaručena obousměrná identita všech zařízení, tedy to, že komunikace skutečně probíhá se správným edge nodem (nikoliv s bránou útočníka), ale zároveň také, že komunikující edge gateway je skutečně ono zařízení, které má přístup k Edge nodu a přijímaná data skutečně pochází z konkrétní gateway a poskytovaná data lze považovat za validní. Příjemným přínosem je samozřejmě i fakt, že takto navázané spojení je zároveň šifrované, a tudíž i odolné vůči vnějším odposlechům. V případě výměny nebo odcizení některého ze zařízení tak lze certifikát snadno zneplatnit a znemožnit tak útočníkovi tuto bránu použít pro komunikaci s edge. Platnost jednotlivých certifikátů však není neomezená a je rovněž třeba počítat s jejich obnovou, respektive vytvoření nového certifikátu obsahujícího nově vygenerovanou sadu privátních klíčů. Takový proces by měl proběhnout automaticky, ideálně ještě před vypršením stávající platnosti certifikátu bez zásahu uživatele. Více informací o protokolu TLS a procesu vzájemné autorizace lze získat například z (IBM Corporation 2003). Procesem výměny klíčů v IoT se následně zabývají například publikace (Rabiah et al.

2018; Ertaul et al. 2019). Z hlediska dodatečné ochrany jednotlivých zařízení je rovněž vhodné zabezpečit obsah jednotlivých zařízení před jeho zkopírováním na nové zařízení, které by se tímto mohlo prezentovat jako původní edge gateway. Tomu lze předejít například použitím dalších klíčů založených na použití HW identifikátoru zařízení, dodatečným šifrováním interního úložiště, nebo fyzickými a SW bariérami bránícími vyčítání obsahu ze zařízení.

Po přijetí a validaci vstupních dat jsou tato data odeslána do následujícího modulu k jejich zpracování. Způsob zpracování se může lišit v závislosti na použitém senzoru, ale také druhu měřeného zvířete. Jednotlivá vstupní data pak mají podobu vzorku o třech až dvanácti složkách v závislosti na použitých měřících senzorech. Pro správnou volbu výpočetního algoritmu jsou vstupní data dále obohacena o metadata specifikující konkrétní metodu snímání dat, použitou vzorkovací frekvenci, ale i informace o snímaném zvířeti, jako jeho druh velikost, nebo váha měřeného zvířete, případně i další informace o aktuální kondici zvířete definované zdravotníkem. Obrázek 4 znázorňuje ukázkou definice konstant pro jednotlivá metadata pro definované kategorie zvířat ve zdravotnické aplikaci. Tato metadata lze následně ještě manuálně upravit, nebo upřesnit na míru každému jednotlivému zvířeti.



Obrázek 4: Ukázkou definice metadat; (autor)

Samotný proces vyhodnocování je však aktuálně stále ještě v experimentální fázi a neustále probíhají procesy jeho ladění a optimalizace metodiky výpočtu dat pro jednotlivé druhy zvířat a měřících zařízení. Autor práce je rovněž pouze spoluautorem původní myšlenky a metodiky vyhodnocování dat. Jako součást návrhu systému se však postaral se o jeho implementaci v jazyce Java díky čemuž umožnil plně automatizované zpracování dat ze senzorů v reálném čase. Konkrétní metodika, stejně tak způsob výpočtu jednotlivých hodnot vychází z patentu č. 33574 a je proto důvěrná. Autor práce je tak vázán mlčenlivostí o detailním principu konstrukce i způsobech vyhodnocování dat. Z tohoto důvodu nebudou podrobně představeny všechny konkrétní podoby výpočetních algoritmů, ani poskytnuty zdrojové kódy výpočetního modulu. Nicméně základní informace o podobě zpracovávaných dat, způsobu jejich vyhodnocení a jejich množství jsou uvedeny v následujících kapitolách.

Samotný algoritmus pro vyhodnocování dat je však stále v procesu vývoje a dochází tak k jeho pravidelnému vylepšování. Ze strany spoluautorů vyhodnocovacího algoritmu tak vznikl logický požadavek na uchování veškerých vstupních dat ze senzorů v nezměněné podobě pro potřeby následného ladění a dalšího vývoje algoritmu. Tomuto požadavku byl rovněž přizpůsoben i zobrazovací řetězec umožňující drobné korekce parametrů přímo za běhu aplikace. Z tohoto důvodu jsou na každém edge nodu uchovány nejen zpracované hodnoty, ale také jejich originální vstupní data. Tento požadavek sice jde proti principům edge computingu, ale z pohledu autorů jej lze obhájit snazší dostupností jednotlivých vstupních vzorků ze všech měřících lokalit a z pohledu vývoje se rovněž jedná o dočasné řešení, které lze později z procesu zpracování jednoduše vyloučit. Z důvodu enormního množství těchto dat, které každý senzor denně vyprodukuje však bylo nutné vyřešit nejen způsob jejich uložení a způsob, jak data průběžně komprimovat a následně přenášet do cloudu, ale i efektivní způsob jakým jednotlivé edge nody od těchto surových dat automaticky čistit a eliminovat tak případný nedostatek místa pro samotné zpracování.

Zpracovaná data již mají podobu konkrétních veličin, jako je dechová a tepová frekvence zvířete, případně množství a druh pohybu vypovídající o jeho psychické a zdravotní kondici. Tyto hodnoty jsou následně ukládány do lokální databáze, ale zároveň slouží jako vstupní data pro zdravotnický monitor a pro detekci anomálií v chování zvířat.

Lokální databáze má podobu relační databáze. Relační databáze byla zvolena především z důvodu vysoké provázanosti výpočtů na ostatní data, jako jsou zdravotní záznamy, podávaná medikace, personál odpovědný za pravidelný dohled, ale i parametry pro detekci anomálií. Díky tomu lze výpočet snadno přizpůsobit na míru každému zvířeti.

Z dostupných relačních databází byla následně vybrána a integrována open source databáze PostgreSQL a to na základě dostupných srovnávacích testů, které poskytují například (2ndQuadrant 2019; DeveloperWeek 2019), ale také na základě předchozích zkušeností autora s touto databází jakožto vhodného nástroje pro uložení, vyhledávání a třídění v objemných datech, což potvrzují i mnohé implementace, například (Sultana a Dixit 2017; Vaisman et al. 2019; Netflix, Inc. 2019; Spotify Technology S.A. 2019), kde je tato databáze úspěchem využívána pro ukládání velkých objemů dat. Veškerá data mohou být šifrována na úrovni jednotlivých atributů, čímž lze chránit některé citlivé údaje před jejich zneužitím.

System pro detekci anomálií, nebo také pravidlový systém (*Rule engine*), je modul reagující na aktuální příchozí data. Jedná se o jednoduchý pravidlový systém, který vyhodnocuje nově příchozí data, vyhodnocuje trendy těchto dat a porovnává příchozí hodnoty s nastavenými prahovými hodnotami. Samotný modul však nemá žádnou vazbu na historické záznamy v databázi a uchovává si pouze poslední známou a aktuálně příchozí hodnotu.

Jednotlivé kritické hranice jsou definovány tabulkovými hodnotami obvyklých fyziologických funkcí psů a koček. Obecně lze říci, že tepová i dechová frekvence je silně závislá na velikosti zvířete. Například menší plemena psů mají zpravidla mnohem vyšší tepovou frekvenci než středně velká, nebo velká plemena psů. Jako příklad lze uvést příklad normální tepové frekvence. Zatímco u malých psů se rozmezí pohybuje mezi 160 až 220 BPM, u středně velkých plemen (mezi 14 a 40 kilogramy) je normální tepová frekvence již pouze 60 až 100 BPM. U velkých plemen (nad 40 kg) je pak normální tepová frekvence od 60 do 80 BPM. Obvyklé tepové frekvence jsou rovněž závislé na věku psa. Štěňata mají obvykle vyšší tepovou frekvenci než dospělí psi. Dále je třeba zohlednit fakt, že tepová frekvence u psů i koček je nepravidelná a mění se v závislosti na nádechu nebo výdechu zvířete. Dechová frekvence se pak u malých psů pohybuje mezi 20-30 nádechy za minutu a u velkých plemen mezi 10-30 nádechy za minutu. Je však

nutné zohlednit také fakt, že psi si udržují přirozenou termoregulaci těla pomocí sliznic na povrchu tlamy a jazyka. V případech, kdy je psovi horko, může dechová frekvence krátkodobě vzrůst i na 200 nádechů za minutu. U koček je závislost tepové a dechové frekvence na věku a velikosti zvířete obdobná, pouze rozdíly nejsou tak markantní. Jako obvyklé se uvádí hodnoty mezi 160 až 220 BPM (Veterinární klinika NISA 2019a; 2019b). U dechu je to pak mezi 20 až 30 nádechy za minutu.

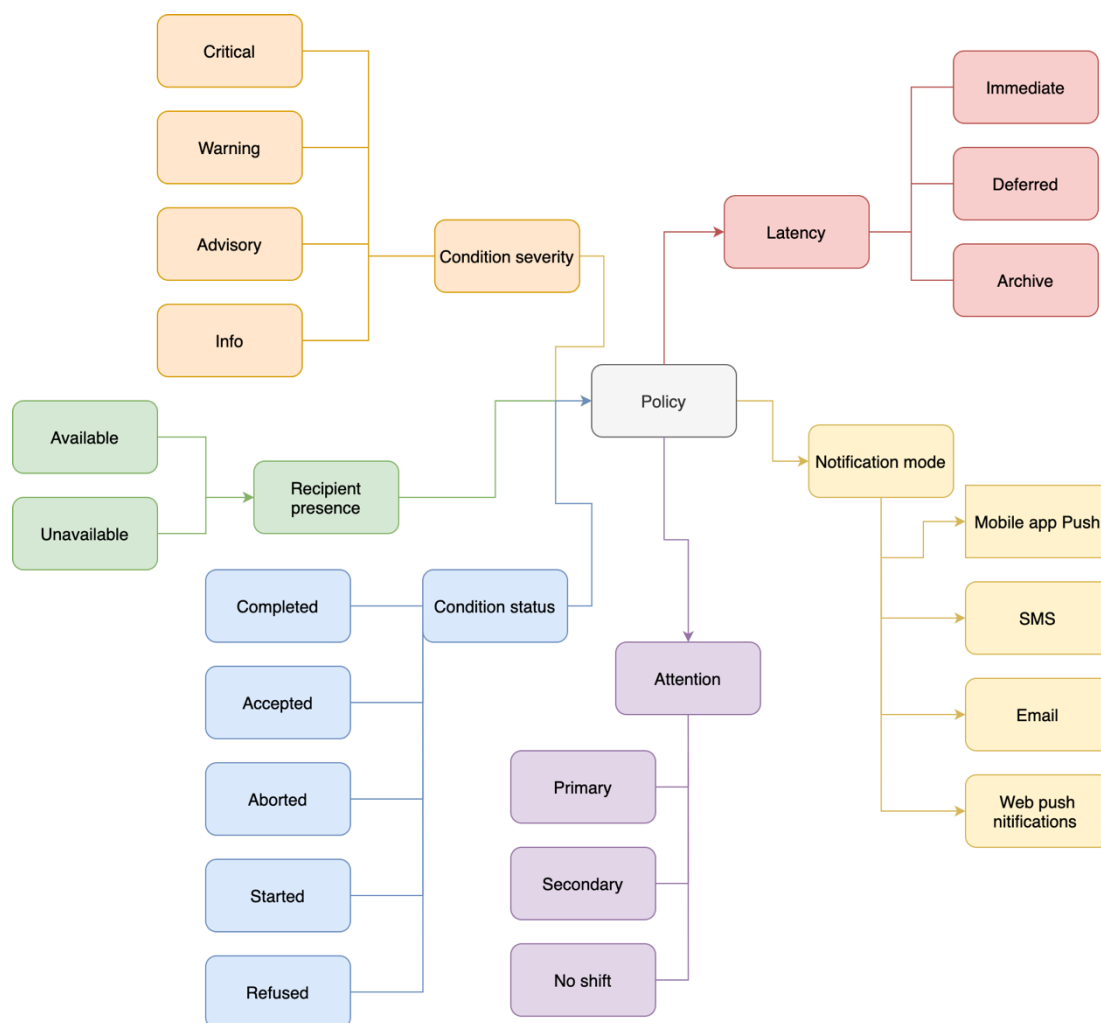
Podle druhu a velikosti hospitalizovaného zvířete jsou automaticky nastaveny výchozí hodnoty alarmů. Z výše uvedených důvodů je však nezbytné, aby zdravotník mohl tyto hodnoty přizpůsobit na míru měřenému zvířeti, ale i jeho aktuálnímu zdravotnímu stavu, věku, nebo tělesné teplotě. Stejně tak je možné jednoduše definovat a snadno za běhu měnit možnosti notifikace jednotlivého zdravotního personálu v dohledové a administrační aplikaci prostřednictvím webového rozhraní. Ukázka nastavení prahových hodnot v uživatelském rozhraní je součástí Přílohy 3.

Systém notifikací má za úkol varovat uživatele, nebo lékaře v případě náhlého zhoršení zdravotního stavu zvířete, ale také jej informovat formou pravidelných reportů o jeho dlouhodobém zdravotním stavu. Systém rovněž pomáhá hlídat a notifikovat uživatele o pravidelném podávání medikace. Ukázka webového rozhraní je součástí Přílohy 4.

Jednotlivé notifikace lze specifikovat podle závažnosti upozornění, statusu, nebo výskytu uživatele a na základě těchto specifikací definovat způsob jakým uživatele notifikovat. Klíčovou funkcí systému je umožnit uživateli detailně popsat případy kdy a jakým způsobem chce být upozorněn o vzniklé situaci. Ale také umožnit uživateli tyto podmínky dynamicky měnit. Grafické znázornění jednotlivých ontologií a způsoby notifikací zobrazuje Obrázek 5.

Jednotlivé notifikace mohou mít různou podobu v závislosti na typu zprávy a její důležitosti. V případě webového prohlížeče se může jednat například o push oznámení (push notifikace), které se následně zobrazí v oznámeních operačního systému. Naopak zpráva s nižším stupněm důležitosti se pak může zobrazit pouze jako ikona ve webové aplikaci samotné. Obdobně tomu může být i v případě mobilní aplikace. Kritické zprávy, nebo zprávy s velmi vysokou prioritou pak mohou mít například podobu SMS zprávy, nebo kombinovat několik způsobů odeslání notifikací naráz. Naopak zprávy informačního charakteru pak mohou mít podobu emailového přehledu událostí

za uplynulé období. V této fázi lze rovněž využít možnosti omezit maximální množství některých typů zpráv za den (týden/měsíc), tak aby uživatel nebyl zbytečně zatěžován množstvím zpráv. Zpoždění (*Latency*) zpráv dále udává, zda se má daná zpráva zobrazit ihned, nebo se zpožděním, například za určitý čas, nebo v určitou hodinu. To je výhodné právě u zobrazování pravidelných reportů, případně pro plánování medikace.



Obrázek 5: Notifikace Ontologie systému; převzato z (Bunch et al. 2005) upraveno

U notifikací je rovněž nutné zajistit, aby dokázali upozornit zdravotní personál i v případě výpadku internetového připojení na jednotlivých edge nodech. V případě webových oznámení je již tento problém vyřešen samotným umístěním edge nodu uvnitř lokální sítě, ale v případě mobilních zařízení nelze spoléhat na standardní systém notifikací například pomocí Google Firebase, nebo Apple Push Notification service, ale je třeba

zajistit alternativní způsob jakým push notifikace zasílat. Jedním z nich je například použití lokálního MQTT brokeru. V takovém případě stačí, aby bylo mobilní zařízení připojeno do stejné lokální sítě, případně byla nastavena směrovací pravidla tak, aby umožňovala komunikaci mezi oběma zařízeními. V případě SMS pak rovněž nelze využívat SMS brány třetích stran, ale je třeba vytvořit lokální SMS bránu ať přímo jako součást edge nodu, nebo jako novou (virtuální) edge gateway uvnitř lokální sítě. Ukázka push notifikací je rovněž součástí Přílohy 3.

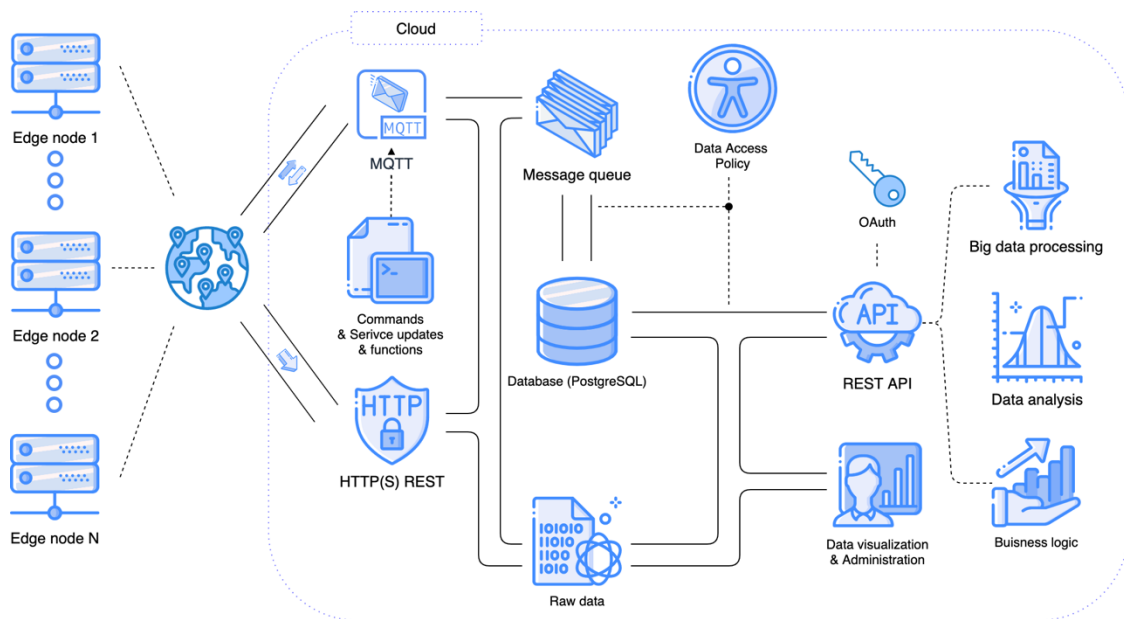
Aplikace pro zdravotní dohled (*Health monitor*) má za úkol zprostředkovávat veškerou interakci mezi zdravotníkem a systémem. Jedná se o webovou aplikaci, která zobrazuje aktuální a historické hodnoty, umožňuje správu parametrů systému, administraci jednotlivých uživatelů a pacientů spadající pod lokální organizaci.

S ohledem na požadavek ze strany zdravotníků na funkčnost monitoru i v případě úplné ztráty internetového spojení byl tento systém nasazen již na úrovni lokální sítě, a nikoliv jako cloudová aplikace. Tím se sice systém stává odolný vůči výpadkům sítě, zároveň však přináší mnohé nevýhody a rizika uvedená v sekci 7.1, zejména jakým způsobem kontrolovat a zajistit dostupnost dané služby a jak udržovat jednotlivé edge nody v aktuální verzi. Celý systém tak využívá výhod kontejnerizace aplikací, konkrétně je to kompletní provoz v rámci Docker kontejnerů. Výhodou takového řešení je nejen fakt, že jednotlivé aplikace jsou provozovány v konzistentním prostředí bez ohledu na hostitelský systém. Dále jednotlivé aplikace běží zcela izolovaně a nemohou se tak navzájem ovlivňovat, ale kontejnerizace přináší zároveň i řadu výhod v oblasti verzování a zálohování aplikací, ale také jejich orchestrace, škálování nebo přenositelnosti jednotlivých aplikací do nového zařízení.

Celá aplikace je zpracována na platformě Jakarta Enterprise Edition (resp. Jakarta EE) a to z důvodu možnosti integrace nepřeborného počtu řešení pro podporu webových aplikací jako nativní součást základní knihovny, stejně tak podpory pokročilé správy transakcí JTA (*Java Transaction API*), metody EJB (*Enterprise Java Beans*) a CDI (*Code Dependency Injection*), nebo pokročilé metody zabezpečení aplikací a práce s business logikou.

8.3 Cloud

Cloudová aplikace primárně slouží jako sběr zpracovaných dat ze všech lokalit, jejich uchování a distribuci mezi jednotlivými lokalitami. Proces přijímání dat, jejich uložení do databáze, případně na lokální uložení a následné vystavení těchto dat dalším službám znázorňuje Obrázek 6.



Obrázek 6: Cloudová aplikace – Proces uložení a získávání dat; (autor)

Data jsou z jednotlivých edge nodů přijata prostřednictvím jedné z dostupných gateway. Aktuálně dostupné technologie jsou MQTT jakožto zástupce komunikační technologie využívající návrhového vzoru publish-subscribe a klasické HTTP(S) REST API jakožto tradiční request-response protokolu pro komunikaci klient-server. MQTT je svou stavbou vhodné pro zasílání velkého objemu malých zpráv, kdy díky kombinaci malé hlavičky paketu a možnosti nastavení spolehlivosti přenosu QoS dokáže efektivně zasílat velké množství zpráv, přičemž zároveň dokáže šetřit přenosovou šířku pásma. Oproti tomu HTTP je pro svou vyšší režii uzpůsobeno k zasílání větších objemů dat, kde se tolik neprojeví výrazně vyšší režie nezbytná pro navázání spojení, které je navíc na rozdíl od MQTT navazováno znovu, vždy před zahájením nového přenosu. Tato gateway je tedy určena primárně právě pro surová data zasílaná v dávkách. Surová data jsou pouze zaindexována a následně uložena na disk. Ostatní data jsou ukládána do databáze, odkud je mohou jednotlivé aplikace získávat prostřednictvím dotazů přes REST API. Výsledky

zpracování těchto aplikací lze následně opět prostřednictvím REST API zasílat zpět od aplikace, nebo mohou být využita pro pravidelnou tvorbu reportů za jednotlivá časová období. Jednotlivé přehledy dat lze rovněž zobrazovat prostřednictvím webové aplikace. Ta je určena výzkumníkům a zobrazuje jednotlivé hodnoty prostřednictvím grafů.

Modul pro správu přístupu k datům (Data access policy) má na starosti řízení přístupu jednotlivých uživatelů k záznamům ať už vlastním, nebo k záznamům z jiných lokalit. V případech, kdy chce uživatel přistupovat k datům z pocházejícím z jiné lokality, musí o přístup k těmto datům požádat u správce dané lokality. Ten může následně přístup k datům udělit, případně specifikovat dobu, po kterou je přístup k datům umožněn. Přístup lze udělovat na úrovni jednotlivého zvířete, skupiny zvířat, nebo celé lokality.

9 Implementace systému, technické výzvy

9.1 Propustnost systému

V rámci testování systému proběhlo rovněž měření propustnosti jednotlivých edge nodů s cílem zjistit, kolik připojených zařízení zvládne jeden edge node obsloužit, bez toho, aby docházelo k ohrožení stability tohoto edge node, případně aniž by docházelo k nežádoucím výpadkům dat.

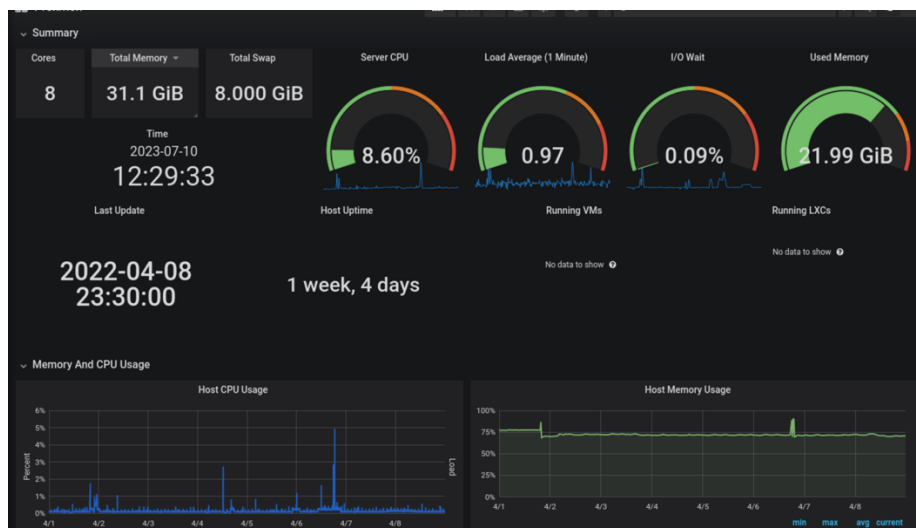
V rámci testovacího scénáře byla vytvořena aplikace emulující provoz senzorické vrstvy tak aby co možná nejvěrohodněji simulovala reálný provoz. Následně byla aplikace pomocí metod kontejnerizace převedena do podoby Docker kontejneru, tak aby mohla být efektivně distribuována na jednotlivá zařízení, ale také velice jednoduše škálována na požadovaný počet paralelně běžících instancí. Následně byla za pomoci standardních linuxových nástrojů monitorována aktivita edge node. Klíčovými parametry pro měření propustnosti bylo obsazení operační paměti, vytížení procesoru, případně byly zkoumány další sekundární parametry jako vytížení sítě, nebo množství dat ukládaných na disk při offline režimu. Pro úspěšné splnění testu musel být systém v provozu bez samovolného, nebo vynuceného restartu minimálně po dobu 7 dní, přičemž průměrné vytížení zdrojů nesmí přesáhnout hranici 75 %. Naměřené hodnoty byly ukládány do InfluxDB NoSQL databáze odkud byly pomocí nástroje pro vizualizaci dat Grafana prezentovány v podobě jednotlivých grafických výstupů uživateli. Ukázka jednoho z nabízených grafických výstupů znázorňuje Obrázek 7.

V rámci testovacího scénáře byl zvolen standardní notebook (8-core i7; 32GB RAM; 512GB SSD)

Pro účely benchmark testování byl vybrán nod produkující data o třech složkách X, Y a Z spolu s časovou značkou rychlostí 1000 Hz, tedy 1000 naměřených datových vzorků za vteřinu. Z pohledu použitých datových typů se jedná o 3* datový typ Double (64 b) a jednou Integer (32 b). Celkový objem dat produkovaný z jedním nodem je tak okolo 225 kB/s v textové nekomprimované podobě.

Jedním z klíčových ukazatelů pro hodnocení propustnosti systému bude ukazatel, kolik paralelně běžících nodů zvládne systém obsloužit. Pro účely testování tak byla vytvořena

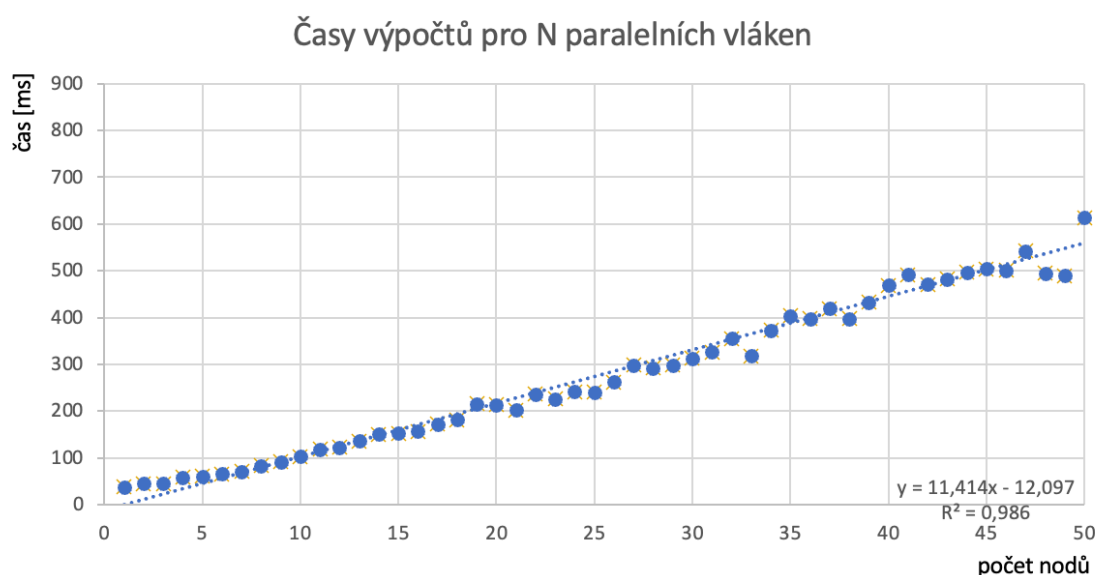
jedna instance edge nodu, která bude nepřetržitě vypočítávat informace o tepové a dechové frekvenci, přičemž budeme postupně systém zatěžovat přidáváním dalších instancí aplikací simulujících provoz jednotlivých senzorů a budeme zkoumat vliv celkového počtu připojených senzorů na stabilitu systému.



Obrázek 7: Ukázka základních metrik – Grafana; (autor)

Na základě testování doby vyhodnocení sta nezávislých vzorků bylo zjištěno, že průměrná doba potřebná pro vyhodnocení dat z jednoho senzoru je 38 ms. Lze předpokládat, že paralelizací dojde k navýšení propustnosti systému. Teoreticky můžeme očekávat, že paralelizací dojde k rozložení zátěže mezi dostupná procesorová jádra a doba výpočtu osmi paralelních úloh tak bude na osmi-jádrovém procesoru totožná s výpočtem totožné úlohy využívající pouze jedno procesorové jádro. V praxi je však třeba počítat nejen s dodatečnou režii nezbytnou pro zajištění paralelního chodu úloh, ale také s faktem, že ne všechny kroky výpočetního algoritmu lze plně paralelizovat. I přesto, že jsou jednotlivé výpočty na sobě nezávislé a není tak nutné čekat na dokončení výpočtu předchozích měření, bude část programu vždy prováděna sekvenčně. Jedná se zejména o operace využívající sdílené zdroje I-O, nebo zápisy do globálních proměnných. Zároveň je třeba uvažovat s faktem, že programovací jazyk Java je již z principu navržen tak, aby dokázal využít všechna dostupná procesorová jádra a většina úloh je automaticky zpracovávána ve více vláknech.

Samotný algoritmus pro vyhodnocení vitálních funkcí má z povahy použitých funkcí výpočetní složitost logaritmického charakteru. Z důvodu konstantní snímkovací frekvence (v tomto případě 1000 vzorků za sekundu) a tedy i konstantní velikosti datového souboru lze samotnou výpočetní složitost zanedbat a můžeme tak předpokládat spíše lineární trend v nárůstu časů se vzrůstajícím počtem připojených zařízení. Obrázek 8 znázorňuje graf závislosti délky výpočtů na počtu připojených zařízení. Osa X znázorňuje počet běžících instancí, osa Y následně časy v milisekundách nezbytné pro zpracování vstupních dat a provedení nezbytných výpočtů. Jednotlivé body jsou tvořeny zprůměrováním výsledných hodnot ze 100 nezávislých měření tak aby došlo k alespoň částečné eliminaci odchylek způsobených vytížením ostatními běžícími procesy



Obrázek 8: Graf závislosti délky výpočtu na počtu paralelních vláken; (autor)

Výsledné body byly následně proloženy přímkou za pomoci lineární regrese. Výsledná hodnota spolehlivosti $R^2 = 0.986$ rovněž poskytuje poměrně přesnou predikci lineárního modelu. Na základě tohoto modelu lze usoudit, že s rostoucím počtem zařízení stoupá čas potřebný pro jejich výpočet lineárně. Zjistili jsme, že tento čas roste tempem zhruba o 100 milisekund na každých 10 nově přidaných instancí.

V rámci daného HW tak jsme schopni bezpečně zpracovat více než 50 aktivních senzorů s frekvencí 1000 Hz, přičemž systém stále schopný poskytnout dostatek času pro další operace prováděné na pozadí, jako je obsluha ostatních komponent, nebo archivace surových dat.

Uvnitř každé lokality jsou obvykle provozovány nižší desítky zařízení s podobnou frekvencí. Propustnost systému je tedy pro daný hardware více než dostatečná. V případě potřeby je rovněž možné edge node vertikálně, nebo horizontálně škálovat.

9.2 Zabezpečení komunikace

V rámci implementace zabezpečené komunikace se senzory byla rovněž provedena analýza zranitelností implementovaného MQTT protokolu. V rámci bezpečnostní analýzy byla zhodnocena nejen potenciální rizika a doporučení použité knihovny při implementaci komunikačního modulu, ale také na způsob a doporučená nastavení samotného MQTT brokeru, který je zodpovědný za distribuci zpráv v rámci dané lokality.

Jak již bylo zmíněno v úvodní kapitole M2M komunikační protokoly jsou s přibývajícím množstvím IoT zařízení na vzestupu a právě MQTT (případně CoAP) patří mezi přední komunikační protokoly v oblasti IoT na úrovni M2M komunikace. Oba IoT protokoly spojuje jeho obecná struktura, která je efektivní a relativně nenáročná na implementaci a umožňující připojení velkého počtu rozdílných zařízení s často omezenými výpočetními zdroji prostřednictvím veřejného internetu. Avšak tato obecná struktura s sebou zároveň přináší určitá rizika a potenciální výzvy pro koncového programátora, jako je zajištění bezpečnosti datových přenosů, ochrana před potenciálními útoky, správa velkého objemu dat a další. Je tak nutné tyto aspekty pečlivě zvážit již při samotném návrhu komunikace a získané zkušenosti promítnout do samotné implementaci a provozu systému.

Specifikace protokolu MQTT umožňuje vývojářům vybrat si z řady dostupných bezpečnostních mechanismů v podobě nastavení sítě, soukromí, autentizace a autorizace. Volba použitých bezpečnostních technologií však bude vždy záviset na požadavcích a způsobu použití konkrétní aplikace, je tak dle oficiálního vyjádření autorů povinností implementátora samotné aplikace zahrnout do jeho návrhu příslušné bezpečnostní funkce (BANKS et al. 2023). Dále je nutné zmínit, že hlavní důraz při návrhu MQTT nebyl kladen na jeho bezpečnost, nýbrž na jeho dostupnost a většina bezpečnostních mechanismů byla implementována až v pozdějších verzích protokolu. K poměrně laxnímu přístupu k řešení zabezpečení komunikace MQTT přispívá rovněž fakt, že u většiny dostupných implementací MQTT brokerů není ve výchozím nastavení aktivován žádný z bezpečnostních mechanismů. Dodatečné nastavení bezpečnostních

mechanismů je tak ponecháno čistě na rozhodnutí administrátora daného zařízení. Častým důsledkem takového přístupu je však situace, kdy je zařízení ponecháno a provozováno zcela nezabezpečené, což logicky nahrává i případným útočníkům. Spolu s rostoucím počtem IoT zařízení se tak zabezpečení M2M protokolů stává zásadním tématem v oblasti internetové bezpečnosti a je tedy žádoucí věnovat tomuto tématu více pozornosti.

V následující kapitole budou shrnuty různé aspekty zabezpečení komunikace protokolu MQTT, popsány techniky pro zajištění bezpečného a důvěryhodného připojení na rozdílných komunikačních vrstvách.

Jedním z efektivních způsobů zabezpečené sítě na úrovni **síťové vrstvy** je využití fyzicky zabezpečené (oddělené) sítě, nebo VPN jakožto prostředek pro veškerou komunikaci mezi klienty a brokerem. Použití VPN zajišťuje, že data jsou odesílána a přijímána pouze předem autorizovanými klienty a VPN rovněž zajišťuje integritu dat uvnitř této privátní sítě.

Zabezpečení na **transportní vrstvě** je zajištěno pomocí TLS v rámci implementace TCP protokolu. Proces prvotní výměny informací pro zajištění zabezpečené komunikace (handshake) se tak nijak neliší od způsobu používaném u standardních TCP paketů například v rámci zajištění HTTPS spojení. Při prvotním handshake si obě strany vymění informace specifikující parametry spojení a použitou šifru, následně server odesílá certifikát X.509 vydaný důvěryhodnou certifikační autoritou a klient generuje náhodnou kombinaci (pre-master secret), která je šifrována veřejným klíčem a následně odeslána zpět na server. Rovněž zde může docházet i k ověření identity klienta pomocí klientského certifikátu. Samotná implementace TLS tak dokáže zajistit důvěryhodnost a integritu přenášených dat. Předpokladem pro zajištění integrity je však použití bezpečné a neprolomené šifrovací sady. TLS je však svou povahou vhodná spíše pro dlouhodobá nepřerušovaná spojení. Zároveň klade vyšší výpočetní nároky na klientská zařízení a rovněž může vlivem šifrování docházet ke zvýšení přenášeného objemu dat. Použité šifry jsou tak často voleny právě s důrazem na omezené energetické a výpočetní zdroje koncových zařízení. Mezi nejčastěji používané šifry v IoT patří AES, ChaCha20, ECC, nebo RSA. Jednotlivé šifry jsou seřazeny od nejméně bezpečné, až po nejbezpečnější, ovšem také nejnáročnější na výpočetní zdroje. Volba konkrétní šifry však vždy závisí

na požadavcích dané aplikace, případně na volbě vhodného kompromisu mezi bezpečností, výkonem a energetickou efektivitou pro konkrétní IoT nasazení.

Druhou častou používanou metodou je autentizace klienta pomocí TLS-PSK (Pre-Shared Key Ciphersuites for Transport Layer Security). Bezpečná komunikace je zde zajištěna sadou předem generovaných kryptografických klíčů. Odpadá tak náročná výměna veřejných klíčů a tato metoda je tak vhodná i pro jednoduchá zařízení s velice omezenými výpočetními možnostmi, nicméně je nutné předem zajistit konfiguraci sady klíčů a jejich následnou distribuci na obě komunikující zařízení. Dalším omezením může být rovněž omezená podpora v rámci některých implementací (Cheng et al. 2017).

MQTT rovněž nabízí možnosti zabezpečení na **aplikační vrstvě**, zde je však nutné zdůraznit, že většina mechanismů spoléhá na implementaci bezpečnostních pravidel na úrovni nižších vrstev. Například autentizace klienta uživatelským jménem a heslem zcela spoléhá na zabezpečení nižších vrstev a v případě jejich absence odchází data zcela nezašifrovaná. Veškeré autentizační mechanismy tak lze chápat pouze jako rozšiřující mechanismy pro ověření identity (autentizaci) klientů v rámci systému ke stávajícímu zabezpečení na síťové a transportní vrstvě. Kromě zmíněné autentizace uživatelským jménem a heslem (v nejnovější verzi MQTT v5.0 již lze k autentizaci použít pouze heslo) nabízí MQTT také autentizaci pomocí jednoznačného identifikátoru, OAuth 2.0, pomocí ACL, případně pomocí řídicího AUTH packetu. Detailní přehled všech dostupných metod je součástí oficiální dokumentace (BANKS et al. 2023).

V případě potřeby je rovněž možné implementovat šifrování obsahu zpráv. MQTT však nijak nedefinuje způsob jakým data šifrovat. Obsah MQTT zprávy může mít podobu libovolných binárních dat což umožňuje mimo šifrování obsahu také implementaci dalších serializačních mechanismů, které mohou například redukovat množství přenášených (Stepan et al. 2017b). Veškeré tyto algoritmy je však nutné implementovat nezávisle na MQTT protokolu až na úrovni konkrétní aplikace.

9.2.1 Testování zranitelností

Součástí testování aplikace byly navrženy jednotlivé penetrační scénáře ověřující nastavení komunikačního brokeru. Pro identifikaci jednotlivých hrozeb bylo vytvořeno testovací prostředí se simulovaným provozem několika zařízení.

Jako MQTT broker byla nainstalována poslední dostupná verze Eclipse Mosquito (v2.0.15), který je dle přehledu nejpoužívanějších MQTT implementací zveřejněného (Agnihotri 2022) aktuálně nejrozšířenější open source implementací MQTT brokeru. Jako zařízení pro penetrační testování byl použit virtuální počítač s distribucí Kali Linux s přímým přístupem do testované sítě. Jednotlivé scénáře zahrnují mechanismy aktivního průzkumu a následné útoky na různé bezpečnostní vrstvy a zabezpečení komunikačního protokolu. Každý z testovacích scénářů bude v úvodu stručně představen a následně popsány způsoby analýzy dané zranitelnosti a případně představeny jednotlivá přijatá bezpečnostní opatření pro eliminaci rizika zneužití dané zranitelnosti.

Samotnému cílenému útoku často předchází prvotní důkladná analýza síťové komunikace zahrnující získávání základních informací o jednotlivých zařízeních umístěných uvnitř sítě, jejich povaze, frekvenci a druhu zasílaných zpráv s cílem sběru citlivých údajů, případně odhalit potenciální možnosti pro cílení jednotlivých útoků. V rámci práce můžeme tento scénář ještě dále rozdělit do dvou částí. V první části bude provedeno skenování testované sítě s cílem identifikovat v síti dostupné brokery. Ve druhé fázi bude následně provedena analýza síťové komunikace s cílem identifikovat zranitelná místa a představit potenciální možnosti včetně míry rizika jejich zneužití. Následně budou představena aktivní opatření pro eliminaci jednotlivých útoků.

9.2.1.1 Sběr informací

Prvním krokem pro identifikace MQTT brokeru v neznámé síti je skenování dané sítě s cílem identifikovat otevřené porty za pomoci jednoduchého scriptu v jazyce Python, který pomocí modulu Nmap skenuje definovaný adresní prostor a s cílem identifikovat otevřené porty 1883 a 8883. Pokud nalezne aktivní spojení na jednom z portů, pokusí se na dané zařízení připojit pomocí funkce `mqtt_subscribe` s cílem prozkoumat všechna dostupná témata. V MQTT lze rovněž pomocí zástupných znaků `+`, nebo `#` specifikovat jednu či více úrovní které lze odebírat. Pomocí výrazu `/#` tak dojde k odběru celého stromu dostupných zpráv, které jsou na broker aktuálně odesílány.

Obrázek 9 znázorňuje výstup python scriptu. Jsou zde patrné systémové informace o brokeru publikované na tématech `$/SYS/broker/#` jako je verze brokeru, případně další metriky, ale také topiky, na kterých jsou publikována reálná data včetně poslední odeslané hodnoty. Na obrázku 8 je zvýrazněn použitý broker spolu s aktuálně provozovanou verzí

aplikace, ale také data publikovaná na tématu *smartVet/data* spolu s ukázkovou interpretací dat ve formátu JSON

```
sh-3.2# cat results.txt
PORT      STATE SERVICE
1883/tcp  open  mosquitto
|
| mqtt-subscribe:
|   Topics and their most recent payloads:
|   $SYS/broker/load/publish/received/5min: 0.27
|   $SYS/broker/publish/messages/received: 7
|   $SYS/broker/heap/current: 39240
|   $SYS/broker/load/messages/sent/15min: 21.54
|   $SYS/broker/load/bytes/sent/5min: 647.13
|   $SYS/broker/clients/disconnected: 40
|   $SYS/broker/clients/connected: 3
|   $SYS/broker/subscriptions/count: 40
|   $SYS/broker/load/publish/received/15min: 0.46
|   $SYS/broker/clients/inactive: 40
|   $SYS/broker/messages/sent: 2318
|   $SYS/broker/load/publish/sent/1min: 2.48
|   $SYS/broker/load/sockets/1min: 0.09
|   $SYS/broker/load/connections/15min: 0.41
|   $SYS/broker/load/bytes/sent/15min: 822.79
|   $SYS/broker/load/sockets/15min: 0.81
|   $SYS/broker/version: mosquitto version 1.4.8
|   $SYS/broker/load/publish/sent/15min: 20.39
|   $SYS/broker/uptime: 225478 seconds
|   $SYS/broker/load/publish/received/1min: 0.05
|   $SYS/broker/publish/messages/dropped: 0
|   $SYS/broker/retained messages/count: 47
|   $SYS/broker/messages/received: 293
|   $SYS/broker/load/connections/5min: 0.28
|   $SYS/broker/load/messages/sent/1min: 2.78
|   $SYS/broker/bytes/sent: 83026
|   $SYS/broker/load/bytes/received/5min: 13.98
|   $SYS/broker/load/messages/received/1min: 0.35
|   $SYS/broker/messages/stored: 147
|   $SYS/broker/publish/messages/sent: 2070
|   $SYS/broker/load/sockets/5min: 0.53
|   $SYS/broker/clients/active: 3
| smartVet/data: { "clientId": "e399acfc-24c4-11e6-be56-0242ac120002", "typeId": 2, "timestamp": 1689612833000, "values": [1.0144, 6.1016, 3.7527, 6.0638, 3.6477, 5.9966, 3.9596, 6.0482] }
|
| $SYS/broker/load/bytes/received/15min: 17.83
| $SYS/broker/publish/bytes/received: 49
| $SYS/broker/load/publish/sent/5min: 16.03
| $SYS/broker/publish/bytes/sent: 9752
| $SYS/broker/load/bytes/sent/1min: 100.49
| $SYS/broker/load/bytes/received/1min: 2.72
| $SYS/broker/load/connections/1min: 0.06
| $SYS/broker/clients/expired: 0
| $SYS/broker/load/messages/received/15min: 1.49
| $SYS/broker/load/messages/sent/5min: 17.00
| $SYS/broker/bytes/received: 2628
| $SYS/broker/heap/maximum: 41992
|_ $SYS/broker/clients/total: 41
sh-3.2#
```

Obrázek 9: Nmap výstup dostupných zpráv; (autor)

Na základě analýzy provedené (Durumeric et al. 2015 a Neshenko et al. 2019) v letech 2015 až 2019 jsou bezmála tři čtvrtiny (74,6%) všech veřejně dostupných brokerů provozována na výchozích portech bez jakéhokoliv zabezpečení, nebo jen s minimálním zabezpečením bez jakéhokoliv dodatečného šifrování přenosu např. pomocí TLS. Rovněž uvádí, že 44,7% všech skenovaných zařízení přijímá anonymní připojení bez jakéhokoliv ověřování identity klienta. Přitom díky absenci zabezpečení lze zprávy nejen číst ale rovněž publikovat na ostatní zařízení a ovlivnit tak jejich následný provoz. Lze tak poměrně jednoduchým způsobem kompromitovat přenášená data a ovlivnit tak výslednou funkci systému ve prospěch útočníka.

Ve druhé části testovaného scénáře bude simulováno odposlouchávání komunikace s cílem zachytit obsah CONNECT packetu a pokusit se vyčíst údaje z tohoto packetu jako je Client ID, případně uživatelské jméno a heslo. Nástrojem Wireshark budeme odposlouchávat síťovou komunikaci a následně zachycená data analyzovat. Obrázek 10 znázorňuje podobu *MQTT CONNECT* packetu ve kterém je modře vyznačena část obsahující vložené uživatelské heslo. Z tohoto obrázku je jasně patrné, že veškeré

informace uvnitř CONNECT packetu jsou zasílány v prostém textu bez jakéhokoliv předchozího šifrování jeho obsahu. Prostá autorizace na úrovni aplikační vrstvy tak bez dalšího šifrování neposkytne téměř žádnou ochranu před útočníky.

```

Frame 28: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface en0,
Ethernet II, Src: Apple_79:14:eb (a0:78:17:79:14:eb), Dst: Routerbo_a5:1f:80 (74:4d:28:a
Internet Protocol Version 4, Src: 172.16.17.61, Dst: 52.57.158.144
Transmission Control Protocol, Src Port: 50539, Dst Port: 1883, Seq: 1, Ack: 1, Len: 53
MQ Telemetry Transport Protocol, Connect Command
0000 74 4d 28 a5 1f 80 a0 78 17 79 14 eb 08 00 45 00 tm(....x..y....E
0010 00 69 00 00 40 00 40 06 aa 78 ac 10 11 3d 34 39 ..i..@..x....=49
0020 9e 90 c5 6b 07 5b 1a c5 be c8 3d b0 98 ad 80 18 ...k[...=.....
0030 08 0a 45 10 00 00 01 01 08 0a f5 41 9b 5a 92 6f ...E.....A.Z.o
0040 e9 7f 10 33 00 04 4d 51 54 54 04 c2 00 3c 00 0c ...3..MQTT...c..
0050 74 65 73 74 43 6c 69 65 6e 74 45 64 00 09 74 65 testClic ntId te
0060 73 74 4c 6f 67 69 6e 0e 73 65 63 72 65 74 50 stLogin secretP
0070 61 73 73 77 6f 72 64 assword

```

Obrázek 10: Wireshark – Analýza CONNECT packetu; (autor)

Získáním klientského ID z odposlechnuté komunikace lze snadno podvrhnout identitu původního klienta. Útočník se tak může vydávat za legitimního klienta, případně se může pokusit podvrhnout obsah zpráv a komunikovat s brokerem nebo dalšími klienty. Může tak opět dojít k narušení integrity a autentičnosti zasílaných zpráv. Zneužitím clientId může také poskytnout útočníkovi cenné informace pro potenciální DoS (Denial of Service) útoky. Útočník tak může snadno zneužít identifikátor k nadměrnému vytěžování zdrojů nebo k přetěžování ostatních klientů zasíláním nadměrného množství zpráv, a výrazně omezit, případně zcela znemožnit legitimním klientům komunikaci s brokerem. Odposlechnutí ClientId může také umožnit útočníkovi sledovat aktivitu konkrétního klienta a získat tak přístup k informacím o zasílaných a přijímaných zprávách klienta, což může útočníkovi zpřístupnit některé citlivé údaje nebo odhalit chování a vzorce v komunikaci a které mohou být následně zneužity pro cílení dalších útoků. ClientId by se tak ze stejných důvodů rovněž nemělo vyskytovat v názvu tématu, nebo v obsahu zprávy, kde může rovněž snadno dojít k jeho zcizení a následnému zneužití.

Důležitost volby silného hesla rovněž podtrhuje fakt, že MQTT nemá žádné vestavěné mechanismy proti brute force útokům na uživatelská jména a hesla. Volba silného hesla je tak u MQTT daleko důležitější než u jiných protokolů, protože případný útok lze často odhalit až z důkladné analýzy síťové komunikace. Částečnou ochranou může poskytovat například doplnění o omezení počtu neúspěšných pokusů dočasným zablokováním uživatele, nebo umělým postupným prodlužováním doby odezvy při opakovaných pokusech o přihlášení a tím i prodlužování celkové doby nutné pro prolomení hesla hrubou silou. Vždy se však bude jednat o dodatečnou implementaci na úrovni aplikace, a tedy je tato volba zcela ponechána na vlastním uvážení vývojáře konkrétního řešení.

Rovněž lze přihlašování uživatelů v případě potřeby rozšířit o například o prvky dvou faktorového ověřování pomocí HW, nebo SW klíče, avšak ve světě jednoduchých IoT zařízení se jedná o poměrně nepraktické a pro převážnou většinu instalací zbytečně komplikované řešení.

Mimo aktivní ochrany proti útokům je rovněž neméně důležitý pasivní monitoring aktuálního provozu s následnou detekcí podezřelých aktivit. Jedním z častých ukazatelů útoku je podezřele vysoký počet pokusů o přihlášení z jedné IP adresy, pokusy o přístup z podezřelých IP adres, nebo právě velké množství odebíraných zpráv z několika různých témat. Pokud není přímo nezbytné přistupovat k brokeru prostřednictvím veřejného internetu, lze většinu bezpečnostních hrozeb eliminovat již zmíněným zabezpečením na úrovni síťové vrstvy. V opačných případech je nutné zabezpečení aplikace na transportní vrstvě doplněné o vhodnou kombinaci zabezpečení aplikační vrstvy.

9.2.1.2 Zabezpečení transportní vrstvy

V předchozích kapitolách bylo zmíněno, proč hraje zabezpečení transportní vrstvy klíčovou roli v zajištění bezpečné komunikace mezi klientem a brokerem a proč je třeba věnovat zabezpečení brokeru zvýšenou pozornost. V rámci testování došlo k nastavení brokeru tak, aby splňoval požadavky zabezpečené komunikace a součástí testovacího scénáře je toto nastavení ověřit a zhodnotit úroveň zabezpečení pomocí nástroje `testssl.sh` (Wetter 2023). Jako certifikát pro zabezpečení transportní vrstvy byl použit stejný certifikát, který je použit pro samotné webové rozhraní a byl vystaven ověřenou certifikační autoritou LetsEncrypt.org. V případě potřeby si rovněž lze vygenerovat certifikát lokálně (tzv. self signed certifikát) pomocí OpenSSL knihovny. Takto vydaný certifikát však nepochází od důvěryhodné certifikační autority a je nutné zajistit uznání certifikátu všemi klienty dodatečným manuálním přidáním certifikátu do seznamu důvěryhodných certifikačních autorit. Většina nastavení brokeru se provádí v konfiguračním souboru `mosquitto.conf`, kde lze mimo jiné nastavit například porty na kterých bude broker naslouchat příchozím komunikacím, možnost připojení pro anonymní klienty, případně možnosti konfigurace autentizačních mechanismů pro přihlášení klientů včetně konfigurace TLS a možnosti vynucení minimální verze TLS šifrování. Výsledek testu znázorňuje Obrázek 11 poskytující kompletní seznam

podporovaných TLS protokolů. V tomto případě bylo v konfiguračním souboru explicitně vynuceno používání protokolu TLS 1.2 a vyšší. Starší verze SSLv2 a SSLv3 nejsou podporovány z důvodu vážných bezpečnostních nedostatků a zranitelností jako například známé zranitelnosti BEAST (Browser Exploit Against SSL/TLS) objevené v roce 2002 a popsané například v publikacích (Eldewahi et al. 2015), POODLE (Padding Oracle On Downgraded Legacy Encryption) z roku 2014 viz. (Möller et al. 2014), ale také podporují celou řadu šifrovacích algoritmů náchylných k útokům. Nejznámější je zranitelnost šifrovacího algoritmu RC4, který byl součástí protokolů SSLv2 a SSLv3 díky které bylo možné dešifrovat a odposlouchávat komunikaci mezi účastníky. Vlivem nedostatečným mechanismům ověřování serveru byly protokoly rovněž náchylné k útokům typu M-I-M (man-in-the-middle). To vše nakonec přispělo k faktu, že jsou od roku 2011 resp. 2015 jsou protokoly SSLv2 a SSLv3 označovány jako nedůvěryhodné a nedoporučuje se jejich používání. Starší verze TLS 1 a TLS 1.1 jsou rovněž aktuálně považovány za zastaralé, a to zejména z důvodu nedostatečného šifrování a i přesto, že jsou stále ve spoustě aplikací jsou i nadále podporovány, dochází k jejich postupnému nahrazování právě zmíněnými verzemi TLS 1.2 a 1.3.

```

Testing protocols via sockets except NPN+ALPN
SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    offered (OK)
TLS 1.3    offered (OK): final
NPN/SPDY   Local problem: /usr/bin/openssl doesn't support NPN/SPDY
ALPN/HTTP2 not offered

```

Obrázek 11: Přehled poskytovaných protokolů; (autor)

Následuje test kategorií podporovaných šifer. Obrázek 12 zobrazuje výsledek testu kdy jsou nabízeny pouze šifry kategorií AES a AEAD. Starší šifry, případně šifry bez autentizace serveru a klienta, stejně tak nešifrovaná spojení nejsou podporovány. Přesto že je použití šifer typu AES dle organizace SSL Labs označováno jako zastaralé a z hlediska bezpečnosti může používání této kategorie šifer představovat určité bezpečnostní riziko, tak je tato kategorie šifer ponechána pro svou jednoduchost a možnost využití i pro jednodušší klientská zařízení a s použitím dostatečné délky šifrovacího klíče (v tomto případě jsou použity klíče o délce 256 bitů) se stále jedná o velice bezpečný šifrovací algoritmus.

Testing cipher categories

NULL ciphers (no encryption)	not offered (OK)
Anonymous NULL Ciphers (no authentication)	not offered (OK)
Export ciphers (w/o ADH+NULL)	not offered (OK)
LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)	not offered (OK)
Triple DES Ciphers / IDEA	not offered
Obsoleted CBC ciphers (AES, ARIA etc.)	offered
Strong encryption (AEAD ciphers) with no FS	offered (OK)
Forward Secrecy strong encryption (AEAD ciphers)	offered (OK)

Obrázek 12: Seznam kategorií podporovaných šifer; (autor)

Následují testy pořadí navrhovaných protokolů, včetně kompletního seznamu podporovaných protokolů (tyto testy jsou součástí příloh), informace o serverovém certifikátu, případně test známých zranitelností. Obrázek 13 zobrazuje výsledek testu na známé zranitelnosti.

<u>Testing vulnerabilities</u>	
Heartbleed (CVE-2014-0160)	not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224)	not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experiment.	(applicable only for HTTPS)
ROBOT	not vulnerable (OK)
Secure Renegotiation (RFC 5746)	supported (OK)
Secure Client-Initiated Renegotiation	not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)	not vulnerable (OK) (not using HTTP anyway)
POODLE, SSL (CVE-2014-3566)	not vulnerable (OK), no SSLv3 support
TLS_FALLBACK_SCSV (RFC 7507)	No fallback possible (OK), no protocol below TLS 1.2 offered
SWEET32 (CVE-2016-2183, CVE-2016-6329)	not vulnerable (OK)
FREAK (CVE-2015-0204)	not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703)	not vulnerable on this host and port (OK) make sure you don't use this certificate elsewhere with SSLv2 enabled services, see https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=CE781FEA8FF76A41FF
ACED4DC27C88E297D6302A0BBBD15F0C8B569FCB9F5C798	
LOGJAM (CVE-2015-4000), experimental	not vulnerable (OK): no DH EXPORT ciphers, no common prime detected
BEAST (CVE-2011-3389)	not vulnerable (OK), no SSL3 or TLS1
LUCKY13 (CVE-2013-0169), experimental	potentially VULNERABLE , uses cipher block chaining (CBC) ciphers with TLS. Check patches
Winshock (CVE-2014-6321), experimental	not vulnerable (OK)
RC4 (CVE-2013-2566, CVE-2015-2808)	no RC4 ciphers detected (OK)

Could not determine the protocol, only simulating generic clients.

Obrázek 13: Test známých zranitelností TLS/SSL; (autor)

Celkové zabezpečení brokeru bylo hodnoceno se skóre 91/100 s výslednou známkou A. Detail hodnocení a váhu jednotlivých testů zobrazuje Obrázek 14. Celkové hodnocení je stanoveno jako vážený průměr výsledků všech dílčích testů jako jsou používané šify, podporované protokoly, nastavení certifikátu, konfigurace serveru a další.

Rating (experimental)

Rating specs (not complete)	SSL Labs's 'SSL Server Rating Guide' (version 2009q from 2020-01-30)
Specification documentation	https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted)	95 (28)
Key Exchange (weighted)	90 (27)
Cipher Strength (weighted)	90 (36)
Final Score	91
Overall Grade	A
Grade cap reasons	Grade capped to A. HSTS is not offered

Obrázek 14: Výsledné hodnocení bezpečnosti; (autor)

Shrnutá doporučení a postupy tak lze aplikovat nejen u zabezpečení konkrétního navrhovaného systému, ale lze je vnímat jako soubor obecných doporučení pro zajištění zabezpečené komunikace mezi IoT zařízeními prostřednictvím veřejné sítě. Důležitost zabezpečené komunikace v rámci M2M rovněž podtrhují výsledky analýzy provedené společností Trend Micro (Maggi et al. 2018) jejímž záměrem bylo zjistit úroveň zabezpečení MQTT a CoAP komunikace mezi klienty a serverem.

Výsledky analýzy odhalily celou řadu situací, kdy nedostatečné zabezpečení MQTT a CoAP komunikace, a v některých případech dokonce úplná absence jakéhokoliv zabezpečení, umožnilo útočníkům neoprávněný přístup k citlivým datům. Příklady zahrnovaly únik dat z oblastí zdravotnictví, zemědělství, chytré infrastruktury měst, a dokonce i uniklé textové konverzace zaslané prostřednictvím mobilních aplikací využívajících MQTT protokol pro přenos zpráv. Tato zjištění jasně ukazují, že zabezpečení komunikace v IoT by mělo být věnováno mnohem více pozornosti, než je tomu doposud a jedině rozšiřováním povědomí o tomto problému v kombinaci s pečlivým dodržováním všech bezpečnostních postupů lze zajistit, že citlivá data mohou být ochráněna proti jejich zneužití.

9.3 Komponentový přístup – Vizualizační řetězec

Jedním ze zásadních úkolů bylo zajistit snadný a uživatelsky přívětivý způsob, jak zobrazovat naměřená data, případně jakým způsobem umožnit drobné korekce v již naměřených datech. Tyto korekce mohou být užitečné při zobrazování dlouhodobých trendů, nebo pro zvýraznění některých užitečných informací v signálu, jako jsou prudké změny srdečního tepu, nebo dechu. Ty mohou nastat jako reakce na poskytnutou léčbu, fyzickou aktivitu, nebo jako důsledek srdeční poruchy.

Jedním z požadavků bylo zajistit možnost dodatečných drobných korekcí naměřených dat, aby bylo možné zdůraznit abnormality v srdečním tepu, ale zároveň nedocházelo k modifikaci již vypočítaných dat. Z tohoto důvodu byla implementována komponenta umožňující dodatečné zpracování dat poté co jsou vypočítané hodnoty načteny z databáze ale ještě před tím, než jsou zobrazena v podobě grafu.

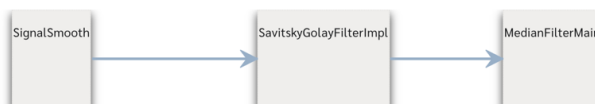
Značnou výhodou takového řešení je že data mohou být dodatečně upravována, a to i ve vyšších vrstvách systému poté co již byla zpracována algoritmy na výpočet

fyziologických funkcí. Vypočtené hodnoty tak mohou být dodatečně přizpůsobovány výběrem konkrétních funkcí, a to včetně pořadí v jakém budou na jednotlivé vypočítané hodnoty aplikovány, ale také přizpůsobením jednotlivých koeficientů každé funkce přímo na míru konkrétnímu zvířeti. Jednotlivé komponenty lze rovněž dočasně deaktivovat. Nejčastěji jsou před zobrazením dat aplikovány různé vyhlazovací funkce, nebo filtry, díky čemuž lze v signálu eliminovat nežádoucí vysokofrekvenční šum, který nebyl odstraněn prvotním výpočtem, případně lze zvýraznit dlouhodobé trendy, které by jinak mohly být maskovány šumem. Lze však implementovat téměř libovolnou novou funkci a díky komponentovému přístupu ji následně jednoduše integrovat do systému jako součást stávající implementace, nebo v podobě dodatečných pluginů.

Případnou nevýhodu takového řešení může představovat zvýšená latence spojená s dodatečným zpracováním dat po jejich načtení z databáze, ke které může teoreticky docházet vlivem vyšší výpočetní náročnosti funkcí použitých při dodatečném zpracování které je nutné provádět při každém načtení grafu uživatelem. Během provozu se však tato dodatečná režie nijak zásadně neprojevovala na celkové odezvě systému. Obrázek 15 znázorňuje ukázkou z webové aplikace zobrazující přehled použitých komponent začleněných do zobrazovacího řetězce spolu s možností deaktivace jednotlivých komponent nebo změny pořadí prostým přetažením řádků tabulky, případně úprava parametrů každé z definovaných funkcí v pravé části tabulky. Seznam aktuálně používaných komponent a jejich pořadí znázorňuje vývojový diagram ve spodní části obrázku.

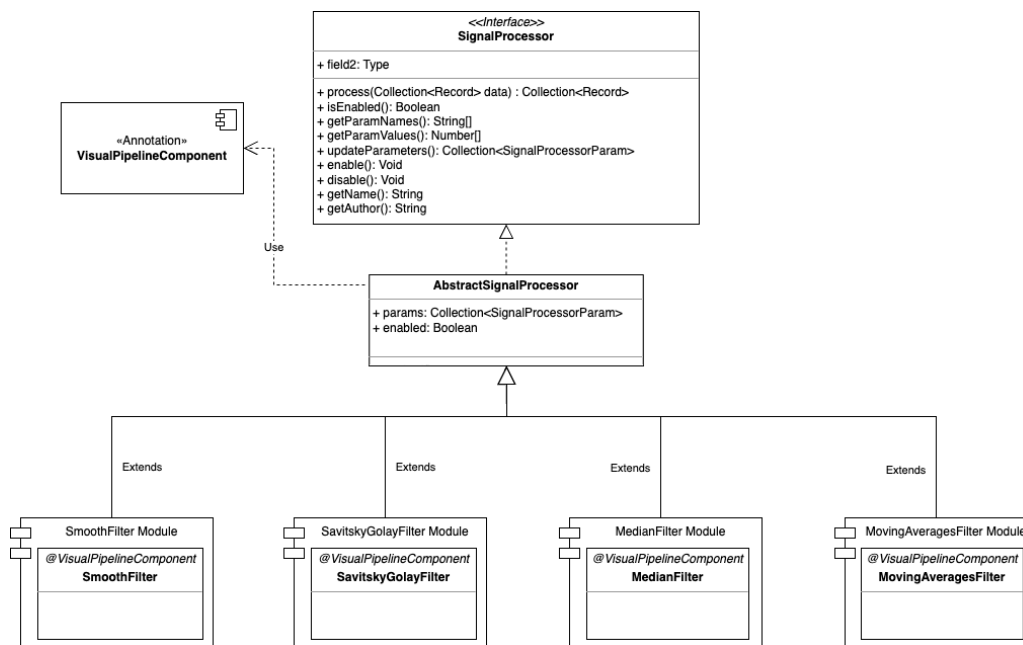
Proces zpracování dat

Moduly pro zpracování dat			
Název	Autor	Parametry	Akce
SignalSmooth	CAT UHK	tolerance = 0.6, vyhlazeni = 25, k = 15,	Deaktivovat Upravit parametry
SavitskyGolayFilterImpl	Marcin Rzeźnicki	nl = 5, nr = 5, degree = 3,	Deaktivovat Upravit parametry
MedianFilterMain	CAT UHK	k = 10,	Deaktivovat Upravit parametry



Obrázek 15: Vizualizační řetězec – ukázkou vybraných modulů a možností jejich nastavení; (autor)

Pro využití komponentového přístupu byl aplikovány pravidla objektově orientovaného přístupu (OOP) a navržena obecná struktura pro jednotlivé komponenty zobrazovacího řetězce s důrazem nejen na jejich znovu použitelnost ale také snadnou úpravu nebo budoucí rozšíření implementace. Tento přístup umožnil nejen abstrakci konkrétní implementace od obecného přístupu k jednotlivým komponentám zobrazovacího řetězce, ale také přispěl k zajištění udržitelnosti provozované aplikace oddělením výpočetních komponent od klíčových částí systému. V rámci OOP přístupu je každá komponenta zobrazovacího řetězce reprezentována jako samostatný objekt, případně soubor vzájemně propojených objektů, které však vzájemně sdílí stejné komunikační rozhraní. Jednotná struktura zaručuje snadnou záměnnost za komponenty s rozdílnou funkcionalitou implementující stejné komunikační rozhraní, nebo využití univerzálního způsobu obsluhy všech komponent uvnitř systému s využitím univerzálního komunikačního rozhraní. Všechny komponenty zobrazovacího řetězce implementují rozhraní *SignalProcessor*. Toto rozhraní rovněž definuje sadu poskytovaných metod pro všechny moduly implementující dané rozhraní. V Jazyce Java lze prostřednictvím Java Reflection API vyhledat všechny třídy splňující definované vlastnosti. Pro označení komponent vizualizačního řetězce byla v projektu zavedena a anotace *@VisualPipeLineComponent* pomocí které lze s využitím reflexe detekovat všechny v systému dostupné komponenty a následně je zobrazit uživateli v seznamu dostupných komponent. Z nich lze následně vytvářet jednotlivé vizualizační řetězce. Obrázek 16 zobrazuje UML diagram návrhu struktury vizualizační komponenty. Abstraktní třída *AbstractSignalProcessor* zde slouží pouze jako zástupná třída, ze které následně dědí všichni potomci představující jednotlivé komponenty.



Obrázek 16: UML diagram implementace vizualizačního řetězce; (autor)

V abstraktní třídě lze definovat společné chování všech komponent spolu s metodami, které by měly být implementovány v potomcích. Tímto způsobem lze zajistit konzistenci a strukturu v rámci všech pluginů, zatímco konkrétní implementace zůstane i nadále ponechána na jednotlivých potomcích. Na tuto abstraktní třídu je rovněž aplikována zmíněná anotace, která se následně automaticky pomocí dědičnosti automaticky promítne i do všech potomků této abstraktní třídy. Seznam prohledávaných tříd pomocí reflexe vždy zahrnuje i zděděné anotace. Vyhledáme-li pomocí reflexe všechny třídy a vyfiltrujeme je na základě této anotace, seznam tříd bude obsahovat nejen samotnou abstraktní třídu, ale i všechny její potomky, kteří tuto anotaci zdědili.

Tímto způsobem lze velice jednoduše vyhledat nejen v současnosti implementované komponenty, ale také komponenty implementované později, které mohou být do aplikace přidány jako součást dalších podpůrných knihoven implementovaných na míru konkrétnímu zákazníkovi, nebo v rámci implementace knihoven prostřednictvím třetích stran.

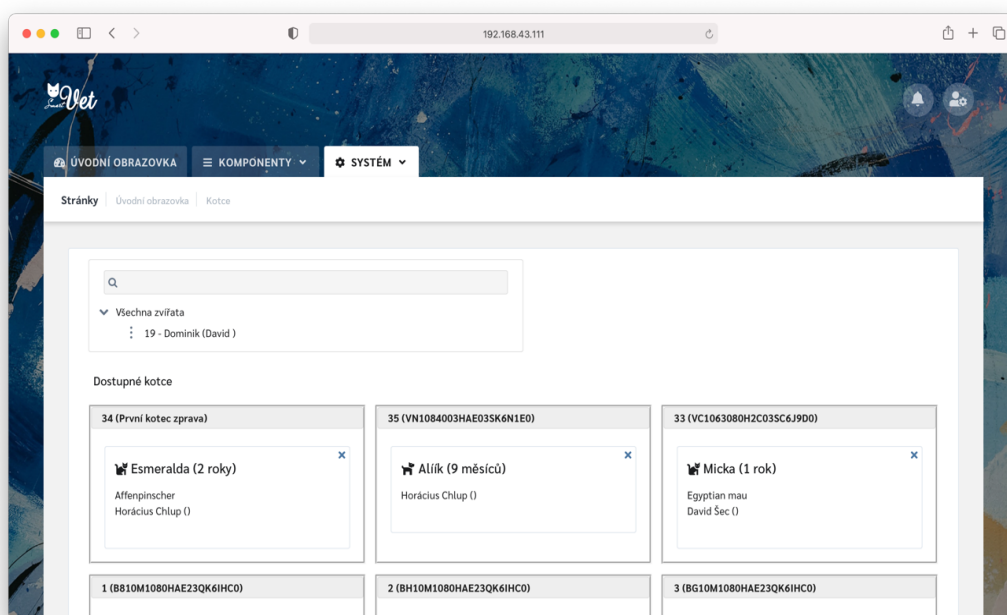
9.4 Mapování naměřených dat

Druhým důležitým kokem bylo zajistit způsob mapování naměřených dat z jednotlivých měřících stanic na konkrétní zvířata takovým způsobem, aby bylo zajištěno, že data

z jedné konkrétní měřicí stanice budou v definovaném čase přiřazena vždy pouze jednomu zvířeti. Mimo jiné tak bylo nezbytné vytvořit takové uživatelské rozhraní, které by bylo maximálně intuitivní a jednoduché na obsluhu, tak aby jednotlivý zdravotní personál, který se navíc v průběhu dne může měnit, mohl efektivně pracovat se systémem bez složité koordinace jednotlivých lékařských pracovníků a zároveň se zamezilo nežádoucím situacím kdy by musely být naměřené intervaly dat dodatečně přiřazovány konkrétním zvířatům.

System je navržen tak, aby odrážel fyzické podmínky a zavedené provozní postupy ve veterinárních stanicích. Jednotlivé kotce, jakožto potenciální prostory pro umístění měřících zařízení, jsou statické. Na druhé straně jednotlivá zvířata mohou být umísťována do kotců pravidelně, a to i opakovaně několikrát v průběhu dne. Zároveň zde není žádný předpoklad, že by bylo jedno zvíře umísťováno vždy do stejného kotce. Tento dynamický průběh je v systému zohledněn takovým způsobem, že jednotlivá měřicí zařízení jsou ve všech kotcích trvale zapnutá a nepřetržitě aktivní, nicméně naměřená data jsou zpracovávána a ukládána až v okamžiku, kdy je zvíře umístěno do kotce. Odpadá tak nutnost uvádět před začátkem měření všechny senzory do aktivního stavu.

V rámci celého systému je každý kotec jednoznačně identifikován pomocí unikátního identifikátoru. Tento identifikátor je definován buď hardwarovým ID daného zařízení, případně je automaticky vygenerováno v prvotní fázích konfigurace daného zařízení. Do systému je zařízení automaticky přidáno v okamžiku, kdy z daného zařízení začnou přicházet první data na edge node, který v případě detekce příchozích dat z nového zařízení toto zařízení automaticky začlení do systému. Tímto způsobem je zajištěno jednoduché přidávání nově připojených zařízení do systému, aniž by byla nezbytná jejich složitá a zdlouhavá instalace. Jednotlivá zařízení lze rovněž jednoduchým způsobem přejmenovat pomocí alternativního názvu (aliasu), přičemž je v aplikaci tento alias zobrazen na místě původního ID. Obrázek 17 zobrazuje dostupná zařízení spolu s aktuálním zvířetem ke kterému jsou data mapována. U právního kotce lze vidět změnu názvu zařízení, u ostatních je ponecháno původní označení v podobě hardwarového id zařízení. V horní části obrazovky se nachází seznam dostupných zvířat. Prostým přetažením daného zvířete do příslušného kotce lze zahájit měření.



Obrázek 17: Mapování dat na konkrétní zvíře – seznam dostupných zařízení; (autor)

Jediné, co je z hlediska obsluhy nutné zajistit je fyzické umístění zvířete do kotce a následně v systému prostým přetažením virtuální karty zvířete do příslušného kotce měření iniciovat. Od tohoto okamžiku jsou data ukládána a mapována konkrétnímu zvířeti. Je tak velice efektivně zajištěno, že nedojde v jeden okamžik k mapování více než jednoho zvířete na stejné zařízení. Po skončení měření již stačí zvíře z kotce jednoduše odebrat pomocí příslušné ikony v pravém horním rohu. V situaci, kdy je do virtuálního kotce umístěno zvíře, avšak v tomto kotci se již nachází jiné zvíře, dochází automaticky k odebrání původního zvířete a vložení nového. Nestane se tak, že by byla vlivem zapomenutého ukončení předchozího měření data mapována nesprávnému zvířeti.

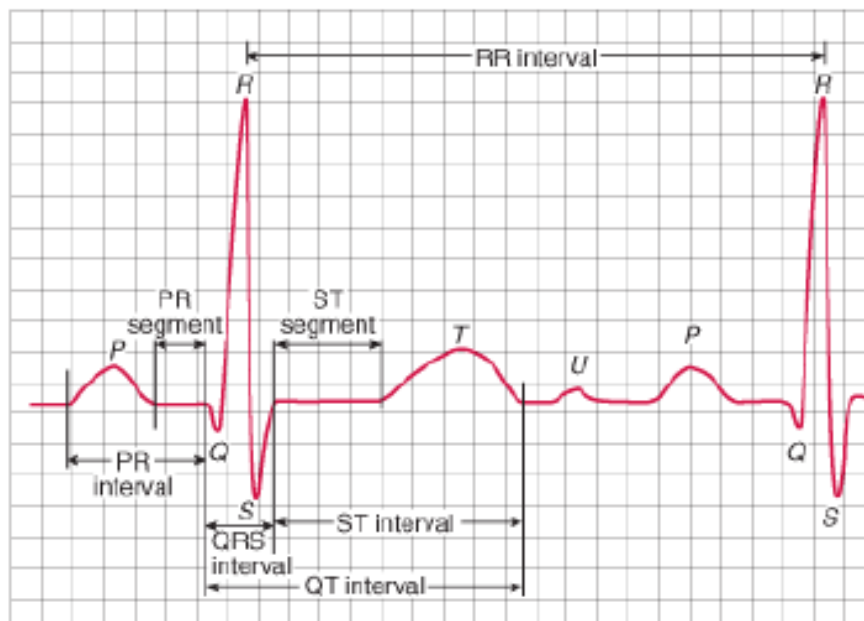
10 Možnosti využití naměřených dat

Následující sekce shrnuje některé možnosti využití naměřených dat až už se jedná o samotnou detekci vitálních funkcí, nebo popis konkrétního řešení pro detekci záchvatů u psů. Dále je v práci prezentován nově vznikající výzkum pro detekci emocí u zvířat, který využívá systém pro sběr dat, ale zároveň využívá některá již nasbíraná data v průběhu provozu systému na jednotlivých veterinárních zařízeních. Následující sekce si tak primárně neklade za cíl prezentovat konkrétní výsledky, ale ukázat potenciál možného využití dat v oblasti vědeckého výzkumu.

10.1 Vyhodnocení HR, BR, HRV

Vyhodnocení dat z akcelerometrů a gyroskopů probíhá v samostatném modulu nezávisle na zbytku aplikace. Modul zpracovává surová data ze senzorů a výsledkem je jedna hodnota HR, BR, a případně HRV za každé časové okno, nejčastěji jedna vteřina. Data ze senzorů přicházejí prostřednictvím nižších vrstev v surovém stavu tak jak byla naměřena. Úkolem vyhodnocení je rovněž tato data očistit od nežádoucích externích vlivů tak aby nedocházelo k ovlivnění výsledků měření vlivem nežádoucího rušení.

Pokud hovoříme pouze o prostém vyhodnocení tepové frekvence, tak samotný počet úderů za minutu je poměrně dobře identifikovatelný i v původním signálu. Pokud se zaměříme čistě na průběh ECG křivky dokážeme zde identifikovat jednotlivé fáze srdečního cyklu postupně popsané jako PQRST a U značící polarizaci, nebo depolarizaci jednotlivých částí srdečního svalu. Každá z těchto fází má svůj unikátní vzor a lze ji v rámci měřeného ECG signálu jednoznačně identifikovat a případně klasifikovat. Uvažujeme-li interval mezi dvěma kompletními srdečními ozvy, hovoříme o tzv. srdečním cyklu.



Obrázek 18: Znárodnění průběhu ECG křivky a jednotlivých intervalů; (převzato z Jordans et al. 2013)

Obrázek 18 znázorňuje průběh ECG křivky spolu s vyznačením jednotlivých fází a intervalů mezi nimi. Velikost jednoho dílku na ose X odpovídá 40 milisekundám, přičemž hodnota jednoho dílku na ose Y odpovídá 0,1mV. Historicky tyto hodnoty odpovídají posunu milimetrového papíru zaznamenávající průběh ECG rychlostí 25 mm/s.

P-vlna tvoří první fázi srdečního cyklu a jedná se o elektrický efekt vyvolaný prvotní depolarizací síní. Bývá zpravidla směřována nahoru a její doba odráží velikost levé síně. Obvyklá amplitudy P vlny dosahují okolo 0,25mV a doba trvání zpravidla nepřesáhne 0,11s. Neobvykle vysoké hodnoty amplitudy případně delší doby trvání P vlny někdy doprovázené jejím zdvojením mohou poukazovat na zvětšení síní.

QRS-komplex tvoří kombinaci tří vln Q R a S. První Q vlna je první negativní kmit. Tento kmit rovněž nemusí být vždy v ECG signálu přítomen. Následuje R kmit, který se ECG v signálu vyznačuje vysokou amplitudou s typickou hodnotou v rozmezí 0,5mV až 1mV. Přesná hodnota amplitudy a stejně tak doba trvání R vlny se však může lišit na základě mnoha faktorů jako je změny srdeční frekvence, s přibývajícím věkem, nebo vlivem nerovnováhy elektrolytů v těle. Délka trvání se měří typicky od začátku QRS komplexu po vrchol amplitudy R vlny a zpravidla dosahuje doby kratší než 100 milisekund a výchylka na ose Y dosahuje typicky hodnot okolo 10 mV (Wagner a Strauss

2014). R vlnu následuje negativní výchylka označovaná jako S vlna. Tato vlna je zpravidla s nižší amplitudou, než R vlna představuje depolarizaci srdeční přepážky a začátek aktivace levé a pravé komory. Amplituda i doba trvání vlny S se opět může lišit v závislosti na velikosti a orientaci srdce, ale také na poloze elektrod, nebo aktuální zdravotní kondici. Doba trvání S vlny zpravidla dosahuje okolo 80 milisekund. Nezvykle vysoké hodnoty amplitudy, nebo neobvykle dlouhé doby trvání S vlny mohou naznačovat výskyt srdečních poruch jako je hypertrofie pravé srdeční komory nebo blokáda pravého raménka.

ST segment je zpravidla vodorovný interval od konce komorového komplexu QRS a začátkem vlny T. Tento segment reprezentuje časový úsek, kdy jsou komory depolarizovány a opět re polarizovány. Typická doba trvání ST segmentu nepřesáhne 120ms. V této fázi neodchází k žádné eklektickým změnám, proto je se tato fáze vyznačuje konstantní úrovní napětí měřitelného na svodových elektrodách. Nezvyklý pokles napětí může opět naznačovat problémy s prokrvením srdce, jako je například infarkt myokardu nebo ischemie.

Poslední **T vlna** je závěrečnou fází srdečního cyklu a představuje repolarizaci komor. Vlna má obecně stejnou polaritu jako QRS komplex a typická hodnota amplitudy nepřesahuje 0,5mV. Její tvar bývá zpravidla symetrický kopulovitý s dobou trvání do 200ms. Abnormality ve vlně T mohou být rovněž způsobeny řadou srdečních stavů, včetně nerovnováhy elektrolytů, ischemie nebo infarktu myokardu, toxicity léků nebo různých genetických a získaných poruch. Například invertovaná vlna T na hrudních svodech může být známkou ischémie nebo infarktu myokardu, zatímco vrcholová nebo vysoká vlna T může být známkou hyperkalémie (zvýšené hladiny draslíku v krvi). Velikost amplitudy T vlny se rovněž může měnit v závislosti na věku, pohlaví, nebo aktuálnímu zdravotnímu stavu (Yan et al. 2006).

I když jsme právě popsali kompletní jednu fázi srdečního cyklu vyplatí se zmínit některé další intervaly, které nám napoví další užitečné informace pro vyhodnocení srdeční, anebo dechové aktivity. Jedním z takových je **QT interval** je označující začátek QRS intervalu a konec T vlny. Tento interval odpovídá celkové depolarizaci a opětovné repolarizaci komorové svaloviny. Tato doba se obvykle měří v sekundách a typické

hodnoty jsou mezi 0,25s a 0,50s a interval odpovídá jedné systole (stažení) srdeční svaloviny.

Dalším nezbytným intervalem pro výpočet Tepové frekvence je **RR interval**. Jedná se o časový úsek mezi dvěma maximy QRS komplexu. Díky jeho snadné detekci v měřeném signálu lze interval použít pro výpočet tepové frekvence, kdy lze jednoduše měřit dobu trvání dvou po sobě následujících RR intervalů, kterou následně využijeme pro výpočet tepové frekvence. RR intervaly lze rovněž využít jako indikátor pravidelnosti srdečního tepu. Pokud jsou intervaly mezi R vlnami konstantní, můžeme srdeční rytmus označit za pravidelný, pokud jsou však výrazné odchylky v naměřených RR intervalech hovoříme o nepravidelném srdečním rytmu. Abnormality mohou být způsobeny různými srdečními poruchami jako je fibrilace síní, nebo předčasné komorové kontrakce, ale jsou rovněž součástí přirozených fyziologických procesů a jejich dlouhodobé sledování může představovat užitečný nástroj pro detekci a monitorování těchto stavů, nebo jako nástroj pro posouzení účinnosti léčby.

RR intervaly lze využít nejen k určení srdeční frekvence, ale také k výpočtu frekvence dýchání. Při nádechu se srdeční frekvence obvykle zvyšuje a při výdechu se srdeční frekvence naopak snižuje. Tato změna srdeční frekvence je známá jako respirační sinusová arytmie (RSA). RSA je způsobena změnami nitrohručního tlaku, ke kterým dochází při dýchání a které ovlivňují plnění a vyprazdňování srdce. Analýzou změn v intervalu RR v průběhu času je možné odhadnout i dechovou frekvenci.

Je však důležité zmínit, že existují další faktory, které mohou interval RR ovlivnit, jako je fyzická aktivita, stres nebo podávaná medikace. Proto je důležité interpretovat RR interval v kontextu dalších klinických informací a používat jej ve spojení s dalšími fyziologickými parametry při monitorování srdeční a dechové frekvence.

V souvislosti se stresem bylo rovněž provedeno několik studií zmiňujících závislost délky RR intervalu na aktuálním emočním rozpoložení. Tomuto tématu však bude věnována samostatná kapitola.

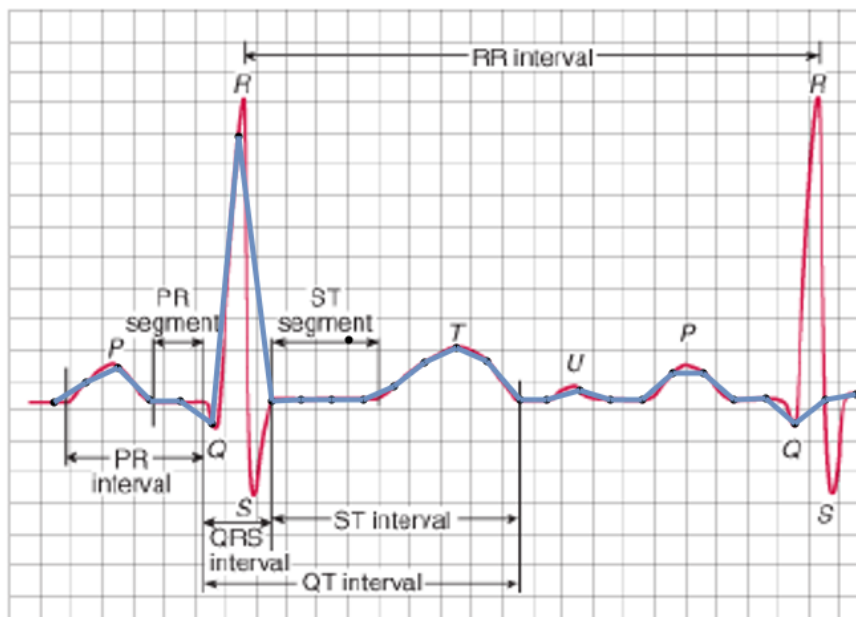
Pro výpočet HR a BR byly využity signály ze dvou různých senzorů. Nejprve byly pro měření využity akcelerometry připevněné na obojku zvířete, jedná se tedy o podobnou technologii měření jako využívají již představené projekty PetPace a FitBark, rozdíl byl ve snímkovacích frekvencích, které jsou několikanásobně vyšší. V tomto konkrétním

případě byla jednotlivá měření snímkována s hodnotou 100 Hz. Tato frekvence byla stanovena jako ideální na základě požadavků na přesnost a tvaru signálu nezbytného pro zachycení detailního průběhu srdečních cyklů.

Minimální snímkovácí frekvence vychází z principů Nyquist-Shannonova teorému, který říká, že pro zachycení průběhu signálu o určité frekvenci potřebujeme snímkovat frekvencí minimálně dvakrát vyšší, než je frekvence měřeného signálu. Tento teorém však hovoří o periodickém signálu o konstantní frekvenci. U neperiodických signálů jsou často potřeba frekvence ještě vyšší v závislosti na povaze měřených dat.

Určit minimální snímkovácí frekvenci můžeme prostým posouzením povahy měřeného signálu. V úvodu kapitoly bylo zmíněno, že jednomu dílku na ose X odpovídá časový interval 40ms. Pro zachycení jedné hodnoty v každém dílku by tak teoreticky stačila frekvence 25 Hz. Pohled na Obrázek 19 však naznačí, že takto zvolená snímkovácí frekvence je příliš nízká na to, aby dokázala zachytit všechny vlny v měřeném signálu.

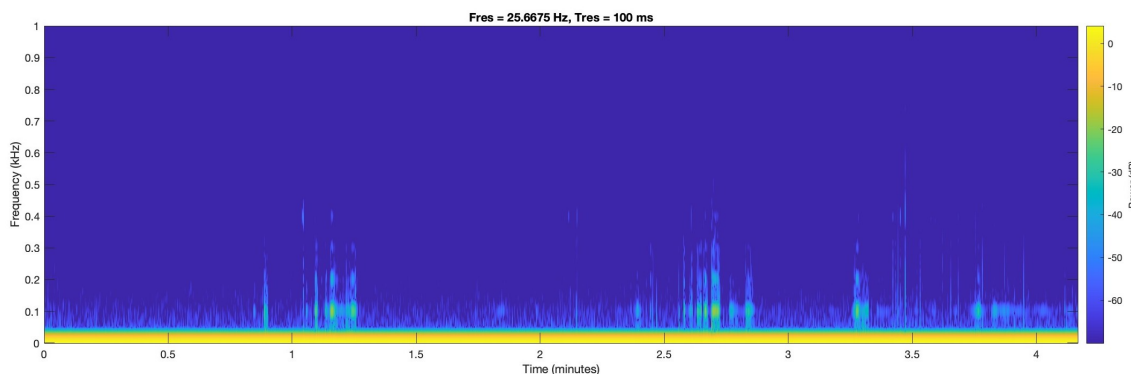
Na Obrázku 19 jsou znázorněny dva signály. Původní signál je znázorněn červeně a modře je znázorněn signál snímkaný nedostatečnou snímkovácí frekvencí o frekvenci 1 snímek na dílek tedy 25 Hz. Zatímco vlny P a T, které mají delší dobu trvání jsou v signálu zřetelně rozpoznatelné, tak rychlejší změny v podobě QRS intervalu jsou značně zkreslené co do tvaru i amplitudy měřeného signálu, případně vlivem nízké snímkovácí frekvence kompletně zaniknou. Přičemž právě správné zachycení QRS intervalu je pro nás klíčovou informací pro detekci HR. Stejně tak pro přesné určení HRV je nezbytné správně identifikovat vrchol R vlny a následně určit velikost RR intervalu. Nesprávná volba snímkovácí frekvence tak může vést ke značným chybám při určování délky jednotlivých intervalů. Budeme-li uvažovat maximální chybu měření velikost $\frac{1}{2}$ díku, tak teoretická chyba měření délky intervalu může v takovém případě dosahovat až $\pm 20\text{ms}$.



Obrázek 19: Definování minimální snímkovací frekvence ECG signálů; ; (převzato z Jordans et al. 2013) upraveno

Pro prostou detekci všech vln je proto nezbytné snímkovací frekvenci minimálně zdvojnásobit, pro zachycení alespoň základního tvaru QRS vlny se pak jeví jako ideální právě snímkovací frekvence každých 10ms (100 Hz).

Obdobných předpokladů pro měření dosáhneme, pokud rozložíme křivku EKG na jednotlivé harmonické frekvence. Následně můžeme Nyquist-Shannonův teorém aplikovat na nejvyšší složku obsaženou v měřeném signálu. Obrázek 20 znázorňuje spektrogram vybraného pětiminutového úseku dat. Letmý pohled na spektrogram naznačuje dominantní frekvence do 50 Hz. Na spektrogramu lze rovněž spatřit úseky s výrazně vyšší frekvencí, které se navíc v pravidelných intervalech opakují.

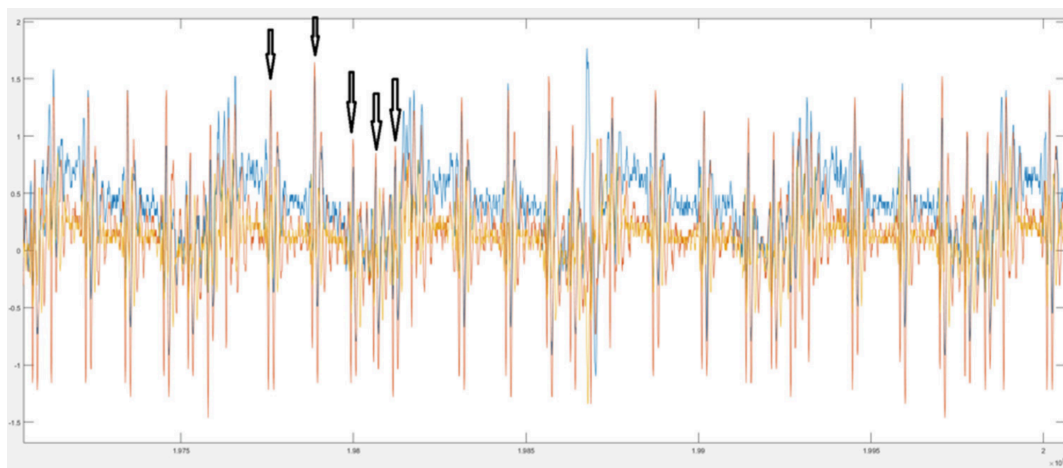


Obrázek 20: Ukázka spektrogramu měřeného signálu; (autor)

Tyto vzory mohou být způsobeny prostým šumem z okolního prostředí, ale také se může jednat o vibrace vyvolané svalovou aktivitou, jako reakce na vnější podněty. Těmi mohou být například bolest, nebo reakce na medikaci. Jedná se tak o jednu z dalších potenciálních oblastí pro zaměření navazujícího výzkumu.

Samotné řešení výpočtu HR a BR bylo publikováno v publikaci (Sec et al. 2018b) kde byl výpočet zmíněn v souvislosti s detekcí záchvatů. Pro výpočet byl použit algoritmus vycházející z řešení (Holderith a Schanze 2018; Fujii et al. 2013) a využívá autokorelaci měřeného signálu k extrakci variability. Ačkoli tato metoda částečně připomíná rozpoznávání vzorů, zaměřuje se pouze na časovou bázi signálu a zanedbává drobné variace, což je ideální pro náš případ. Analogický postup lze použít rovněž při extrakci informací o dýchání, ale je nutné očistit vstupní signál pomocí příslušných frekvenčních filtrů od složek souvisejících se srdeční činností.

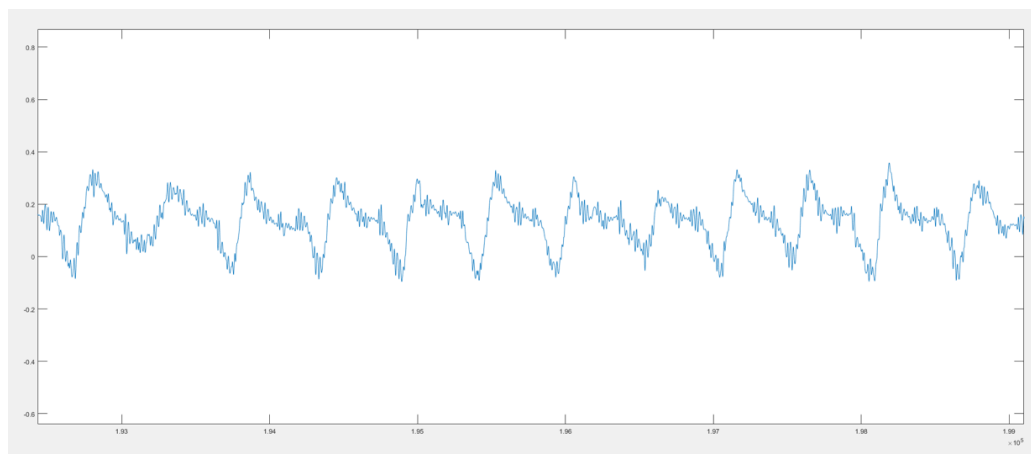
Na Obrázek 21 je znázorněn původní nijak neupravovaný signál naměřený pomocí tříosého gyroskopu na krku německého ovčáka o stáří cca 1 roku.



Obrázek 21: Vizualizace naměřeného signálu; převzato z (Sec et al. 2018b)

Již prostým pozorováním průběhu měřeného signálu lze poměrně přesně identifikovat jednotlivé údery srdce. Tyto údery jsou charakterizovány určitými vlnami známými jako balistokardiografické vlny, které jsou tvořeny jako mechanická reakce na vyvolaná pohyby krve ve velkých tepnách jako důsledek srdeční aktivity.

Další zajímavostí, která lze u konkrétního psa pozorovat je určitý typ arytmie, kdy se vzdálenost jednotlivých tepů periodicky mění tak, že vzdálenost mezi jednotlivými údery srdce roste a následně opět klesá. Tento jev je známý jako sinusová respirační arytmie a je způsoben změnami vzorců dýchání. Sinusová respirační arytmie je však u mladých jedinců poměrně běžným a přirozeným jevem, který pro psa nepředstavuje žádná zdravotní rizika.



Obrázek 22: Křivka dýchání; převzato z (Sec et al. 2018b)

Obrázek 22 znázorňuje křivku dýchání vyextrahovanou z původního signálu s použitím nízkofrekvenčního filtru. Tento filtr odstraňuje nežádoucí vysokofrekvenční šum a případné další artefakty, které mohou být přítomny v nezpracovaných datech. Následně jsou z křivky extrahovány data za pomoci autokorelace. Jedná se o statistickou techniku, kdy je podobnost signálu porovnávána se zpožděnou verzí stejného signálu. Pomocí této techniky lze poměrně přesně určit dechovou frekvenci zvířete až na jednotlivé nádechy.

Přesné měření frekvence dýchání pomocí autokorelace má rovněž potenciál pro širší uplatnění, včetně diagnostiky a léčby respiračních onemocnění, sledování zdravotního stavu zvířat, a dokonce i při vývoji nových zdravotnických prostředků.

Bylo to ověřeno, že data z tříosého gyroskopu o dostatečné frekvenci mohou poskytovat relevantní výsledky při měření dechové a tepové frekvence mají potenciál být cenným nástrojem při sledování zdraví zvířat. Stejný postup měření byl proto následně použit při zjišťování nástupu záchvatů nebo nepravidelnosti srdečního rytmu u projektu popsáném v Kapitole 10.3 pro měření epileptických záchvatů u psů.

Později byly způsoby měření rozšířeny o speciální podložky se zabudovanými tenzometry. U těchto podložek je maximální snímkovací frekvence zvýšena až na 1000 Hz s cílem získat detailní informace o jednotlivých srdečních cyklech, které umožní detekovat i drobné změny v srdeční aktivitě. Použití tohoto řešení pro výpočet dechové a tepové frekvence bylo následně patentováno.

Zároveň se jedná o oblast s vysokým potenciálem pro možné další využití naměřených data rozšíření výzkumu, zejména pak dalšího porozumění daných technik a jejich následnou aplikaci tak aby mohli přispět rozvoji monitorování poruch respiračních funkcí u lidí i zvířat.

10.2 Detekce emocí

Další z oblastí výzkumu bylo využití systému pro detekci emocí u zvířat. Tento výzkum si kladl za cíl zlepšení životních podmínek zvířat, a to nejen těch domácích, ale zejména hospodářských zvířat chovaných na velkofarmách, kde často nebývá psychické pohodě zvířat věnováno zdaleka tolik pozornosti. Nicméně lze předpokládat, že s rozšiřujícím se povědomím o problematice zlepšování psychické pohody zvířat bude v blízké budoucnosti této problematice věnováno mnohem více pozornosti nejen z pohledu širší veřejnosti, ale také provozovatelů podobných zařízení jakožto reakce trhu na rostoucí poptávku po kvalitnějších potravinách produkovaných těmito zvířaty. Hlavní idea systému spolu s dílčími výsledky byly publikovány v (Sec a Mikulecky 2023), ale vzhledem k rozsáhlosti dané problematiky lze předpokládat pokračování výzkumu i v nadcházejícím období.

Pro uvedení čtenáře do dané problematiky asi není nutné dlouze vysvětlovat, že nejen lidé jsou schopni prožívat emoce, ale ve skutečnosti jsou i zvířata schopna vyjadřovat řadu nejrůznějších emocí. Jako zásadní průlom ve studiu emocí u lidí i zvířat je považována práce Charlese Darwina (Darwin 1872), která pomohla definovat jednotlivé pohledy na univerzálnost emocionálních projevů a jejich evoluční původ. Darwin zde publikoval základní myšlenku, že zvířata jsou schopna vyjadřovat emoce podobným způsobem jako lidé. Darwin rovněž věřil, že emoce se u živých organismů vyvinuli v průběhu času jako evoluční adaptace a pomáhala tak organismům reagovat na nejrůznější situace. Darwin rovněž ve své knize popisuje, že emoce rovněž mohou být vyjadřovány prostřednictvím

nejrůznějších neverbálních podnětů, jako jsou výrazy obličeje, řeč těla a různé hlasové projevy a hrají klíčovou roli pro jejich přežití a zkoumal různé emoce, včetně radosti, strachu, hněvu, smutku a překvapení, a následně popisoval jejich projevy u lidí i zvířat. Zkoumal také příčiny emocionálních projevů, jako jsou sociální a environmentální faktory.

Důkazem toho, že zvířata jsou schopna vyjadřovat širokou škálu emocí může být nejen řada vědeckých studií provedená v pozdějších letech, namátkou lze uvést například (Bekoff 2000; Bliss-Moreau a Rudebeck 2021; Feighelstein 2021; Kremer et al. 2020; Morozov et al. 2021; Paul et al. 2020), ale v neposlední řadě také zkušenosti snad každého chovatele domácích mazlíčků, ale také chovatelů hospodářských i exotických druhů zvířat. Důkazem může být rovněž i prostý fakt, že zvíře dokáže určitým způsobem reagovat na prostou přítomnost svého majitele v jeho blízkosti. V důsledku toho roste zájem o pochopení emocí zvířat, a to nejen pro vědecké účely, ale i nejrůznějších institucí zabývajících se podporou zlepšení životních podmínek zvířat.

Jedním z klíčových aspektů pro zlepšení životních podmínek zvířat je sledování jejich základních životních funkcí včetně srdeční frekvence, dýchání a teploty ze kterých lze následně vyhodnocovat aktuální zdravotní stav a identifikovat případné zdravotní problémy. Dále můžeme najít celou řadu studií využívající těchto dat k identifikaci emočního stavu zvířete. Závěry těchto studií se shodují na tom, že změny srdeční frekvence a dýchání mohou u zvířat indikovat stres, úzkost, nebo vzrušení. Rovněž můžeme najít i studie zaměřené na detekci obličeje zvířete, který v kombinaci s umělou inteligencí dokáže poskytnou vodítka pro určení aktuálního emočního stavu snímaného zvířete.

Detekce emocí u zvířat tak může pomoci identifikovat, jakým způsobem mohou různé externí faktory ovlivnit emoce u zvířat. Následným zkoumáním těchto reakcí zvířat na okolní prostředí lze využít k vytvoření optimálních životních podmínek nejen domácích mazlíčků, ale podobné informace lze využít rovněž na farmách, nebo zoologických zahradách. Zlepšováním životních podmínek lze rovněž předcházet nežádoucímu chování a zdravotním problémům. Rovněž je dokázáno, že zvířata dlouhodobě vystavovaná chronickému stresu mohou být náchylnější k rozvoji zdravotních problémů jako jsou kardiovaskulární onemocnění nebo oslabený imunitní systém (Moberg a Mench

2000; Sherwen a Hemsworth 2019). Eliminací některých nežádoucích jevů tak lze nejen zlepšit životní podmínky zvířat, ale také ušetřit značné náklady na dlouhodobou zdravotní péči.

10.2.1 Způsoby detekce emocí

Jedním ze způsobů, jak lze účinně detekovat emoce u zvířat je monitorováním variability srdečního tepu (HRV). Mnoho předchozích výzkumů prokázalo korelaci mezi HRV a emocemi nejen u zvířat, ale také u lidí (Bekoff 2000; Feighelstein 2021; Neethirajan 2022; Paul et al. 2020). Řada z nich využívá k detekci emocí různé techniky, nicméně všechny výše uvedené studie dospívají k závěru, že emocionální změny u zvířat mohou rovněž vést k měřitelným změnám HRV. Zatímco u lidí lze výzkum emocí podpořit i dalšími způsoby jako je například dotazníkové šetření u zvířat lze spoléhat ryze na reakce nervového systému, případně na drobné změny v chování, které však nemusí být vždy spolehlivě rozpoznatelné, případně správně interpretovány.

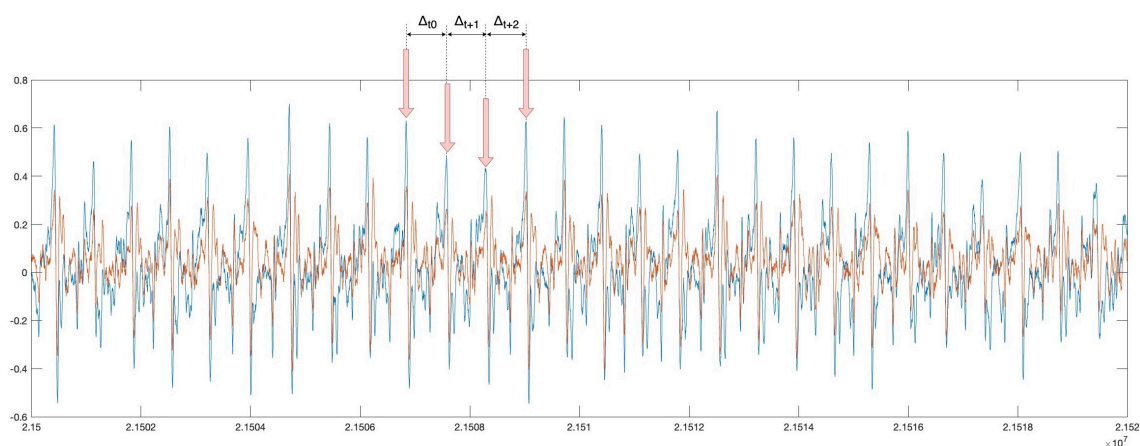
Jak již bylo zmíněno výše, HRV tvoří jeden z klíčových ukazatelů pro detekci emocí, protože je ovlivňován a regulován autonomním nervovým systémem (ANS). V ANS lze identifikovat dvě různé větve, sympathetic nervous system (SNS) dále jen symaptikum a parasympathetic nervous system (PNS) dále označené jako prarsymaptikum, ale stejně tak se lze pro prarsymaptikum setkat s pojmem vagu. Zatímco SNS je zodpovědná za reakce typu „bojuj, nebo uteč“, druhá PNS větev zodpovídá za reakce „odpočinek a trávení“.

Pokud je zvíře vystaveno určité intenzivní aktivitě, nebo stresovým situacím, jako je strach nebo vzrušení, vede tato změna k odpovídající akci ve změně aktivity ANS, která následně vyvolá odpovídající změnu v HRV. V tomto případě dochází k poklesu HRV oproti normálu. Například u bojácných zvířat můžeme pozorovat nižší hodnotu HRV v důsledku zvýšené aktivity SNS. Naopak pozitivní emoce mají často za následek zvýšení HRV v důsledku převládající PNS aktivity. Tento fakt rovněž potvrzuje řada praktických studií (Hachenberger et al. 2023; Kok et al. 2013; Kremer et al. 2020) věnovaných zkoumání vlivu emocí na změny HRV pro detekci emocí nejrůznějších druhů zvířat včetně psů, koček, koní případně ovcí. Příkladem může být rovněž studie (Gehrke et al. 2011) zkoumající změny HRV v průběhu terapie. Tyto informace byly následně

zpětně využity pro zhodnocení efektivity poskytované léčby a případnému dalšímu přizpůsobení terapeutického přístupu.

Pro identifikaci variability srdečního tepu v ECG signálu byl proveden výpočet lokálního maxima pro detekci R vlny v měřeném signálu podle algoritmu popsáném v předchozí kapitole. Jak již bylo zmíněno v předchozí kapitole R vlna tvoří nejvyšší vrchol v QRS komplexu a lze ji tak jednoduše využít k detekci doby trvání kompletního srdečního cyklu.

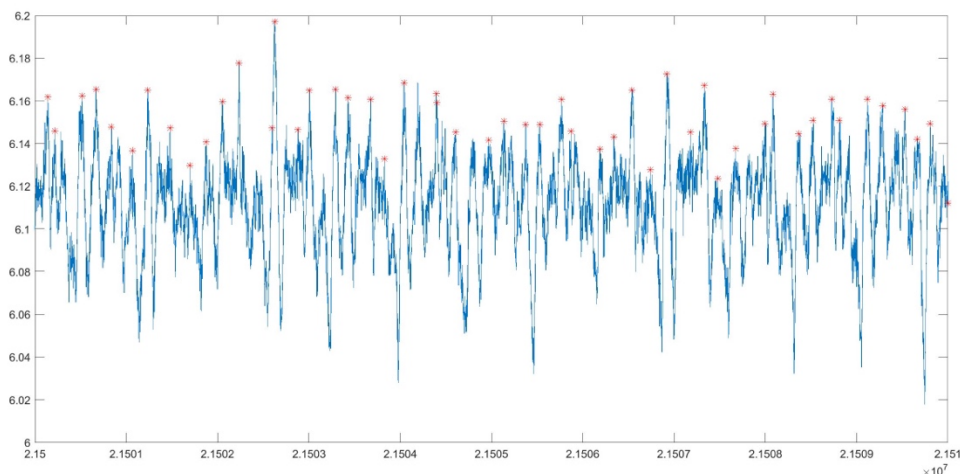
Následně jsou identifikovány jednotlivé intervaly mezi po sobě následujícími R vlnami a podle časových značek vypočítány doby trvání těchto intervalů, dále označené jako velikost intervalu RR. Obrázek 23 popisuje proces detekce vrcholu R vlny nejprve metodou vizuálního hledání lokálního maxima a následný Obrázek 24 znázorňuje automatickou detekci jednotlivých RR intervalů v měřeném signálu pomocí algoritmu. Červené značky představují jednotlivé srdeční cykly. Na ose X jsou znázorněna čísla vzorků a na ose Y je následně znázorněn průběh měřeného napětí na tenzometru se snímkovací frekvencí 1000 Hz.



Obrázek 23: Graf znázornění RR intervalů pro výpočet HRV; (autor)

Jednotlivé RR intervaly jsou následně využity k výpočtu časových a frekvenčních měření HRV, jako je standardní odchylka NN (R-R) intervalů (SDNN), další často využívané technikou pro měření časových řad je střední kvadrát kořenů rozdílů dvou následujících RR intervalů (RMSSD - Root Mean Square of Successive Differences), nebo výkonová spektrální hustota (PSD) HRV v různých frekvenčních pásmech jako nízká frekvence

(LF), vysoká frekvence (HF), nebo velmi nízká frekvence (VLF). Detailní přehled dostupných metod poskytuje publikace (Shaffer a Ginsberg 2017). Extrahované vlastnosti jsou následně analyzovány tak, aby mohly být identifikovány klíčové vlastnosti pro detekci emocí. Toho lze dosáhnout použitím celé řady statistických metod, jako je korelační analýza nebo algoritmy výběru vlastností s využitím modelů strojového učení.



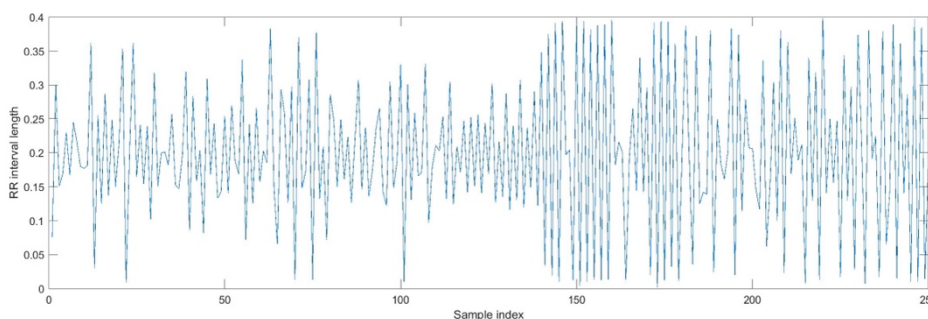
Obrázek 24: Detekce RR intervalů v měřeném signálu (autor)

10.2.2 Statistické analýzy HRV

Statistickou analýzu měřeného HRV signálu můžeme rozlišovat na dva základní způsoby. Prvním ze způsobů je analýza podle času (Time domain analysis) jejímž základním smyslem je identifikovat časové polohy QRS komplexů, z nichž se následně určí pozice jednotlivých RR intervalů. Identifikace RR intervalů znázorňuje Obrázek 24 z jednotlivých časových značek je následně je spočítána délka jednotlivých intervalů jako časový rozdíl mezi dvěma po sobě jdoucími srdečními tepy. Tento interval se obvykle měří v milisekundách a dosahuje obvyklých hodnot v řádů stovek, až tisíce milisekund. Rovněž je vhodné z dalšího zpracování vyloučit příliš krátké, nebo naopak příliš dlouhé intervaly, které zde mohou nastat z důvodu nežádoucích interferencí vnějšího prostředí, případně v důsledku výpadků měření, nebo chybné (ne)identifikace následující R vlny, které se může negativně projevit v podobě příliš dlouhých intervalů. Volbu těchto hranic pro vyloučení intervalů je však nutné provádět s notnou obezřetností, protože samotná délka intervalů je zároveň ukazatelem pro rozlišení sympatické (SNS) a parasympatické

(PNS) a může se značně lišit u rozdílných druhů zvířat. Proto je vhodné tyto hranice posuzovat vždy individuálně na základě předchozí analýzy.

Samotné zpracování pomocí časové analýzy můžeme dále rozdělit na statistické a goniometrické metody. Zatímco statistická metoda analýzy je založena na klasických statistických aparátech jako je průměr směrodatná odchylka, případně odmocnina průměru druhých mocnin, tak geometrická analýza využívá grafické znázornění RR intervalů například formou histogramů a dokáže tak poskytnout rychlý náhled na aktuální rozložení délek intervalů. Příkladem může být prosté zobrazení délek intervalů v čase, nebo formou histogramu.

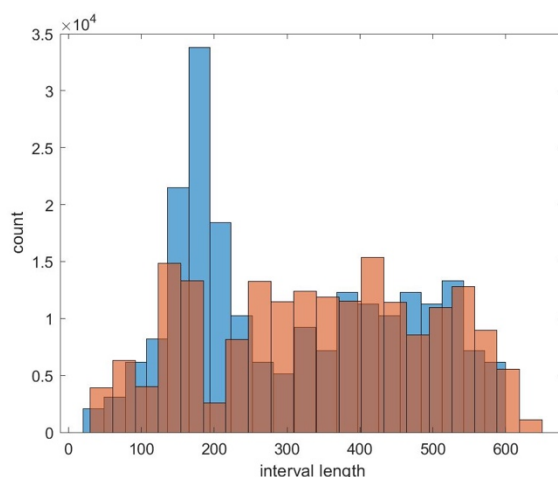


Obrázek 25: Graf délek RR intervalů; (autor)

Obrázek 25 poskytuje znázornění délek jednotlivých RR intervalů v čase. Na ose X je znázorněno číslo vzorku a na ose Y je vynesena délka RR intervalu.

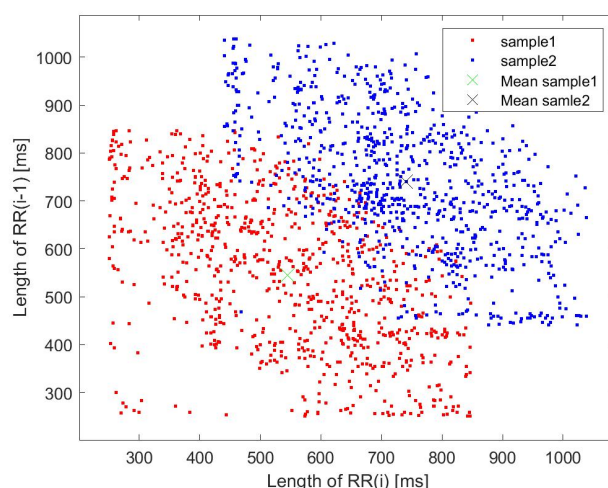
Pro vyhodnocení histogramu mohou být použity tři základní metody, jako je posouzení rozptylu variability srdečního rytmu. Posuzovat lze variabilitu mezi jednotlivými hodnotami a jejich rozptýlení v rámci histogramu. Například může se vyhodnocovat šířka histogramového sloupce nebo směrodatná odchylka hodnot v jednotlivých částech histogramu. Posouzení rozptylu pomáhá identifikovat rozdíly mezi různými kategoriemi HRV. Druhou možností je interpolace histogramu určitým geometrickým tvarem, nejčastěji se jedná trojúhelník, a v následné analýze se již využijí parametry tohoto aproximovaného tvaru, např. trojúhelníkový index. Poslední možností je rozdělení histogramu podle tvaru do několika kategorií, přičemž každé kategorii následně odpovídá určitá třída HRV. Obrázek 26 poskytuje porovnání dvou měřených vzorků signálu stejného zvířete (pes; německý ovčák 8 let) s odstupem času 1 hodiny při různých aktivitách. Modře vyznačený histogram znázorňuje měření bez přítomnosti majitele

a červený histogram značí měření při kterém byl majitel zvířete přítomen v po celý průběh měření. Z grafu je patrné, že pouhá přítomnost majitele může výrazně ovlivnit variabilitu srdeční frekvence potažmo i emoční stav zvířete. Tato hypotéza bude rovněž ověřena ve statistické části.



Obrázek 26: Histogram porovnání četností délek intervalů dvou signálů; (autor)

Další možností, jak lze pomocí grafického znázornění zkoumat variabilitu srdeční frekvence poskytuje nelineární analýza. Non-lineární zobrazení se zaměřují na zobrazení rozdílu po sobě následujících RR pomocí vynesení bodů, z nichž každý jeden odpovídá rozdílu dvou po sobě následujících RR. Výsledným grafem tedy není spojitá křivka, nebo přímka, ale shluk nespojitých bodů. Poincarého (někdy také Lorenzův) graf, který zobrazuje závislost každého RR intervalu na intervalu předcházejícím. Kvalitativní zhodnocení výsledného obrazce lze provést několika způsoby, nejčastěji se využívá aproximace výsledného tvaru elipsou, přičemž rozhodující je velikost obrazce v podélné i kolmé rovině na osu identity, ale také pozice středu elipsy vůči počátku souřadnicového systému. Hlavní výhodou použití Poincarého zobrazení je, že tato metoda je nenáročná na implementaci, ale zároveň velice názorná pro vizualizaci změn v rozložení vzdáleností. Kratší vzdálenosti RR intervalů se projeví zobrazením blíže středu, zatímco delší vzdálenosti RR intervalů budou rozesety dále od středu pomyslné elipsy. Následující Obrázek 27 zachycuje porovnání obou měření z předchozího příkladu. Za povšimnutí stojí, že zatímco plocha mapy je téměř totožná, změnila se délka RR intervalu, čímž došlo k posunu obrazce ve směru osy identity směrem vzhůru.



Obrázek 27: Poincarého graf – porovnání vzorků; (autor)

Statistická zpracování časových řad zahrnuje použití nejrůznějších statistických metod sloužících ke zkoumání a extrakci relevantních informací z měřeného HRV za pomoci klasické popisné statistiky jako je průměr, průměr, směrodatná odchylka, minimum, maximum nebo jednotlivé kvartily, ale také analýzu časových oblastí zahrnujících výpočty jednotlivých parametrů HRV na základě několika po sobě jdoucích intervalů.

Běžné měření v časové oblasti pro HRV zahrnuje parametry jako je průměrná délka RR intervalu, směrodatná odchylka intervalů RR (SDNN) a případně druhou odmocninu z násobků po sobě jdoucích rozdílů (RMSSD) a patří mezi časové ukazatele variability srdeční frekvence. Tato zkratka je odvozena z anglického názvu „*square Root of the Mean of the Squares of the Successive Differences between adjacent RR intervals*“ a jedná se o metriku poskytující informace o celkové HRV a krátkodobých variacích. Výsledná hodnota výpočtu (Rovnice 1) je v sekundách, resp. v milisekundách a hodnoty mají zpravidla rozdělení pravděpodobnosti, které se statisticky liší od normálního rozdělení (Botek et al. 2017).

$$rMSSD = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n-1} (RR_{i+1} - RR_i)^2}$$

Rovnice 1: Vzorec pro výpočet RMSSD

Umocnění rozdílů sudou mocninou a jejich následné průměrování a opětovné odmocnění stejným exponentem (zpravidla se jedná o druhou mocninu) tak tvoří obvyklý způsob jakým lze zdůraznit sice nepatrné, ale z hlediska zpracování signálu zásadní rozdíly ve statistickém souboru čítajícím mnoho podobných hodnot. Sudý exponent mocniny zároveň poskytuje efektivní způsob, jakým lze eliminovat záporné hodnoty.

Pomocí logaritmické transformace lze dále získat odvozený vztah $\ln \text{RMSSD}$ který využívá přirozeného logaritmu pro eliminaci obrovských hodnot vlivem umocnění rozdílů. Použití přirozeného logaritmu dokáže tyto rozdíly opticky snížit a zároveň neztratit jejich význam. Výsledek nabývá řádů jednotek sekund a výsledek se obvykle statisticky významně neliší od normálního rozdělení. To nám umožní využití parametrických testů, které jsou zpravidla jednodušší a při znalosti konkrétního rozdělení také poskytují mnohem přesnější výsledky (Hopkins et al. 2009).

Obecně platí, že nižší hodnota značí převahu sympatiku a vyšší naopak parasympatiku a vyšší rezervu vegetativního systému.

10.2.3 Frekvenční analýza HRV

Poslední možností je zpracování signálu HRV pomocí frekvenčních analýz. Ta dokáže poskytnout informace o rozložení energetických složek do různých frekvenčních pásem. Princip spočívá v převedení časového signálu, který je reprezentován jako sekvence časových intervalů mezi jednotlivými po sobě jdoucími RR intervaly do frekvenčního spektra pomocí Fourierova transformace na spektrální výkonovou hustotu (PSD).

Převodem na PSD získáme přehled o přítomných frekvenčních složkách v HRV a jejich intenzitě. Spektrální výkonová hustota je typicky rozdělena do několika frekvenčních pásem, která jsou běžně označována jako frekvenční složky HRV.

Výsledné frekvenční spektrum HRV lze následně rozdělit do několika frekvenčních složek (pásem), přičemž každá složka má specifický význam v kontextu autonomního nervového systému. Typickým rozdělením frekvencí je do tří základních pásem podle hraničních frekvencí. Charakteristika každého pásma je stručně popsána níže. Dále je nutné zmínit, že frekvence uvedené níže vychází ze standardizované stupnice navržené Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology (1996) a vychází z dlouhodobého zkoumání HRV u lidí.

Je však potřeba zdůraznit že vzhledem k velice odlišné fyziologii zvířat nelze chápat tyto hodnoty jako univerzálně aplikovatelné na jakoukoliv zvířecí populaci, ale je nutná tyto frekvence přizpůsobit měřenému zvířeti. Například (Carnevali et al. 2013) použil při zkoumání srdečních onemocnění u laboratorních potkanů rozdělení LF: 0,2–0,75 Hz; HF: 0,75–2,5 Hz. Pro zachování obecných standardů však budou uváděná spektra ponechána v původní podobě. Vzhledem k odlišné fyziologii zvířat jsou však tyto frekvence pouze orientační a měly by být vždy přizpůsobeny konkrétnímu zvířeti a jeho typické srdeční frekvenci. Například u dospělého velkého psa se jeví jako optimální hranice LF: 0,06 – 0,2 Hz; HF: 0,2 – 1 Hz.

Very Low Frequencies (VLF) kam spadají všechny frekvence do 0,04 Hz. Toto pásmo je dle (Blaber et al. 1995) z velké části tvořeno neperiodickými (fraktálními) signály a je proto nevhodné pro spektrální analýzu, resp. spektrální analýza dle autora neposkytuje upokojivé výsledky, protože je těžké odlišit neperiodické zdánlivě náhodné kolísání RR intervalů od okolního šumu. I přes toto tvrzení se rovněž objevují některé studie, které spojují pásmo VLF s možným ukazatelem infarktu myokardu (Bigger et al. 1992), případně (Stejskal et al. 2002) považuje poměr VLF/HF jako ukazatel poměru mezi sympatikem a parasympatikem. Většina dostupných studií, se však přiklání k faktu, že VLF spektrum je spojováno s různými fyziologickými a patologickými procesy. Studie využívající spektrální analýzu HRV a zkoumající VLF složky jsou zaměřeny na různé dlouhodobé faktory, jakými jsou například stárnutí, fyzická kondice, metabolické stavy a další. Většina závěrů však dochází ke tvrzení, že přesný význam VLF složek v HRV zatím není zcela objasněn.

Low Frequencies (LF) v mají typicky rozmezí od 0,04 do 0,15 Hz. Jednotlivé názory na interpretaci se opět mírně liší, ale převládá názor, že LF je považován za aktivitu sympatiku. Například (Malliani et al. 1991) zaznamenal zvýšené aktivity sympatiku při mentální a fyzické zátěži vyvolaly zvýšení oscilací v pásmu LF u lidí, ale také u experimentálních zvířat. (Usui a Nishida 2017) rovněž popisuje, že LF může mít spojitost s reakcemi na stresové podněty.

Oproti tomu High Frequency (HF) pásmo 0,15 – 0,4 Hz je ovlivňováno převážně parasympatickým nervovým systémem a je spojeno s dýcháním a fyziologickou regulací srdeční frekvence.

Z výše uvedených pásem lze rovněž získat další odvozené ukazatele jako je PT (Total power), který lze získat sečtením všech výkonových spekter v jednotlivých pásmech VLF + LF + HF a vyjadřuje celkovou variabilitu. Odvozené hodnoty %VLF, %LF, %HF lze následně získat jako relativní výkony vyjádřené v procentech vůči celkovému výkonu.

Analýza frekvenčního spektra HRV poskytuje kvantitativní parametry, jako jsou výkonové spektrální hustoty PSD případně poměr mezi jednotlivými frekvenčními pásmy. Tyto parametry slouží k charakterizaci autonomní regulace srdeční frekvence a mohou poskytnout informace o stavu stresu, relaxace nebo rizika kardiovaskulárních onemocnění. Zároveň je však třeba poznamenat, že neexistuje žádná jednotná norma nebo standard pro výpočet frekvenčních ukazatelů HRV. Tyto ukazatele jsou na rozdíl od tradičního zpracování časových řad více subjektivní a mohou se výrazně lišit v závislosti na použité metodě nebo konkrétním výzkumu. Vzhledem k těmto faktorům se tak tradiční statistické ukazatele stále těší vysoké popularitě, protože dokáží poskytnout lepší porovnání výsledků mezi různými výzkumy a nabízejí rámec pro objektivnější hodnocení HRV a umožňují získání komparativních dat nebo srovnání s referenčními hodnotami.

10.2.4 Potenciál pro další využití dat

Další potenciály pro využití a případné zpřesnění získaných výsledků jsou poměrně široká. Data získaná za pomoci výše popsaných metod mohou například posloužit při trénování modelu strojového učení: Model strojového učení, jako je support vector machine (SVM), neuronová síť nebo rozhodovací strom, může být trénován pomocí vytipovaných vlastností a k získaným parametrům následně přiřazeny odpovídající emocionální záznamy. Pro trénování modelu mohou být použity vypočítané variace srdečního rytmu spolu s poznámkami od lékařů, majitelů zvířat nebo chovatelů psů. S jejich spoluprací by mělo být možné identifikovat skutečné emoce zvířat nebo rozsah emocí. Tato měření mohou poskytnout cenným zdrojem informací souvisejících s HRV a dále přispět k identifikaci jednotlivých emocí. Druhou možností, jakým lze rozšířit možnost detekce emocí u zvířat je rozšíření stávajících technik o měření fyziologických příznaků zvířat které by kromě detekce emocí zahrnovaly také zaznamenávání fyziologických signálů spojených s emocemi, jako je vodivost kůže a tváří nebo vokálních projevů. Tyto techniky detekce jsou však obtížně dosažitelné v domácím prostředí a jsou

svým charakterem spíše vhodnější pro lékařská zařízení nebo laboratoře specializované na dlouhodobý výzkum zvířat.

Celkově může poskytovat kombinace HRV spolu s dalšími ukazateli užitečný nástroj pro studium zvířecích emocí a pomoci upřesnit aktuální stav mysli. Tato technika nabízí neinvazivní a objektivní měření aktivity ANS, které může být přínosné pro snadnou a rychlou identifikaci emočních stavů a hodnocení účinnosti intervencí ke snížení stresu a podpoře pohody zvířat. Tato oblast tak i nadále skýtá velký potenciál pro budoucí výzkum a nabízí stále mnoho potenciálních příležitostí jak ve vědecké, tak i komerční sféře.

Jako součást navazujícího výzkumu byla rovněž publikována platforma pro (Sec a Mikulecky 2023) ve které byly představeny základní způsoby detekce emocí s využitím strojového učení a neuronových sítí pro vyhodnocení aktuálních emocí u domácích a hospodářských zvířat za účelem zajištění jejich optimálních životních podmínek a eliminace některých zdravotních problémů způsobených dlouhodobým stresem. Tato publikace prezentuje nejen možnosti využití platformy pro samotný sběr a vyhodnocení vitálních funkcí ale také jako průzkum možného využití dat pro samotnou detekci základních emočních stavů u zvířat a jejich následnou implementaci do podoby konkrétních výpočetních algoritmů. I přesto že je tento výzkum emocí u zvířat stále ještě ve velmi rané fázi a jedná se o v současnosti o velice zřídka prozkoumanou část, která však skýtá vysoký potenciál pro případný budoucí výzkum a poskytuje spoustu příležitostí k hlubšímu porozumění emocionálních projevů u zvířat, díky čemuž může přispět k zásadním změnám a rozvoji v péči o zvířata a právem si tak zaslouží si své místo v této sekci.

10.3 Detekce záchvatů

V neposlední řadě byl navržený systém využit jako platforma pro sběr informací pro vyhodnocení a predikce epileptických záchvatů u psů postižených epilepsií. Tento výzkum probíhal v letech 2017 - 2018 a jeho cílem bylo praktické zhodnocení proveditelnosti daného řešení, ověření z fyzikálního hlediska možnost získávání a vyhodnocení dat z komerčně dostupných, případně vlastních senzorů a následné vytvoření platformy pro vzdálený monitoring epileptických záchvatů u psů, který umožní

sledovat a zaznamenávat epileptické záchvaty v reálném čase a umožní tak majitelům psů, nebo veterinářům získat podrobné informace o průběhu a intenzitě záchvatu a přispět tak ke zhodnocení aktuálního stavu zvířete, případně stanovení dalšího postupu léčby tohoto onemocnění.

Epilepsie je jedním z nejčastějších chronických neurologické onemocnění postihující dle (Packer a Volk 2015) okolo 0,6 – 0,75% psů. Zároveň uvádí, že je v raných fázích velice obtížné epilepsii u psů diagnostikovat. Epilepsie je stejně jako u lidí celoživotní onemocnění a v současné době neexistuje efektivní způsob, jak tuto nemoc zcela efektivně eliminovat. K záchvatům dochází v důsledku abnormální elektrické aktivity, což vede k náhlým, ale krátkodobým změnám v chování a nekoordinovaných pohybech psa. (Licht et al. 2002) rovněž poukázal na fakt, že některá plemena mohou být mnohem náchylnější k epilepsii a jejich prevalence může být vyšší než u ostatních plemen. Epilepsie je psovi diagnostikována za předpokladu, kdy prodělá neméně dva epileptické záchvaty v rozmezí menším než 24 hodin (Packer et al. 2017b). Doba trvání záchvatů je v rozmezí řádů několika vteřin až po dobu několika minut (McGrath 2017) a dle (Chandler 2006) u většiny psů nemají záchvaty žádnou zjevně identifikovatelnou základní příčinu. Mezi nejčastější projevy epileptických záchvatů jsou ztráta dobrovolné kontroly, která je často doprovázena křečemi (otřesy nebo třesoucí se pohyby a záškuby svalů) a může být dále doprovázena i zvukovými projevy, nebo znaky agrese, případně bývá naopak pohybová aktivita výrazně utlumena. (Packer et al. 2017b) popisuje jednotlivé výskyty jako velice náhlé, přičemž projevy záchvatu jsou pokaždé téměř totožné a mají shodný klinický obraz.

Většina dostupných studií (Berendt et al. 2015; Thomas 2010; McGrath et al. 2019) identifikuje dva základní typy epileptických záchvatů určených jejich etiologií.

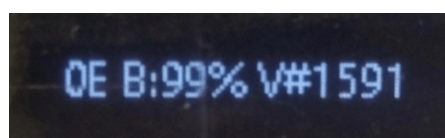
Idiopatická epilepsie (Idiopathic Epilepsy – IE), též někdy nazývána jako primární je v současnosti nejběžněji diagnostikovaným typem epilepsie. Takto diagnostikovány jsou případy, kdy nelze identifikovat žádnou základní příčinu ani specifický spouštěč. Výraz "idiopatický" se odkazuje na stav, který vzniká spontánně bez jakékoliv známé příčiny. Dle (Scorza et al., 2013) je takto diagnostikováno až 80 % všech případů. Léčba idiopatické epilepsie u psů často zahrnuje užívání antiepileptik (AED) jejichž účelem je snížení míry a frekvence záchvatů na přijatelnou úroveň.

Druhým typem epilepsie je strukturální epilepsie (Structural Epilepsy – StE), která má naopak známou příčinu spojenou se změnami v mozku jako jsou nádory, případně vrozené, nebo vývojové poruchy mozku. Tyto abnormality lze poměrně úspěšně diagnostikovat pomocí magnetické rezonance (MR), vyšetřením mozkomíšního moku, případně krevními testy. Léčba se provádí buď chirurgicky přímo odstraněním příčiny, případně pokud toto není možné je opět přistupováno k léčbě pomocí AED (De Risio a Platt 2014). Ve většině případů je však poměrně obtížné identifikovat přesnou příčinu vzniku záchvatů u psů. Včasná detekce epileptických záchvatů však může pomoci majitelům i jejich psům, aby zabránili utrpení, úrazu nebo dokonce smrti u postižených psů. Tímto způsobem může přispět k sociálnímu, emocionálnímu a fyzickému zlepšení kvality jejich života. Účelem tohoto výzkumu je tedy prozkoumat schopnosti zařízení pro snímání životních funkcí psa, která mohou pomoci včas detekovat epileptické záchvaty u psů minuty nebo hodiny před zahájením, a diskutovat o jejich výhodách a případných omezeních.

Cílem výzkum tak bylo nejen posouzení proveditelnosti daného řešení z hlediska informatiky, ale také identifikace potenciální indikátorů, které mohou pomoci s identifikací probíhajících záchvatů, nebo predikovat nadcházející záchvat. V neposlední řadě bylo také praktické zhodnocení, zda je možné celý systém provozovat na baterii bez nutnosti stálého připojení k el. síti, případně na jakou vzdálenost lze data ze sensorů přenášet tak, aby je stále bylo možné efektivně vyhodnocovat. Investorem tohoto projektu je firma NF2 s.r.o. a cílem celého projektu bylo přinést na trh řešení nebo službu, která by umožnila uživateli rozpoznat blížící se záchvat, nebo upozornit na právě probíhající záchvat.

Pro samotné snímání dat bylo po celkovém zhodnocení dostupných zařízení vybráno zařízení Metawear, které svými rozměry natolik malé, že lze umístit pod obojek zvířete, ale zároveň dokáže poskytnout dostatečnou snímkovací frekvenci pro efektivní vyhodnocení klíčových ukazatelů z naměřených dat až 200 Hz a udávanou výdrž na baterii okolo 7 dní. Detailní rešerše existujících řešení a dostupných zařízení je obsažena v publikaci (Sec et al. 2018b). Jediným limitujícím faktorem tohoto zařízení tak byla technologie Bluetooth používaná pro přenos dat a která svým efektivním dosahem okolo 5-10 metrů předurčovala celý systém spíše pro domácí použití, nebo měření uvnitř kotce. Jako základnová stanice pro příjem dat ze senzoru na obojku posloužila platforma

Raspberry Pi 3. Jedná se o jednoduchá jednodeskový počítač s dostatečným výkonem pro zpracování naměřených dat, který zároveň disponuje možností bezdrátového připojení k internetu. Odpadá tak složitá a zdlouhavá instalace kabeláží a v případě potřeby lze rovněž celý systém provozovat z baterie. V rámci provedených testů bylo ověřeno, že na standardní nabíjecí Lithium iontovou baterii s napětím 5 V a kapacitě 10 000 mAh (běžně používanou například jako externí zdroj pro dobíjení mobilních telefonů) dokázal systém nepřetržitě pracovat po dobu tří dnů, Základnová stanice je podobně jako mobilní telefon napájena pomocí standardního micro USB kabelu, baterii tak lze v případě potřeby velice jednoduše vyměnit za novou s vyšší kapacitou, případně lze baterie střídat. Později se jako zásadní nevýhoda projevila skutečnost, že samotné zařízení nijak neinformuje uživatele, zda měření skutečně probíhá a případné chyby se projeví až v podobě absence dat na serveru. V pozdějších fázích vývoje prototypové stanice tak byl přidán jednoduchý informativní OLED display, který informuje o stavu baterie zařízení na obojku a aktuálním počtu naměřených a zpracovaných vzorků. Obrázek 28 zobrazuje prvotní konstrukci zařízení spolu s baterií (vlevo) a náhled informačního panelu s poskytovanými informacemi (vpravo).



Obrázek 28: Prototyp zařízení pro detekci záchvatů (vlevo) Detail display s přehledem o aktuálním stavu baterie a průběhu měření (vpravo); (autor)

Prvotní testování zařízení probíhalo v laboratorních podmínkách na UHK. Součástí testování bylo nejen způsob a spolehlivost komunikace, ale také ověření přesnosti naměřených hodnot a v neposlední řadě také schopnost dlouhodobého provozu zařízení z externí baterie. V rámci jednotlivých testů rovněž proběhla kontrolní měření životních funkcí za pomoci kalibrovaných senzorů přímo v laboratořích UHK, která později posloužila jako referenční data k porovnání s naměřenými hodnotami ze senzoru na obojku a následnému ověření prvotní teorie, že zvolený senzor od společnosti Metawear skutečně dokáže poskytnout relevantní výsledky a naměřené hodnoty HR a BR jsou srovnatelné s profesionálními měřicími přístroji.

Další fáze testování již probíhali v reálném prostředí, nejprve u zdravého psa (Německý ovčák; 3 roky). Pro měření v domácím prostředí byla základová stanice připojena do elektrické sítě. Pro měření mimo domov, například na procházkách, nebo při cestování byla použita pro napájení základové stanice již zmíněný externí zdroj napájení v podobě power banky. Tím bylo možné pořizovat data při fyzické zátěži, což se později ukázalo jako velice užitečné při zkoumání dalšího vlivu HRV na aktivitu zvířete. Ani zde nepředstavoval efektivní dosah do 10 metrů zásadní omezení pro spolehlivost měření. Data pořízená mimo připojení k internetu byla ukládána na interní SD kartu základnové stanice a výsledky odeslány ke zpracování až po opětovném připojení stanice k internetu.

Od začátku prací na projektu rovněž probíhala intenzivní jednání s veterinárními stanicemi za účelem nalezení psa s epilepsií, u kterého by bylo možné toto zařízení instalovat a umožnit tak naměření průběhů jednotlivých záchvatů pro jeho následnou analýzu. První instalace u reálných pacientů tak proběhla až v prosinci 2017 a to u dvou vytipovaných psů v Praze (Golden Retriever; 3 roky) a Brně (Beagle; 5 let).

Pro predikci blížícího se záchvatu mohou být použita data o vitálních funkcích zvířete, která mohou mít určitý vzor před začátkem záchvatu a jejichž analýza může být předmětem další studie. Dalším indikátorem mohou být historická data o předešlých záchvatech. Pokud jsou k dispozici i přesné informace o čase a datu záchvatu, mohou být hledány různé spouštěče těchto záchvatů, jako například barometrický tlak, teplota, fáze měsíce a další.

V rámci těchto teorií byly stanoveny hypotézy, že záchvaty nemají náhodný charakter, jak uvádí některé prameny (Packer et al. 2017a), ale mohou být vyvolány externími vlivy.

Zároveň byla pomocí statistické analýzy zkoumána vliv četnosti záchvatů na aktuální hodnoty barometrického tlaku, a to jak v jeho absolutní hodnotě, tak i v rámci jeho relativní výchylky v čase. Data o aktuální teplotě a barometrickém tlaku, nebo aktuální fázi měsíce byla získávána jak z dat dostupných na webu ČHMU z dané oblasti, tak i ze senzorů umístěných přímo v místnosti měřeného zvířete. Hypotéza o náhodnosti záchvatů byla nakonec zamítnuta s téměř nulovou p-hodnotou v řádech 10^{-17} a 10^{-23} . Bylo tak jasně prokázáno, že záchvaty nejsou vyvolány náhodně, ale mají určitý externí spouštěč. Rovněž nebylo potvrzeno, že se změnou léčby statisticky významně zvýšil počet záchvatů. Zde vyšel test dobré shody s p-hodnotou 0,12. Samotná statistická analýza dat však již není dílem autora této Disertační práce, a proto nebudou v práci mimo stanovených hypotéz uvedeny žádné dílčí postupy ani výsledky statistického zpracování dat, nicméně veškeré výstupy jsou obsaženy v závěrečné zprávě projektu.

11 Zhodnocení cílů disertační práce

Cílem disertační práce bylo navrhnout a v reálných podmínkách otestovat funkčnost systému pro sběr a monitoring vitálních funkcí zvířat. Jedním ze základních předpokladů pro úspěšné naplnění těchto cílů zahrnovala důkladná řešení všech aktuálně dostupných řešení v oblasti vědy a výzkumu, ale také v komerčním sektoru.

Úvodní kapitoly shrnují teoretické poznatky o možnostech snímání vitálních funkcí, nejčastěji dechové a tepové frekvence spolu s nejčastěji používanými technologiemi. U každého zařízení byla následně zhodnocena jako konstrukční stránka, případně představeny základní techniky vyhodnocení dat, orientační frekvence snímání dat a případná úskalí spojená s použitou technologií. Tyto poznatky byly rovněž publikovávány jako součást několika publikací (Sec et al. 2018; Sec a Mikulecky 2023).

Základní myšlenka decentralizované architektury využitelná pro automatizované řízení chytrých domácností byla poprvé autorem publikována již v roce 2017 jako součást publikace (Sec et al. 2017) využívající distribuované systémy a decentralizované výpočty ke sběru a vyhodnocení dat z IoT senzorů v rámci řešení Smart Home systémů. Tato myšlenka byla později dále rozšířena o návrh komunikačního protokolu speciálně optimalizovaného pro komunikaci M2M v systémech IoT (Stepan et al. 2017) včetně srovnání s běžně používanými způsoby komunikace. Následovala publikace zabývající se detekcí chybných hodnot s využitím prvků fuzzy logiky v publikaci (Sec a Mikulecky 2019), která představila možnosti detekce chybných hodnot v datech včetně způsobů řešení těchto chyb při následném zpracování dat.

Kapitoly 6 a 7 definují výhody použití Edge computingu jakožto základního principu pro vyhodnocení a přenos dat, mezi jednotlivými vrstvami systému. Představují základní strukturu systému a definují některé technické výzvy spojené s konstrukcí systému, které byly následně promítnuty do samotné implementace systému a případně posloužily jako základ pro testovací scénáře, kterým byla rovněž věnována samostatná část práce.

Kapitoly 7 a 8 dále popisují vybrané klíčové moduly systému. Součástí dosavadního výzkumu tak spočívala v kompletním návrhu a implementaci systému dle principů prezentovaných v Disertační práci, ale také zahrnovala praktické testy spočívající v měření vitálních funkcí zvířat nejprve v laboratorních podmínkách, a následně

v reálném provozu na několika veterinárních a chovatelských stanicích, nebo v domácnostech po celé České republice. Jmenovitě se jednalo například o kliniky HK-Vet v Hradci Králové a veterinární klinika v Heřmanově Městci, ale část systému byla rovněž použita jako platforma pro sběr a vyhodnocení epileptických záchvatů u psů v domácích podmínkách u majitelů v Praze a Brně. Veškeré dosavadní poznatky byly rovněž publikovány v podobě publikací, patentu a užitných vzorů uvedených v seznamu publikací autora a případné další výsledky budou publikovány v průběhu navazujícího výzkumu.

Součástí představeného systému bylo rovněž vytvoření cloudové části, implementace zabezpečeného komunikačního kanálu mezi cloudovou aplikací a jednotlivými výpočetními nody a následné ověřující bezpečnost daného řešení v podobě interního auditu shrnujícího provedená bezpečnostní opatření zajišťující bezpečnost dané aplikace spolu s případnými návrhy na zvýšení bezpečnosti přenášených dat a způsobů zabezpečení jednotlivých prvků systému a sítě. Výsledná kontrola zabezpečení provedená nástrojem testssl.sh rovněž potvrdila vysokou úroveň zabezpečení pomocí nezávislého testu s výslednou známkou A, a celkovým skóre 91/100.

Provedené testy propustnosti systému ověřující schopnosti jednotlivých výpočetních modulů paralelně zpracovávat příchozí data ze senzorů a ověřili možnosti zpracování více než 50 senzorů současně, přičemž každý edge node stále poskytoval dostatek (cca 40%) výkonu na obsluhu systému a delších podpůrných aplikací. Nasbíraná data v průběhu testování rovněž posloužila pro vytvoření lineárního regresního modelu predikujícího vývoj zátěže systému s ohledem na množství připojených zařízení. I přestože jsou výsledky regresního modelu silně vázány na konkrétní použitý HW, dokázal poskytnout alespoň základní představu do jaké míry ovlivní každé nově přidané zařízení celkový výkon jednotlivých edge nodů.

V práci byly rovněž prezentovány vybrané projekty využívající představenou platformu pro sběr a vyhodnocení dat ze senzorů. Mezi představenými systémy byly systémy pro detekci záchvatů u psů využívající bezdrátové senzory od společnosti Metawear, ale také systém pro detekci emocí u domácích a hospodářských zvířat s využitím strojového učení a neuronových sítí k vyhodnocování aktuálních emocí, s cílem zajistit optimální životní

podmínky a eliminovat zdravotní problémy způsobené stresem, kde byla použita kombinace bezdrátových senzorů i speciálních měřících podložek.

V době pandemie COVID-19 tato platforma rovněž posloužila pro aktivní monitoring životních funkcí na plicním oddělení Fakultní nemocnice Hradec Králové za účelem monitorování aktuálních životních funkcí a dlouhodobého sběru dat s cílem monitorování průběhu nemoci u pacientů hospitalizovaných s onemocněním COVID-19.

Jedním z dílčích cílů práce rovněž spočíval v ověření funkčnosti a robustnosti dané platformy jakožto nástroje pro sběr a vyhodnocení dat celou řadou laboratorních testů, ale také podrobení systému dlouhodobému provozu v reálných podmínkách. Nasazením systému a jeho dlouhodobým provozem na celkem 8 rozdílných vědeckovýzkumných projektech byla potvrzena nejen robustnost navržené platformy ale zároveň i vysoká univerzálnost navrženého řešení pro široké možnosti použití a schopnost zpracovávat data z rozdílných senzorů. Za dobu provozu systému bylo nasbíráno více než 900 GB dat, která posloužila pro samotnou optimalizaci výpočetního algoritmu, případně poskytla cenný zdroj dat v dalších oblastech výzkumu.

Možnosti dalšího vývoje pak skýtají optimalizace stávajících výpočetních algoritmů, tak aby mohly být vybrané algoritmy v budoucnu implementovány přímo do měřících senzorů. Další možnosti skýtají rozšíření výpočetního systému o nejrůznější filtry zajišťující eliminaci nežádoucího šumu. Součástí výzkumu tak bude výběr vhodných filtračních metod a jejich implementace a zařazení do vyhodnocovacího řetězce. Efektivní filtrací vstupních dat, ale také jednotlivých výsledků lze výrazně zvýšit robustnost výpočetních algoritmů a zároveň přispět k nižší náchylnosti systému pro detekci anomálií k chybám prvního i druhého druhu. Systém pro detekci anomálií může být rovněž dále rozšířen o prvky fuzzy logiky, jejichž výsledky lze využít pro efektivnější řízení ovládacích prvků, nebo zasílání notifikací.

Stejně tak lze v budoucnu navázat na výzkum detekce emocí u zvířat, který rovněž skýtá vysoký potenciál poskytnout hlubší porozumění emocionálním projevům u zvířat a přispět k tak k zásadnímu zlepšení životních podmínek zvířat.

12 Závěr

V současnosti lze pozorovat rostoucí trend rozvoje IoT zařízení ve všech odvětvích, včetně průmyslu obchodu autonomní dopravy, nebo právě zdravotnictví. V práci představený systém se tak snaží využít tohoto nastupujícího trendu a integrovat aktuálně dostupné, ale i nově vznikající technologie a postupy. Jednotlivé oblasti jsou v práci představeny a vysvětleny a následně efektivně aplikovány při návrhu a implementaci samotného systému.

Navržený systém splňuje všechny v práci vytyčené cíle včetně stanovených požadavků na rychlost zpracování dat, stejně tak i na bezpečnost jejich uchování, která je zajištěna odesláním již anonymizovaných dat do vyšších vrstev systému ale také jejich šifrováním na lokální úrovni. K vyšší bezpečnosti rovněž přispívá použití TLS šifrování pro veškerý přenos dat v síti. Zvolená architektura rovněž umožnila přesunout veškeré klíčové výpočty na lokální úroveň, čímž bylo docíleno nejen splnění klíčových požadavků na samotnou funkci systému, ale také snížení celkové zátěže na cloudovou službu samotnou a zvýšení odolnosti celého řešení na případné výpadky spojení i vyšší bezpečnost dat.

V práci jsou vymezeny základní termíny související s tvorbou systému, použitou technologií, včetně zhodnocení přínosů a možných rizik a nechybí zde ani představení vybraných alternativních řešení. Dále byly na základě non funkčních požadavků na systém definovány základní vlastnosti systému a identifikovány klíčové komponenty a vazby uvnitř systému a stejně tak druh i způsoby komunikace jednotlivých vrstev.

Na základě této analýzy byly následně představeny jednotlivé problémy a nastíněny způsoby jejich řešení. V případech, kdy bylo k dispozici podobné řešení byly srovnány výhodný nově navrženého řešení oproti konkurenčnímu.

Výsledná platforma byla otestována nejen v rámci laboratorních testů, ale byla rovněž úspěšně provozována na několika veterinárních zařízeních a domácnostech v České republice. V době pandemie COVID-19 rovněž sloužil systém jako platforma pro nepřetržitý dohled pacientů na plicním oddělení ve Fakultní nemocnici Hradci Králové.

V práci jsou rovněž byly prezentovány další navazující projekty a aplikace využívající nasbíraná data v průběhu provozování systému jakožto zdroje dat sloužícího pro další vědeckovýzkumnou činnost.

13 Použitá literatura

- 2NDQUADRANT, 2019. PostgreSQL vs MySQL. *2ndQuadrant | PostgreSQL* [online]. [vid. 2020-02-19]. Dostupné z: <https://www.2ndquadrant.com/en/postgresql/postgresql-vs-mysql/>
- ABADLEH, Ahmad, Eshraq AL-HAWARI, Esra'a ALKAFaweEN a Hamad AL-SAWALQAH, 2017. Step detection algorithm for accurate distance estimation using dynamic step length. In: *2017 18th IEEE International Conference on Mobile Data Management (MDM)* [online]. s. 324–327. ISSN 2375-0324. Dostupné z: doi:10.1109/MDM.2017.52
- ABDEL-BASSET, Mohamed, Gunasekaran MANOGARAN, Abdullaha GAMAL a Victor CHANG, 2019. A Novel Intelligent Medical Decision Support Model Based on Soft Computing and IoT. *IEEE Internet of Things Journal* [online]. 1–1. ISSN 2372-2541. Dostupné z: doi:10.1109/JIOT.2019.2931647
- AGNIHOTRI, Nikhil, 2022. The top MQTT brokers of 2022. *Engineers Garage* [online] [vid. 2023-04-13]. Dostupné z: <https://www.engineersgarage.com/top-mqtt-brokers-2022/>
- AI, Yuan, Mugen PENG a Kecheng ZHANG, 2018. Edge computing technologies for Internet of Things: a primer. *Digital Communications and Networks* [online]. 4(2), 77–86. ISSN 2352-8648. Dostupné z: doi:10.1016/j.dcan.2017.07.001
- ALIAN, Aymen A. a Kirk H. SHELLEY, 2014. Photoplethysmography. *Best Practice & Research Clinical Anaesthesiology* [online]. 28(4), Hemodynamic Monitoring Devices, 395–406. ISSN 1521-6896. Dostupné z: doi:10.1016/j.bpa.2014.08.006
- AL-TURJMAN, Fadi, 2018. *Edge Computing: From Hype to Reality*. B.m.: Springer. ISBN 978-3-319-99061-3.
- ALVAREZ, Brianne, 2019. What is Fog Computing? *QOS Networks* [online] [vid. 2020-02-17]. Dostupné z: <https://qosnet.com/what-is-fog-computing/>

- ANDREA, Ioannis, Chrysostomos CHRYSOSTOMOU a George HADJICHRISTOFI, 2015. Internet of Things: Security vulnerabilities and challenges. In: *2015 IEEE Symposium on Computers and Communication (ISCC)* [online]. s. 180–187. ISSN null. Dostupné z: doi:10.1109/ISCC.2015.7405513
- Anon., [b.r.]. *Machine learning based posture estimation for a wireless canine machine interface - IEEE Conference Publication* [online] [vid. 2020-03-03]. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/6613658>
- APC, 2016. *Co je edge computing a jak může podpořit vaši digitální transformaci.* [online] [vid. 2020-02-17]. Dostupné z: <https://www.apc.com:443/cz/cs/solutions/business-solutions/edge-computing/what-is-edge-computing>
- ARAS, Emekcan, Gowri Sankar RAMACHANDRAN, Piers LAWRENCE a Danny HUGHES, 2017. Exploring the Security Vulnerabilities of LoRa. In: *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)* [online]. s. 1–6. ISSN null. Dostupné z: doi:10.1109/CYBCConf.2017.7985777
- ASHTON, Kevin, 2009. That „Internet of Things“ Thing. **2009**(22), RFID journal, 97–114.
- BANKS, Andrew, Ed. BRIGGS, Ken BORGENDALE a Rahul GUPTA, 2023. *MQTT Version 5.0* [online]. 2023. B.m.: OASIS Standard. Dostupné z: <https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.htm>
- BASHSHUR, Rashid, Patricia A. ARMSTRONG, Zakhour I. YOUSSEF a UNIVERSITY OF MICHIGAN, ed., 1975. *Telemedicine; explorations in the use of telecommunications in health care.* Springfield, Ill: C. C. Thomas. ISBN 978-0-398-03276-0.
- BEKOFF, Marc, 2000. Animal Emotions: Exploring Passionate Natures. *BioScience* [online]. **50**(10), 861. ISSN 0006-3568. Dostupné z: doi:10.1641/0006-3568(2000)050[0861:AEEP]2.0.CO;2

- BELDA, B., M. ENOMOTO, B.C. CASE a B.D.X. LASCELLES, 2018. Initial evaluation of PetPace activity monitor. *The Veterinary Journal* [online]. **237**, 63–68. ISSN 10900233. Dostupné z: doi:10.1016/j.tvjl.2018.05.011
- BERENDT, Mette, Robyn G. FARQUHAR, Paul J. J. MANDIGERS, Akos PAKOZDY, Sofie F. M. BHATTI, Luisa DE RISIO, Andrea FISCHER, Sam LONG, Kaspar MATIASEK, Karen MUÑANA, Edward E. PATTERSON, Jacques PENDERIS, Simon PLATT, Michael PODELL, Heidrun POTSCHKA, Martí Batlle PUMAROLA, Clare RUSBRIDGE, Veronika M. STEIN, Andrea TIPOLD a Holger A. VOLK, 2015. International veterinary epilepsy task force consensus report on epilepsy definition, classification and terminology in companion animals. *BMC Veterinary Research* [online]. **11**(1), 182, s12917-015-0461-2. ISSN 1746-6148. Dostupné z: doi:10.1186/s12917-015-0461-2
- BIGGER, J T, J L FLEISS, R C STEINMAN, L M ROLNITZKY, R E KLEIGER a J N ROTTMAN, 1992. Frequency domain measures of heart period variability and mortality after myocardial infarction. *Circulation* [online]. **85**(1), 164–171. ISSN 0009-7322, 1524-4539. Dostupné z: doi:10.1161/01.CIR.85.1.164
- BLABER, A. P., Y. YAMAMOTO a R. L. HUGHSON, 1995. Change in phase relationship between SBP and R-R interval during lower body negative pressure. *American Journal of Physiology-Heart and Circulatory Physiology* [online]. **268**(4), H1688–H1693. ISSN 0363-6135, 1522-1539. Dostupné z: doi:10.1152/ajpheart.1995.268.4.H1688
- BLISS-MOREAU, Eliza a Peter H. RUDEBECK, 2021. Animal models of human mood. *Neuroscience & Biobehavioral Reviews* [online]. **120**, 574–582. ISSN 01497634. Dostupné z: doi:10.1016/j.neubiorev.2020.06.024
- BLUETOOTH SIG, 2020. GATT Specifications. *Bluetooth® Technology Website* [online] [vid. 2020-03-10]. Dostupné z: <https://www.bluetooth.com/specifications/gatt/>

- BONOMI, Flavio, 2011. Connected vehicles, the internet of things, and fog computing. In: *The eighth ACM international workshop on vehicular inter-networking (VANET), Las Vegas, USA*. s. 13–15.
- BONOMI, Flavio, Rodolfo MILITO, Jiang ZHU a Sateesh ADDEPALLI, 2012. Fog computing and its role in the internet of things. In: *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* [online]. Helsinki, Finland: Association for Computing Machinery, s. 13–16 [vid. 2020-02-17]. MCC '12. ISBN 978-1-4503-1519-7. Dostupné z: doi:10.1145/2342509.2342513
- BOTEK, Michal, Jakub KREJČÍ a Andrew J. MCKUNE, 2017. *Variabilita srdeční frekvence v tréninkovém procesu: historie, současnost a perspektiva*. B.m.: Univerzita Palackého v Olomouci. ISBN 978-80-244-5202-9.
- BRUGAROLAS, Rita, Tahmid LATIF, James DIEFFENDERFER, Katherine WALKER, Sherrie YUSCHAK, Barbara L. SHERMAN, David L. ROBERTS a Alper BOZKURT, 2016. Wearable Heart Rate Sensor Systems for Wireless Canine Health Monitoring. *IEEE Sensors Journal* [online]. **16**(10), 3454–3464. ISSN 2379-9153. Dostupné z: doi:10.1109/JSEN.2015.2485210
- BUNCH, Larry, Maggie BREEDY, Jeffrey M. BRADSHAW, Marco CARVALHO a Niranjana SURI, 2005. KARMEN: Multi-agent Monitoring and Notification for Complex Processes. In: Vladimír MAŘÍK, Robert WILLIAM BRENNAN a Michal PĚCHOUČEK, ed. *Holonics and Multi-Agent Systems for Manufacturing* [online]. Berlin, Heidelberg: Springer, s. 197–206. Lecture Notes in Computer Science. ISBN 978-3-540-31831-6. Dostupné z: doi:10.1007/11537847_18
- CARNEVALI, Luca, Mimosa TROMBINI, Alberto PORTA, Nicola MONTANO, Sietse F. DE BOER a Andrea SGOIFO, 2013. Vagal Withdrawal and Susceptibility to Cardiac Arrhythmias in Rats with High Trait Aggressiveness. *PLoS ONE* [online]. **8**(7), e68316. ISSN 1932-6203. Dostupné z: doi:10.1371/journal.pone.0068316
- CASADO-VARA, Roberto, Fernando DE LA PRIETA, Javier PRIETO a Juan M. CORCHADO, 2018. Blockchain framework for IoT data quality via edge computing. In: *Proceedings of the 1st Workshop on Blockchain-enabled*

- Networked Sensor Systems* [online]. Shenzhen, China: Association for Computing Machinery, s. 19–24 [vid. 2020-03-05]. BlockSys'18. ISBN 978-1-4503-6050-0. Dostupné z: doi:10.1145/3282278.3282282
- CASTIGLIONI, Paolo, Andrea FAINI, Gianfranco PARATI a Marco DI RIENZO, 2007. Wearable seismocardiography. *Conference proceedings: ... Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual Conference* [online]. **2007**, 3954–3957. ISSN 1557-170X. Dostupné z: doi:10.1109/IEMBS.2007.4353199
- CIMR, Dalibor a Filip STUDNIČKA, 2020. Automatic detection of breathing disorder from ballistocardiography signals. *Knowledge-Based Systems* [online]. **188**, 104973. ISSN 0950-7051. Dostupné z: doi:10.1016/j.knosys.2019.104973
- CONBOY, Alan, 2019. The Future of Healthcare Starts With Edge Computing - DZone IoT. *dzone.com* [online] [vid. 2020-02-17]. Dostupné z: <https://dzone.com/articles/the-future-of-healthcare-starts-with-edge-computin>
- CUGMAS, Blaž, Eva ŠTRUC a Jānis SPIGULIS, 2019. Photoplethysmography in dogs and cats: a selection of alternative measurement sites for a pet monitor. *Physiological Measurement* [online]. **40**(1), 01NT02. ISSN 1361-6579. Dostupné z: doi:10.1088/1361-6579/aaf433
- DARWIN, Charles, 1872. *The expression of the emotions in man and animals* (P. Ekman, Ed.). 1872. B.m.: Oxford University Press. <https://doi.org/10.1037/10001-000>.
- DATTA, Soumya Kanti, Rui Pedro Ferreira DA COSTA, Jérôme HÄRRI a Christian BONNET, 2016. Integrating connected vehicles in Internet of Things ecosystems: Challenges and solutions. In: *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)* [online]. s. 1–6. ISSN null. Dostupné z: doi:10.1109/WoWMoM.2016.7523574
- DE RISIO, Luisa a Simon R. PLATT, 2014. *Canine and feline epilepsy: diagnosis and management*. Wallingford, Oxfordshire: CABI. ISBN 978-1-78064-109-6.

- DEVELOPERWEEK 2019, 2019. *2019 Database Trends - SQL vs. NoSQL, Top Databases, Single vs. Multiple Database Use* [online] [vid. 2020-02-19].
Dostupné z: <https://scalegrid.io/blog/2019-database-trends-sql-vs-nosql-top-databases-single-vs-multiple-database-use/>
- DI RIENZO, Marco, Paolo MERIGGI, Francesco RIZZO, Emanuele VAINI, Andrea FAINI, Giampiero MERATI, Gianfranco PARATI a Paolo CASTIGLIONI, 2011. A wearable system for the seismocardiogram assessment in daily life conditions. In: *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society* [online]. s. 4263–4266. ISSN 1557-170X.
Dostupné z: doi:10.1109/IEMBS.2011.6091058
- DIN, Sadia, M. Mazhar RATHORE, Awais AHMAD, Anand PAUL a Murad KHAN, 2017. SDIoT: Software Defined Internet of Thing to Analyze Big Data in Smart Cities. In: *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)* [online]. s. 175–182. ISSN null. Dostupné z: doi:10.1109/LCN.Workshops.2017.84
- DJELOUAT, Hamza, Mohamed AL DISI, Issam BOUKHENOUBA, Abbas AMIRA, Faycal BENSALI, Christos KOTRONIS, Elena POLITI, Mara NIKOLAIDOU a George DIMITRAKOPOULOS, 2020. Real-time ECG monitoring using compressive sensing on a heterogeneous multicore edge-device. *Microprocessors and Microsystems* [online]. **72**, 102839. ISSN 0141-9331. Dostupné z: doi:10.1016/j.micpro.2019.06.009
- DONGXIN LU a TAO LIU, 2011. The application of IOT in medical system. In: *2011 IEEE International Symposium on IT in Medicine and Education* [online]. s. 272–275. ISSN null. Dostupné z: doi:10.1109/ITIME.2011.6130831
- DUBEY, Harishchandra, Admir MONTEIRO, Nicholas CONSTANT, Mohammadreza ABTAHI, Debanjan BORTHAKUR, Leslie MAHLER, Yan SUN, Qing YANG, Umer AKBAR a Kunal MANKODIYA, 2017. Fog Computing in Medical Internet-of-Things: Architecture, Implementation, and Applications. In: Samee U. KHAN, Albert Y. ZOMAYA a Assad ABBAS, ed. *Handbook of Large-Scale*

Distributed Computing in Smart Healthcare [online]. Cham: Springer International Publishing, Scalable Computing and Communications, s. 281–321 [vid. 2020-02-17]. ISBN 978-3-319-58280-1. Dostupné z: doi:10.1007/978-3-319-58280-1_11

DUPLAGA, Mariusz a Krzysztof ZIELIŃSKI, 2006. Evolution of IT-Enhanced Healthcare: From Telemedicine to e-Health. In: Krzysztof ZIELIŃSKI, Mariusz DUPLAGA a David INGRAM, ed. *Information Technology Solutions for Healthcare* [online]. London: Springer London, s. 1–21. ISBN 978-1-84628-141-9. Dostupné z: doi:10.1007/1-84628-141-5_1

DURUMERIC, Zakir, David ADRIAN, Ariana MIRIAN, Michael BAILEY a J. Alex HALDERMAN, 2015. A Search Engine Backed by Internet-Wide Scanning. In: *CCS'15: The 22nd ACM Conference on Computer and Communications Security: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* [online]. Denver Colorado USA: ACM, s. 542–553 [vid. 2023-07-17]. ISBN 978-1-4503-3832-5. Dostupné z: doi:10.1145/2810103.2813703

ECKENFELS, A., 1986. The voltage of R-waves in the normal electrocardiogram of the conscious beagle. *Arzneimittel-Forschung*. **36**(7), 1024–1029. ISSN 0004-4172.

ELDEWAHI, Abeer E. W., Tasneem M. H. SHARFI, Abdelhamid A. MANSOR, Nashwa A. F. MOHAMED a Samah M. H. ALWAHBANI, 2015. SSL/TLS attacks: Analysis and evaluation. In: *2015 International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE): 2015 International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE)* [online]. Khartoum, Sudan: IEEE, s. 203–208 [vid. 2023-07-18]. ISBN 978-1-4673-7869-7. Dostupné z: doi:10.1109/ICCNEEE.2015.7381362

ELHOSENY, Mohamed, Gustavo RAMÍREZ-GONZÁLEZ, Osama M. ABU-ELNASR, Shihab A. SHAWKAT, N. ARUNKUMAR a Ahmed FAROUK, 2018. Secure Medical Data Transmission Model for IoT-Based Healthcare Systems. *IEEE*

Access [online]. 6, 20596–20608. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2018.2817615

ERTAUL, Levent, Peter CHUDINOV a Brian MORALES, 2019. IoT Security: Authenticated Lightweight Key Exchange (ALIKE). In: *Proceedings of the International Conference on Wireless Networks (ICWN)*. B.m.: The Steering Committee of The World Congress in Computer Science, Computer ..., s. 45–50.

ESSNER, Ann, Rita SJÖSTRÖM, Erik AHLGREN, Pia GUSTÅS, Laurie EDGE-HUGHES, Lena ZETTERBERG a Karin HELLSTRÖM, 2015. Comparison of Polar® RS800CX heart rate monitor and electrocardiogram for measuring inter-beat intervals in healthy dogs. *Physiology & Behavior* [online]. 138, 247–253. ISSN 0031-9384. Dostupné z: doi:10.1016/j.physbeh.2014.10.034

FEIGHELSTEIN, Marcelo Gabriel, 2021. Towards Automatic Recognition of Emotional States of Animals. In: *ACI'21: Eight International Conference on Animal-Computer Interaction: Eight International Conference on Animal-Computer Interaction* [online]. Bloomington IN USA: ACM, s. 1–4 [vid. 2023-05-13]. ISBN 978-1-4503-8513-8. Dostupné z: doi:10.1145/3493842.3493897

FELTER, Blair, 2019. *5 Use Cases You Need to Know for Edge Computing and Healthcare* [online] [vid. 2020-02-17]. Dostupné z: <https://www.vxchnge.com/blog/edge-computing-use-cases-healthcare>

FITBARK INC., 2019. FitBark GPS Dog Trackers & Activity Monitors | Healthy Together. *FitBark GPS Dog Tracker* [online] [vid. 2020-02-17]. Dostupné z: <https://www.fitbark.com/>

FREDERICK, William H. a E. E. EDDLEMAN, 1958. A Simple Bed Suspension for Ultra-Low Frequency Ballistocardiography on Dogs. *Journal of Applied Physiology* [online]. 12(2), 347–348. ISSN 8750-7587. Dostupné z: doi:10.1152/jappl.1958.12.2.347

FUJII, Takahide, Masanao NAKANO, Ken YAMASHITA, Toshihiro KONISHI, Shintaro IZUMI, Hiroshi KAWAGUCHI a Masahiko YOSHIMOTO, 2013.

- Noise-tolerant instantaneous heart rate and R-peak detection using short-term autocorrelation for wearable healthcare systems. In: *2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC): 2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* [online]. Osaka: IEEE, s. 7330–7333 [vid. 2023-05-10]. ISBN 978-1-4577-0216-7. Dostupné z: doi:10.1109/EMBC.2013.6611251
- GARTNER, INC., 2019. Edge Computing. *Gartner* [online] [vid. 2020-02-17]. Dostupné z: <https://www.gartner.com/en/information-technology/glossary/edge-computing>
- GEHRKE, Ellen Kaye, Ann BALDWIN a Patric M. SCHILTZ, 2011. Heart Rate Variability in Horses Engaged in Equine-Assisted Activities. *Journal of Equine Veterinary Science* [online]. **31**(2), 78–84. ISSN 07370806. Dostupné z: doi:10.1016/j.jevs.2010.12.007
- GORDON, J. W., 1877. Certain Molar Movements of the Human Body produced by the Circulation of the Blood. *Journal of Anatomy and Physiology*. **11**(Pt 3), 533–536.
- GOTTER, Ana, 2017. Pulse Oximetry: Uses, Readings, and How It Works. *Healthline* [online] [vid. 2020-03-03]. Dostupné z: <https://www.healthline.com/health/pulse-oximetry>
- GROVER, Jitender a Ram Murthy GARIMELLA, 2019. Optimization in Edge Computing and Small-Cell Networks. In: Fadi AL-TURJMAN, ed. *Edge Computing* [online]. Cham: Springer International Publishing, EAI/Springer Innovations in Communication and Computing, s. 17–31 [vid. 2024-03-17]. ISBN 978-3-319-99060-6. Dostupné z: doi:10.1007/978-3-319-99061-3_2
- GYARMATHY, Kaylie, 2019. *The Benefits and Potential of Edge Computing* [online] [vid. 2020-02-17]. Dostupné z: <https://www.vxchnge.com/blog/the-5-best-benefits-of-edge-computing>
- HACHENBERGER, Justin, Yu-Mei LI, Michael SINIATCHKIN, Katharin HERMENAU, Sebastian LUDYGA a Sakari LEMOLA, 2023. Heart Rate

- Variability's Association with Positive and Negative Affect in Daily Life: An Experience Sampling Study with Continuous Daytime Electrocardiography over Seven Days. *Sensors* [online]. **23**(2), 966. ISSN 1424-8220. Dostupné z: doi:10.3390/s23020966
- HAMPTON, John R, 2013. *EKG stručně, jasně, přehledně - Překlad 7. vydání*. B.m.: Grada Publishing a.s. ISBN 978-80-247-4246-5.
- HAN, Tao, Lijuan ZHANG, Sandeep PIRBHULAL, Wanqing WU a Victor Hugo C. DE ALBUQUERQUE, 2019. A novel cluster head selection technique for edge-computing based IoMT systems. *Computer Networks* [online]. **158**, 114–122. ISSN 1389-1286. Dostupné z: doi:10.1016/j.comnet.2019.04.021
- HAYES, Matthew J. a Peter R. SMITH, 1998. Artifact reduction in photoplethysmography. *Applied Optics* [online]. **37**(31), 7437–7446. ISSN 2155-3165. Dostupné z: doi:10.1364/AO.37.007437
- HEGEMANN, Lisa, 2020. Robert Koch-Institut: Diese App wird die Krise nicht lösen. *Die Zeit* [online]. [vid. 2020-04-17]. ISSN 0044-2070. Dostupné z: <https://www.zeit.de/digital/internet/2020-04/robert-koch-institut-app-coronavirus-forschung-daten>
- HOLDERITH, Melanie a Thomas SCHANZE, 2018. Cross-Correlation based comparison between the conventional 12-lead ECG and an EASI derived 12-lead ECG. *Current Directions in Biomedical Engineering* [online]. **4**(1), 621–624. ISSN 2364-5504. Dostupné z: doi:10.1515/cdbme-2018-0149
- HOPKINS, William, Stephen MARSHALL, Alan BATTERHAN a Juri HANIN, 2009. Progressive statistics for studies in sports medicine and exercise science. *Medicine+ Science in Sports+ Exercise* [online]. **41**(1), 3. Dostupné z: doi:10.7752/jpes.2019.s2051
- HOSKINS, Katherine, 2016. Security Vulnerabilities in Z-Wave Home Automation Protocol. *Tufts University Department of Computer Science*. **14**.

- HOWBERT, J. Jeffry, Edward E. PATTERSON, S. Matt STEAD, Ben BRINKMANN, Vincent VASOLI, Daniel CREPEAU, Charles H. VITE, Beverly STURGES, Vanessa RUEDEBUSCH, Jaideep MAVOORI, Kent LEYDE, W. Douglas SHEFFIELD, Brian LITT a Gregory A. WORRELL, 2014. Forecasting Seizures in Dogs with Naturally Occurring Epilepsy. *PLoS ONE* [online]. **9**(1) [vid. 2020-02-17]. ISSN 1932-6203. Dostupné z: doi:10.1371/journal.pone.0081920
- HU, Bo, Hongfeng XIE, Yutao MA, Jian WANG a Liang-Jie ZHANG, 2018. A Robust Retail POS System Based on Blockchain and Edge Computing. In: Shijun LIU, Bedir TEKINERDOGAN, Mikio AOYAMA a Liang-Jie ZHANG, ed. *Edge Computing – EDGE 2018* [online]. Cham: Springer International Publishing, s. 99–110. Lecture Notes in Computer Science. ISBN 978-3-319-94340-4. Dostupné z: doi:10.1007/978-3-319-94340-4_8
- HURNANEN, Tero, Eero LEHTONEN, Mojtaba Jafari TADI, Tom KUUSELA, Tuomas KIVINIEMI, Antti SARASTE, Tuija VASANKARI, Juhani AIRAKSINEN, Tero KOIVISTO a Mikko PÄNKÄÄLÄ, 2017. Automated Detection of Atrial Fibrillation Based on Time–Frequency Analysis of Seismocardiograms. *IEEE Journal of Biomedical and Health Informatics* [online]. **21**(5), 1233–1241. ISSN 2168-2208. Dostupné z: doi:10.1109/JBHI.2016.2621887
- CHAN, Stephanie, 2017. *Fog brings the cloud closer to the ground: Cisco innovates in fog computing* [online] [vid. 2020-02-17]. Dostupné z: <https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1894659>
- CHANDLER, Kate, 2006. Canine epilepsy: What can we learn from human seizure disorders? *The Veterinary Journal* [online]. **172**(2), 207–217. ISSN 10900233. Dostupné z: doi:10.1016/j.tvjl.2005.07.001
- CHEN, Lixing, Sheng ZHOU a Jie XU, 2018a. Computation Peer Offloading for Energy-Constrained Mobile Edge Computing in Small-Cell Networks. *IEEE/ACM Transactions on Networking* [online]. **26**(4), 1619–1632. ISSN 1558-2566. Dostupné z: doi:10.1109/TNET.2018.2841758

- CHEN, Yi, Shuai DING, Zheng XU, Handong ZHENG a Shanlin YANG, 2018b. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *Journal of Medical Systems* [online]. **43**(1), 5. ISSN 1573-689X. Dostupné z: doi:10.1007/s10916-018-1121-4
- CHENG, Chi, Rongxing LU, Albrecht PETZOLDT a Tsuyoshi TAKAGI, 2017. Securing the Internet of Things in a Quantum World. *IEEE Communications Magazine* [online]. **55**(2), 116–120. ISSN 0163-6804. Dostupné z: doi:10.1109/MCOM.2017.1600522CM
- IBM CORPORATION, 2003. Prostředí: Vzájemná autentizace pomocí certifikátů. In: *IBM Tivoli Access Manager WebSEAL: Průvodce administrátora* [online]. [vid. 2020-02-20]. Dostupné z: http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1134-01/cs_CZ/HTML/amweb41_admin189.htm
- IDENTITY MANAGEMENT INSTITUTE, 2019. *Edge Computing Security and Challenges* [online] [vid. 2020-02-17]. Dostupné z: <https://www.identitymanagementinstitute.org/edge-computing-security-and-challenges/>
- INAN, Omer T., Pierre-Francois MIGEOTTE, Kwang-Suk PARK, Mozziyar ETEMADI, Kouhyar TAVAKOLIAN, Ramon CASANELLA, John ZANETTI, Jens TANK, Irina FUNTOVA, G. Kim PRISK a Marco DI RIENZO, 2015. Ballistocardiography and Seismocardiography: A Review of Recent Advances. *IEEE Journal of Biomedical and Health Informatics* [online]. **19**(4), 1414–1427. ISSN 2168-2208. Dostupné z: doi:10.1109/JBHI.2014.2361732
- JORDANS, Roel, Rosilde CORVINO, Lech JOZWIAK a Henk CORPORAAL, 2013. Instruction-set architecture exploration strategies for deeply clustered VLIW ASIPs. In: *2013 2nd Mediterranean Conference on Embedded Computing (MECO): 2013 2nd Mediterranean Conference on Embedded Computing (MECO)* [online]. Budva, Montenegro: IEEE, s. 38–41 [vid. 2023-05-03]. ISBN 978-9940-9436-1-5. Dostupné z: doi:10.1109/MECO.2013.6601361

- KAISLER, Stephen, Frank ARMOUR, J. Alberto ESPINOSA a William MONEY, 2013. Big Data: Issues and Challenges Moving Forward. In: *2013 46th Hawaii International Conference on System Sciences* [online]. s. 995–1004. ISSN 1530-1605. Dostupné z: doi:10.1109/HICSS.2013.645
- KAISTI, Matti, Mojtaba Jafari TADI, Olli LAHDENOJA, Tero HURNANEN, Antti SARASTE, Mikko PÄNKÄÄLÄ a Tero KOIVISTO, 2019. Stand-Alone Heartbeat Detection in Multidimensional Mechanocardiograms. *IEEE Sensors Journal* [online]. **19**(1), 234–242. ISSN 2379-9153. Dostupné z: doi:10.1109/JSEN.2018.2874706
- KAMAL, A. A. R., J. B. HARNESS, G. IRVING a A. J. MEARNS, 1989. Skin photoplethysmography — a review. *Computer Methods and Programs in Biomedicine* [online]. **28**(4), 257–269. ISSN 0169-2607. Dostupné z: doi:10.1016/0169-2607(89)90159-4
- KANWAL, Maria, Asad Waqar MALIK, Anis Ur RAHMAN, Imran MAHMOOD a Muhammad SHAHZAD, 2019. Sustainable vehicle-assisted edge computing for big data migration in smart cities. *IEEE Internet of Things Journal* [online]. 1–1. ISSN 2372-2541. Dostupné z: doi:10.1109/JIOT.2019.2957127
- KATAL, Avita, Mohammad WAZID a R. H. GOUDAR, 2013. Big data: Issues, challenges, tools and Good practices. In: *2013 Sixth International Conference on Contemporary Computing (IC3)* [online]. s. 404–409. ISSN null. Dostupné z: doi:10.1109/IC3.2013.6612229
- KAZAR, Mike, David NICHOLS, John ZSARNAY a Ivor DURHAM, 1982. *The „only“ coke machine on the internet* [online] [vid. 2020-03-11]. Dostupné z: https://www.cs.cmu.edu/~coke/history_long.txt
- KEARY, Tim, 2018. Healthcare and edge computing: responsive healthcare. *Information Age* [online]. [vid. 2020-02-17]. Dostupné z: <https://www.information-age.com/edge-computing-responsive-healthcare-123476810/>

- KERNER, Sean Michael, 2019. *Edge Security: How to Secure the Edge of the Network* [online] [vid. 2020-02-17]. Dostupné z: <https://www.esecurityplanet.com/network-security/edge-security.html>
- KHAN, Latif U., Ibrar YAQOOB, Nguyen H. TRAN, S. M. Ahsan KAZMI, Tri Nguyen DANG a Choong Seon HONG, 2019. Edge Computing Enabled Smart Cities: A Comprehensive Survey. *arXiv:1909.08747 [cs]* [online]. [vid. 2020-03-05]. Dostupné z: <http://arxiv.org/abs/1909.08747>
- KHANJI, Salam, Farkhund IQBAL a Patrick HUNG, 2019. ZigBee Security Vulnerabilities: Exploration and Evaluating. In: *2019 10th International Conference on Information and Communication Systems (ICICS)* [online]. s. 52–57. ISSN 2471-125X. Dostupné z: [doi:10.1109/IACS.2019.8809115](https://doi.org/10.1109/IACS.2019.8809115)
- KOK, Bethany E., Kimberly A. COFFEY, Michael A. COHN, Lahna I. CATALINO, Tanya VACHARKULKSEMSUK, Sara B. ALGOE, Mary BRANTLEY a Barbara L. FREDRICKSON, 2013. How Positive Emotions Build Physical Health: Perceived Positive Social Connections Account for the Upward Spiral Between Positive Emotions and Vagal Tone. *Psychological Science* [online]. **24**(7), 1123–1132. ISSN 0956-7976, 1467-9280. Dostupné z: [doi:10.1177/0956797612470827](https://doi.org/10.1177/0956797612470827)
- KREMER, L., S.E.J. KLEIN HOLKENBORG, I. REIMERT, J.E. BOLHUIS a L.E. WEBB, 2020. The nuts and bolts of animal emotion. *Neuroscience & Biobehavioral Reviews* [online]. **113**, 273–286. ISSN 01497634. Dostupné z: [doi:10.1016/j.neubiorev.2020.01.028](https://doi.org/10.1016/j.neubiorev.2020.01.028)
- KWIATKOWSKA-STENZEL, Agnieszka, Janina SOWIŃSKA a Dorota WITKOWSKA, 2016. The Effect of Different Bedding Materials Used in Stable on Horses Behavior. *Journal of Equine Veterinary Science* [online]. **42**, 57–66. ISSN 07370806. Dostupné z: [doi:10.1016/j.jevs.2016.03.007](https://doi.org/10.1016/j.jevs.2016.03.007)
- LABRIE GREG, 2019. *Top 5 Benefits of Edge Computing* [online] [vid. 2020-02-17]. Dostupné z: <https://blog.wei.com/top-5-benefits-of-edge-computing>

- LAHDENOJA, Olli, Tero HURNANEN, Matti KAISTI, Juho KOSKINEN, Jarno TUOMINEN, Matti VÄHÄ-HEIKKILÄ, Laura PARIKKA, Maria WIBERG, Tero KOIVISTO a Mikko PÄNKÄÄLÄ, 2019. Cardiac monitoring of dogs via smartphone mechanocardiography: a feasibility study. *BioMedical Engineering OnLine* [online]. **18**(1), 47. ISSN 1475-925X. Dostupné z: doi:10.1186/s12938-019-0667-9
- LICHT, Barbara G., Mark H. LICHT, Kathleen M. HARPER, Shili LIN, John J. CURTIN, Linda L. HYSON a Kristen WILLARD, 2002. Clinical presentations of naturally occurring canine seizures: similarities to human seizures. *Epilepsy & Behavior* [online]. **3**(5), 460–470. ISSN 15255050. Dostupné z: doi:10.1016/S1525-5050(02)00523-1
- LING, Zhen, Junzhou LUO, Yiling XU, Chao GAO, Kui WU a Xinwen FU, 2017. Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. *IEEE Internet of Things Journal* [online]. **4**(6), 1899–1909. ISSN 2372-2541. Dostupné z: doi:10.1109/JIOT.2017.2707465
- LIU, Hong, Yan ZHANG a Tao YANG, 2018. Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing. *IEEE Network* [online]. **32**(3), 78–83. ISSN 1558-156X. Dostupné z: doi:10.1109/MNET.2018.1700344
- LIU, Kaikai, Abhishek GURUDUTT, Tejeshwar KAMAAL, Chinmayi DIVAKARA a Praveen PRABHAKARAN, 2017. Edge computing framework for distributed smart applications. In: *2017 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computed, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)* [online]. s. 1–8. ISSN null. Dostupné z: doi:10.1109/UIC-ATC.2017.8397448
- LIU, Yi, Chao YANG, Li JIANG, Shengli XIE a Yan ZHANG, 2019. Intelligent Edge Computing for IoT-Based Energy Management in Smart Cities. *IEEE Network* [online]. **33**(2), 111–117. ISSN 1558-156X. Dostupné z: doi:10.1109/MNET.2019.1800254

- LOVEN, Lauri, Teemu LEPPANEN, Ella PELTONEN, Juha PARTALA, Erkki HARJULA, Pawani PORAMBAGE, Mika YLIANTTILA a Jukka RIEKKI, 2019. EdgeAI: A Vision for Distributed, Edge-native Artificial Intelligence in Future 6G Networks. **2019**, The 1st 6G Wireless Summit, 2.
- MAGGI, Federico, Rainer VOSSELER a Davide QUARTA, 2018. The fragility of industrial iot's data backbone. *Trend Micro Inc.*
- MALLIANI, A, M PAGANI, F LOMBARDI a S CERUTTI, 1991. Cardiovascular neural regulation explored in the frequency domain. *Circulation* [online]. **84**(2), 482–492. ISSN 0009-7322, 1524-4539. Dostupné z: doi:10.1161/01.CIR.84.2.482
- MARCELLI, Emanuela, Laura CERCENELLI, Mario PARLAPIANO, Roberto FUMERO, Paola BAGNOLI, Maria Laura COSTANTINO a Gianni PLICCHI, 2007. Effect of Right Ventricular Pacing on Cardiac Apex Rotation Assessed by a Gyroscopic Sensor. *ASAIO Journal* [online]. **53**(3), 304–309. ISSN 1058-2916. Dostupné z: doi:10.1097/MAT.0b013e31805370e3
- MAROS, Katalin, Antal DÓKA a Ádám MIKLÓSI, 2008. Behavioural correlation of heart rate changes in family dogs. *Applied Animal Behaviour Science* [online]. **109**(2–4), 329–341. ISSN 01681591. Dostupné z: doi:10.1016/j.applanim.2007.03.005
- MARTENS, Benedikt, Marc WALTERBUSCH a Frank TEUTEBERG, 2012. Costing of Cloud Computing Services: A Total Cost of Ownership Approach. In: *2012 45th Hawaii International Conference on System Sciences* [online]. s. 1563–1572. ISSN 1530-1605. Dostupné z: doi:10.1109/HICSS.2012.186
- MCCORRY, Laurie Kelly, 2007. Physiology of the Autonomic Nervous System. *American Journal of Pharmaceutical Education* [online]. **71**(4), 78. ISSN 0002-9459, 1553-6467. Dostupné z: doi:10.5688/aj710478
- MCGRATH, J., 2017. *Epilepsy in dogs: Causes and symptoms*. [online]. Dostupné z: <https://www.petfinder.com/dogs/dog-health/epilepsy-in-dogs-causes/>

- MCGRATH, Stephanie, Lisa R. BARTNER, Sangeeta RAO, Rebecca A. PACKER a Daniel L. GUSTAFSON, 2019. Randomized blinded controlled clinical trial to assess the effect of oral cannabidiol administration in addition to conventional antiepileptic treatment on seizure frequency in dogs with intractable idiopathic epilepsy. *Journal of the American Veterinary Medical Association* [online]. **254**(11), 1301–1308. ISSN 0003-1488. Dostupné z: doi:10.2460/javma.254.11.1301
- MENDL, Michael, Vikki NEVILLE a Elizabeth S. PAUL, 2022. Bridging the Gap: Human Emotions and Animal Emotions. *Affective Science* [online]. **3**(4), 703–712. ISSN 2662-2041, 2662-205X. Dostupné z: doi:10.1007/s42761-022-00125-6
- MHEALTH, INC., 2011. mHealth Data Interoperability. *Open mHealth* [online] [vid. 2020-02-17]. Dostupné z: <https://www.openmhealth.org/>
- MLADENOV, Martin a Michael MOCK, 2009. A step counter service for Java-enabled devices using a built-in accelerometer. In: *Proceedings of the 1st International Workshop on Context-Aware Middleware and Services: affiliated with the 4th International Conference on Communication System Software and Middleware (COMSWARE 2009)* [online]. Dublin, Ireland: Association for Computing Machinery, s. 1–5 [vid. 2020-02-17]. CAMS '09. ISBN 978-1-60558-525-3. Dostupné z: doi:10.1145/1554233.1554235
- MOBERG, Gary P. a Joy A. MENCH, ed., 2000. *The biology of animal stress: basic principles and implications for animal welfare*. Wallingford, UK ; New York, NY, USA: CABI Pub. ISBN 978-0-85199-359-1.
- MOHR, Elmar, Jan LANGBEIN a Gerd NÜRNBERG, 2002. Heart rate variability: A noninvasive approach to measure stress in calves and cows. *Physiology & Behavior* [online]. **75**(1), 251–259. ISSN 0031-9384. Dostupné z: doi:10.1016/S0031-9384(01)00651-5
- MÖLLER, Bodo, Thai DUONG a Krzysztof KOTOWICZ, 2014. This POODLE bites: exploiting the SSL 3.0 fallback. *Security Advisory*. **21**, 34–58.

- MOROZOV, Anna, Lisa A. PARR, Katalin GOTHARD, Rony PAZ a Raviv PRYLUK, 2021. Automatic Recognition of Macaque Facial Expressions for Detection of Affective States. *eneuro* [online]. **8**(6), ENEURO.0117-21.2021. ISSN 2373-2822. Dostupné z: doi:10.1523/ENEURO.0117-21.2021
- MUSET, Bogdan a Simina EMERICH, 2012. Distance Measuring using Accelerometer and Gyroscope Sensors. 4.
- NAMEE, Khanista, Nuttapat PANONG a Jantima POLPINIJ, 2019. Integration of IoT, Edge Computing and Cloud Computing for Monitoring and Controlling Automated External Defibrillator Cabinets in Emergency Medical Service. In: *2019 5th International Conference on Information Management (ICIM)* [online]. s. 237–241. ISSN null. Dostupné z: doi:10.1109/INFOMAN.2019.8714717
- NEETHIRAJAN, Suresh, 2022. Affective State Recognition in Livestock—Artificial Intelligence Approaches. *Animals* [online]. **12**(6), 759. ISSN 2076-2615. Dostupné z: doi:10.3390/ani12060759
- NESHENKO, Nataliia, Elias BOU-HARB, Jorge CRICHIGNO, Georges KADDOUM a Nasir GHANI, 2019. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Communications Surveys & Tutorials* [online]. **21**(3), 2702–2733. ISSN 1553-877X, 2373-745X. Dostupné z: doi:10.1109/COMST.2019.2910750
- NETFLIX, INC., 2019. *Netflix - Watch TV Shows Online, Watch Movies Online* [online] [vid. 2020-02-19]. Dostupné z: <https://www.netflix.com/>
- O'BRIEN, Samuel, 2019. *5 Benefits of Edge Computing for Enterprises* [online] [vid. 2020-02-17]. Dostupné z: <https://www.vxchnge.com/blog/edge-computing-for-enterprises>
- ORTMEYER, Heidi, Lynda ROBEY a Tara MCDONALD, 2018. Combining Actigraph Link and PetPace Collar Data to Measure Activity, Proximity, and Physiological

- Responses in Freely Moving Dogs in a Natural Environment. *Animals* [online]. **8**(12), 230. ISSN 2076-2615. Dostupné z: doi:10.3390/ani8120230
- PACKER, R. M. A., R. LUCAS a H. A. VOLK, 2017a. Owner perception of focal seizures in canine epilepsy. *Veterinary Record* [online]. **180**(6), 150–150. ISSN 00424900. Dostupné z: doi:10.1136/vr.104099
- PACKER, R.M.A., H.A. VOLK a R.C. FOWKES, 2017b. Physiological reactivity to spontaneously occurring seizure activity in dogs with epilepsy and their carers. *Physiology & Behavior* [online]. **177**, 27–33. ISSN 00319384. Dostupné z: doi:10.1016/j.physbeh.2017.04.008
- PACKER, Rowena M. A. a Holger A. VOLK, 2015. Epilepsy beyond seizures: a review of the impact of epilepsy and its comorbidities on health-related quality of life in dogs. *Veterinary Record* [online]. **177**(12), 306–315. ISSN 00424900. Dostupné z: doi:10.1136/vr.103360
- PADMAJA, P. a G.V. MARUTHESWAR, 2018. Energy efficient data aggregation in wireless sensor networks. *Materials Today: Proceedings* [online]. **5**(1), 388–396. ISSN 22147853. Dostupné z: doi:10.1016/j.matpr.2017.11.096
- PALMER, Theresa a Anne Frances OWEN, 2020. *The Common Data Model - Common Data Model* [online] [vid. 2020-02-17]. Dostupné z: <https://docs.microsoft.com/en-us/common-data-model/>
- PAUL, Elizabeth S., Shlomi SHER, Marco TAMIETTO, Piotr WINKIELMAN a Michael T. MENDEL, 2020. Towards a comparative science of emotion: Affect and consciousness in humans and animals. *Neuroscience & Biobehavioral Reviews* [online]. **108**, 749–770. ISSN 01497634. Dostupné z: doi:10.1016/j.neubiorev.2019.11.014
- PEREDNIA, Douglas A a Ace ALLEN, 1995. Telemedicine technology and clinical applications. *Jama*. **273**(6), 483–488.
- PETPACE, 2018. Smart Dog Collar - Heart Rate Monitor & More | Petpace. *PetPace Smart Collar* [online] [vid. 2020-03-02]. Dostupné z: <https://petpace.com/>

- PINHEIRO, Eduardo, Octavian POSTOLACHE a Pedro GIRÃO, 2010. Theory and Developments in an Unobtrusive Cardiovascular System Representation: Ballistocardiography. *The Open Biomedical Engineering Journal* [online]. **4**, 201–216. ISSN 1874-1207. Dostupné z: doi:10.2174/1874120701004010201
- PITPATPET LTD, 2019. Dog Activity Monitor - Exercise, Weight & Fitness Tracker App. *PitPat* [online] [vid. 2020-02-17]. Dostupné z: <https://www.pitpat.com/>
- QARDIO, INC, 2020. QardioMD - Easy remote monitoring platform for doctors. *Qardio* [online]. [vid. 2020-03-10]. Dostupné z: <https://www.getqardio.com/en/qardiomd-heart-health/>
- QUINTANA, Daniel S., James A. J. HEATHERS a Andrew H. KEMP, 2012. On the validity of using the Polar RS800 heart rate monitor for heart rate variability research. *European Journal of Applied Physiology* [online]. **112**(12), 4179–4180. ISSN 1439-6327. Dostupné z: doi:10.1007/s00421-012-2453-2
- RABIAH, AB, KK RAMAKRISHNAN, Elizabeth LIRI a Koushik KAR, 2018. A lightweight authentication and key exchange protocol for IoT. In: *Proc. Workshop Decentralized IoT Secur. Standards (DISS)*.
- RADIN, Jennifer M., Nathan E. WINEINGER, Eric J. TOPOL a Steven R. STEINHUBL, 2020. Harnessing wearable device data to improve state-level real-time surveillance of influenza-like illness in the USA: a population-based study. *The Lancet Digital Health* [online]. **2**(2), e85–e93. ISSN 2589-7500. Dostupné z: doi:10.1016/S2589-7500(19)30222-5
- RATHORE, M. Mazhar, Awais AHMAD, Anand PAUL, Jiafu WAN a Daqiang ZHANG, 2016. Real-time Medical Emergency Response System: Exploiting IoT and Big Data for Public Health. *Journal of Medical Systems* [online]. **40**(12), 283. ISSN 1573-689X. Dostupné z: doi:10.1007/s10916-016-0647-6
- REZNIK, Alex, 2018. ETSI - ETSI Blog - What is Edge? *ETSI* [online] [vid. 2020-02-17]. Dostupné z: <https://www.etsi.org/newsroom/blogs/entry/what-is-edge>

- SANDERS, James, 2020. How to include edge computing in your 2020 IT budget. *ZDNet* [online] [vid. 2020-02-17]. Dostupné z: <https://www.zdnet.com/article/how-to-include-edge-computing-in-your-2020-it-budget/>
- SEC, David, Dalibor CIMR, Jan STEPAN, Richard CIMLER a Jitka KUHNOVA, 2018a. Automatic address assigning problem in smart homes. In: *2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* [online]. s. 1–6. ISSN null. Dostupné z: doi:10.1109/FUZZ-IEEE.2018.8491477
- SEC, David, Jan MATYSKA, Blanka KLIMOVA, Richard CIMLER, Jitka KUHNOVA a Filip STUDNICKA, 2018b. System for Detailed Monitoring of Dog's Vital Functions. In: Ngoc Thanh NGUYEN, Elias PIMENIDIS, Zaheer KHAN a Bogdan TRAWIŃSKI, ed. *Computational Collective Intelligence* [online]. Cham: Springer International Publishing, s. 426–435. Lecture Notes in Computer Science. ISBN 978-3-319-98443-8. Dostupné z: doi:10.1007/978-3-319-98443-8_39
- SEC, David, Lubos MERCL a Peter MIKULECKY, 2018c. Low Cost Architecture of Autonomous Subsystems for Internet of Things. In: Fernando DE LA PRIETA, Zita VALE, Luis ANTUNES, Tiago PINTO, Andrew T. CAMPBELL, Vicente JULIÁN, Antonio J.R. NEVES a María N. MORENO, ed. *Trends in Cyber-Physical Multi-Agent Systems. The PAAMS Collection - 15th International Conference, PAAMS 2017* [online]. Cham: Springer International Publishing, s. 39–49. Advances in Intelligent Systems and Computing. ISBN 978-3-319-61578-3. Dostupné z: doi:10.1007/978-3-319-61578-3_4
- SEC, David a Peter MIKULECKY, 2023. A System for Animal Health Monitoring and Emotions Detection. In: Nuno MONIZ, Zita VALE, José CASCALHO, Catarina SILVA a Raquel SEBASTIÃO, ed. *Progress in Artificial Intelligence* [online]. Cham: Springer Nature Switzerland, Lecture Notes in Computer Science, s. 41–52 [vid. 2024-03-17]. ISBN 978-3-031-49007-1. Dostupné z: doi:10.1007/978-3-031-49008-8_4

- SETO, Hiromitsu, Eitaro NISHIHARA, Yuki FUKUSHIMA a Mohammad Ali NEMATBAKHS, 2000. Medical support system [online]. US6157914A. [vid. 2020-03-10]. 5. prosinec 2000. Dostupné z: <https://patents.google.com/patent/US6157914A/en>
- SHA, Kewei, T. Andrew YANG, Wei WEI a Sadegh DAVARI, 2019. A survey of edge computing based designs for IoT security. *Digital Communications and Networks* [online]. [vid. 2020-03-05]. ISSN 2352-8648. Dostupné z: [doi:10.1016/j.dcan.2019.08.006](https://doi.org/10.1016/j.dcan.2019.08.006)
- SHAFFER, Fred a J. P. GINSBERG, 2017. An Overview of Heart Rate Variability Metrics and Norms. *Frontiers in Public Health* [online]. **5**, 258. ISSN 2296-2565. Dostupné z: [doi:10.3389/fpubh.2017.00258](https://doi.org/10.3389/fpubh.2017.00258)
- SHERWEN, Sally L. a Paul H. HEMSWORTH, 2019. The Visitor Effect on Zoo Animals: Implications and Opportunities for Zoo Animal Welfare. *Animals* [online]. **9**(6), 366. ISSN 2076-2615. Dostupné z: [doi:10.3390/ani9060366](https://doi.org/10.3390/ani9060366)
- SHI, Weisong, Jie CAO, Quan ZHANG, Youhuizi LI a Lanyu XU, 2016a. Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal* [online]. **3**(5), 637–646. ISSN 2327-4662. Dostupné z: [doi:10.1109/JIOT.2016.2579198](https://doi.org/10.1109/JIOT.2016.2579198)
- SHI, Weisong, Jie CAO, Quan ZHANG, Youhuizi LI a Lanyu XU, 2016b. Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal* [online]. **3**(5), 637–646. ISSN 2372-2541. Dostupné z: [doi:10.1109/JIOT.2016.2579198](https://doi.org/10.1109/JIOT.2016.2579198)
- SINGH, Ajit, 2019. *Edge Computing: Simply In Depth*. B.m.: Amazon Digital Services LLC - KDP Print US. ISBN 978-1-09-133529-5.
- SITTÓN-CANDANEDO, Inés, Ricardo S. ALONSO, Óscar GARCÍA, Lilia MUÑOZ a Sara RODRÍGUEZ-GONZÁLEZ, 2019. Edge Computing, IoT and Social Computing in Smart Energy Scenarios. *Sensors* [online]. **19**(15), 3353. Dostupné z: [doi:10.3390/s19153353](https://doi.org/10.3390/s19153353)
- SITTÓN-CANDANEDO, Inés, Ricardo S. ALONSO, Sara RODRÍGUEZ-GONZÁLEZ, José Alberto GARCÍA CORIA a Fernando DE LA PRIETA, 2020. Edge

Computing Architectures in Industry 4.0: A General Survey and Comparison. In: Francisco MARTÍNEZ ÁLVAREZ, Alicia TRONCOSO LORA, José António SÁEZ MUÑOZ, Héctor QUINTIÁN a Emilio CORCHADO, ed. *14th International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO 2019)* [online]. Cham: Springer International Publishing, s. 121–131. Advances in Intelligent Systems and Computing. ISBN 978-3-030-20055-8. Dostupné z: doi:10.1007/978-3-030-20055-8_12

SPOTIFY TECHNOLOGY S.A., 2019. *Spotify* [online] [vid. 2020-02-19]. Dostupné z: <https://www.spotify.com/us/>

STANCIU, Alexandru, 2017. Blockchain Based Distributed Control System for Edge Computing. In: *2017 21st International Conference on Control Systems and Computer Science (CSCS)* [online]. s. 667–671. ISSN 2379-0482. Dostupné z: doi:10.1109/CSCS.2017.102

STEJSKAL, Pavel, Radim ŠLACHTA, Milan ELFMARK, Jiří SALINGER a Petra GAUL-ALÁCOVÁ, 2002. SPECTRAL ANALYSIS OF HEART RATE VARIABILITY: NEW EVALUATION METHOD. *Acta Universitatis Palackianae Olomucensis. Gymnica.* **32**(2).

STEPAN, Jan, Richard CIMLER, Jan MATYSKA, David SEC a Ondrej KREJCAR, 2017a. Lightweight Protocol for M2M Communication. In: Ngoc Thanh NGUYEN, George A. PAPADOPOULOS, Piotr JĘDRZEJOWICZ, Bogdan TRAWIŃSKI a Gottfried VOSSSEN, ed. *Computational Collective Intelligence* [online]. Cham: Springer International Publishing, s. 335–344. Lecture Notes in Computer Science. ISBN 978-3-319-67077-5. Dostupné z: doi:10.1007/978-3-319-67077-5_32

STEPAN, Jan, Richard CIMLER, Jan MATYSKA, David SEC a Ondrej KREJCAR, 2017b. Lightweight Protocol for M2M Communication. In: Ngoc Thanh NGUYEN, George A. PAPADOPOULOS, Piotr JĘDRZEJOWICZ, Bogdan TRAWIŃSKI a Gottfried VOSSSEN, ed. *Computational Collective Intelligence* [online]. Cham: Springer International Publishing, Lecture Notes in Computer

- Science, s. 335–344 [vid. 2024-03-31]. ISBN 978-3-319-67076-8. Dostupné z: doi:10.1007/978-3-319-67077-5_32
- STRONG, V., S. W. BROWN a R. WALKER, 1999. Seizure-alert dogs — fact or fiction? *Seizure* [online]. **8**(1), 62–65. ISSN 1059-1311. Dostupné z: doi:10.1053/seiz.1998.0250
- SULTANA, S. a S. DIXIT, 2017. Indexes in PostgreSQL. In: [online]. s. 512–515. Dostupné z: doi:10.1109/ICIMIA.2017.7975511
- ŠKRAŇKOVÁ, Ivana, 2017. *Laboratorní práce z biofyziky - elektrokardiografie* [online]. B.m. [vid. 2020-02-17]. Bakalářská práce. Univerzita Hradec Králové, Přírodovědecká fakulta. Dostupné z: <https://theses.cz/id/x3v4nq/>
- TADI, Mojtaba Jafari, Eero LEHTONEN, Mikko PANKÄÄLÄ, Antti SARASTE, Tuija VASANKARI, Mika TERÁS a Tero KOIVISTO, 2016. Gyrocardiography: A new non-invasive approach in the study of mechanical motions of the heart. Concept, method and initial observations. In: *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* [online]. s. 2034–2037. ISSN 1557-170X. Dostupné z: doi:10.1109/EMBC.2016.7591126
- THOMAS, William B., 2010. Idiopathic Epilepsy in Dogs and Cats. *Veterinary Clinics of North America: Small Animal Practice* [online]. **40**(1), 161–179. ISSN 01955616. Dostupné z: doi:10.1016/j.cvsm.2009.09.004
- TULI, Shreshth, Nipam BASUMATARY, Sukhpal Singh GILL, Mohsen KAHANI, Rajesh Chand ARYA, Gurpreet Singh WANDER a Rajkumar BUYYA, 2020. HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. *Future Generation Computer Systems* [online]. **104**, 187–200. ISSN 0167-739X. Dostupné z: doi:10.1016/j.future.2019.10.043
- TYNAN, Dan, 2019. Will Edge Computing Transform Healthcare? *Technology Solutions That Drive Healthcare* [online] [vid. 2020-02-17]. Dostupné

z: <https://healthtechmagazine.net/article/2019/08/will-edge-computing-transform-healthcare>

UNWALA, Ishaq, Zafar TAQVI a Jiang LU, 2018. IoT Security: ZWave and Thread. In: *2018 IEEE Green Technologies Conference (GreenTech)* [online]. s. 176–182. ISSN 2166-5478. Dostupné z: [doi:10.1109/GreenTech.2018.00040](https://doi.org/10.1109/GreenTech.2018.00040)

USUI, Harunobu a Yusuke NISHIDA, 2017. The very low-frequency band of heart rate variability represents the slow recovery component after a mental stress task. *PLOS ONE* [online]. **12**(8), e0182611. ISSN 1932-6203. Dostupné z: [doi:10.1371/journal.pone.0182611](https://doi.org/10.1371/journal.pone.0182611)

VAISMAN, A., F. BESTEIRO a M. VALVERDE, 2019. Modelling and Querying Star and Snowflake Warehouses Using Graph Databases. *Communications in Computer and Information Science* [online]. **1064**, 144–152. Dostupné z: [doi:10.1007/978-3-030-30278-8_18](https://doi.org/10.1007/978-3-030-30278-8_18)

VARGHESE, Blesson, Nan WANG, Sakil BARBHUIYA, Peter KILPATRICK a Dimitrios S. NIKOLOPOULOS, 2016. Challenges and Opportunities in Edge Computing. In: *2016 IEEE International Conference on Smart Cloud (SmartCloud)* [online]. s. 20–26. ISSN null. Dostupné z: [doi:10.1109/SmartCloud.2016.18](https://doi.org/10.1109/SmartCloud.2016.18)

VETERINÁRNÍ KLINIKA NISA, 2019a. Co je normální. *Klinika NISA* [online] [vid. 2020-02-19]. Dostupné z: <https://www.klinikanisa.cz/co-je-normalni/>

VETERINÁRNÍ KLINIKA NISA, SMWORKS digital, 2019b. Jaké jsou normální fyziologické parametry. *Klinika NISA* [online] [vid. 2020-04-03]. Dostupné z: <https://www.klinikanisa.cz/jake-jsou-normalni-fyziologicke-parametry/>

VIRTANEN, Juhani, Sanni SOMPPPI, Heini TÖRNQVIST, Vala JEYHANI, Patrique FIEDLER, Yulia GIZATDINOVA, Päivi MAJARANTA, Heli VÄÄTÄJÄ, Anna VALLDEORIOLO CARDÓ, Jukka LEKKALA, Sampo TUUKKANEN, Veikko SURAKKA, Outi VAINIO a Antti VEKKAJOJA, 2018. Evaluation of Dry

- Electrodes in Canine Heart Rate Monitoring. *Sensors* [online]. **18**(6), 1757. Dostupné z: doi:10.3390/s18061757
- VOJTAS, Pavel, Jan STEPAN, David SEC, Richard CIMLER a Ondrej KREJCAR, 2018. Voice Recognition Software on Embedded Devices. In: Ngoc Thanh NGUYEN, Duong Hung HOANG, Tzung-Pei HONG, Hoang PHAM a Bogdan TRAWIŃSKI, ed. *Intelligent Information and Database Systems* [online]. Cham: Springer International Publishing, s. 642–650. Lecture Notes in Computer Science. ISBN 978-3-319-75417-8. Dostupné z: doi:10.1007/978-3-319-75417-8_60
- WAGNER, Galen S. a David G. STRAUSS, 2014. *Marriott's practical electrocardiography*. Twelfth edition. Philadelphia: Wolters Kluwer Health/Lippincott Williams & Wilkins. ISBN 978-1-4511-4625-7.
- WANG, Jianyu, Jianli PAN, Flavio ESPOSITO, Prasad CALYAM, Zhicheng YANG a Prasant MOHAPATRA, 2020. Edge Cloud Offloading Algorithms: Issues, Methods, and Perspectives. *ACM Computing Surveys* [online]. **52**(1), 1–23. ISSN 0360-0300, 1557-7341. Dostupné z: doi:10.1145/3284387
- WETTER, Dikr, 2023. /bin/bash based SSL/TLS tester: testssl.sh. *Testing TLS/SSL encryption* [online] [vid. 2023-07-18]. Dostupné z: <https://testssl.sh/>
- WIENS, Andrew D. a Omer T. INAN, 2015. A Novel System Identification Technique for Improved Wearable Hemodynamics Assessment. *IEEE Transactions on Biomedical Engineering* [online]. **62**(5), 1345–1354. ISSN 1558-2531. Dostupné z: doi:10.1109/TBME.2014.2387354
- WINSYSTEMS INC. COMPANY, 2017. *Cloud Computing - Fog Computing & Edge Computing: WinSystems* [online] [vid. 2020-02-17]. Dostupné z: <https://www.winsystems.com/cloud-fog-and-edge-computing-whats-the-difference/>
- WONDERMENTO INC., 2017. Wonderwoof. *Wonderwoof | The activity tracker for dogs* [online] [vid. 2020-02-17]. Dostupné z: <https://wonderwoof.com/>

- XIONG, Zehui, Yang ZHANG, Dusit NIYATO, Ping WANG a Zhu HAN, 2018. When Mobile Blockchain Meets Edge Computing. *IEEE Communications Magazine* [online]. **56**(8), 33–39. ISSN 1558-1896. Dostupné z: doi:10.1109/MCOM.2018.1701095
- XU, Boyi, Li Da XU, Hongming CAI, Cheng XIE, Jingyuan HU a Fenglin BU, 2014. Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services. *IEEE Transactions on Industrial Informatics* [online]. **10**(2), 1578–1586. ISSN 1941-0050. Dostupné z: doi:10.1109/TII.2014.2306382
- XU, Xiaolong, Qingxiang LIU, Yun LUO, Kai PENG, Xuyun ZHANG, Shunmei MENG a Lianyong QI, 2019. A computation offloading method over big data for IoT-enabled cloud-edge computing. *Future Generation Computer Systems* [online]. **95**, 522–533. ISSN 0167-739X. Dostupné z: doi:10.1016/j.future.2018.12.055
- YAN, Hongmei, Yingtao JIANG, Jun ZHENG, Chenglin PENG a Qinghui LI, 2006. A multilayer perceptron-based medical decision support system for heart disease diagnosis. *Expert Systems with Applications* [online]. **30**(2), 272–281. ISSN 0957-4174. Dostupné z: doi:10.1016/j.eswa.2005.07.022
- YANG, Chenxi a Negar TAVASSOLIAN, 2018. Combined Seismo- and Gyro-Cardiography: A More Comprehensive Evaluation of Heart-Induced Chest Vibrations. *IEEE Journal of Biomedical and Health Informatics* [online]. **22**(5), 1466–1475. ISSN 2168-2208. Dostupné z: doi:10.1109/JBHI.2017.2764798
- ZANETTI, John M. a Kouhyar TAVAKOLIAN, 2013. Seismocardiography: Past, present and future. In: *2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* [online]. s. 7004–7007. ISSN 1558-4615. Dostupné z: doi:10.1109/EMBC.2013.6611170
- ZHANG, Daniel, Nathan VANCE a Dong WANG, 2019. When Social Sensing Meets Edge Computing: Vision and Challenges. In: *2019 28th International Conference on Computer Communication and Networks (ICCCN)* [online]. s. 1–9. ISSN 1095-2055. Dostupné z: doi:10.1109/ICCCN.2019.8847174

ZHANG, Jiale, Bing CHEN, Yanchao ZHAO, Xiang CHENG a Feng HU, 2018. Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. *IEEE Access* [online]. **6**, 18209–18237. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2018.2820162

ZHAO, Neil, 2010. Full-Featured Pedometer Design Realized with 3-Axis Digital Accelerometer. **5**.

ZINK, Matthias Daniel, Christoph BRÜSER, Björn-Ole STÜBEN, Andreas NAPP, Robert STÖHR, Steffen LEONHARDT, Nikolaus MARX, Karl MISCHKE, Jörg B. SCHULZ a Johannes SCHIEFER, 2017. Unobtrusive Nocturnal Heartbeat Monitoring by a Ballistocardiographic Sensor in Patients with Sleep Disordered Breathing. *Scientific Reports* [online]. **7**(1), 1–13. ISSN 2045-2322. Dostupné z: doi:10.1038/s41598-017-13138-0

14 Seznam publikací autora

- SEC, D., & MIKULECKÝ, P. (2023). A System for Animal Health Monitoring and Emotions Detection. In EPIA Conference on Artificial Intelligence (pp. 41-52). Springer Nature Switzerland Cham.
- SEC, D., & MIKULECKÝ, P. (2019). Two Phase Failure Detection Using Fuzzy Logic. In Computational Collective Intelligence: 11th International Conference, ICCCI 2019, Hendaye, France, September 4--6, 2019, Proceedings, Part I 11 (pp. 271-282). Springer International Publishing.
- SEC, D., MERCL, L., & MIKULECKÝ, P. (2018). Low Cost Architecture of Autonomous Subsystems for Internet of Things. In Trends in Cyber-Physical Multi-Agent Systems. The PAAMS Collection-15th International Conference, PAAMS 2017 15 (pp. 39-49). Springer International Publishing.
- SEC, D., CIMR, D., STEPAN, J., CIMLER, R., & KUHNNOVA, J. (2018). Automatic address assigning problem in smart homes. In 2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE) (pp. 1-6). IEEE.
- SEC, D., MATYSKA, J., KLIMOVA, B., CIMLER, R., KUHNNOVA, J., & STUDNICKA, F. (2018). System for detailed monitoring of dog's vital functions. In Computational Collective Intelligence: 10th International Conference, ICCCI 2018, Bristol, UK, September 5-7, 2018, Proceedings, Part I 10 (pp. 426-435). Springer International Publishing.
- SEC, D., CIMR, D., STEPAN, J., CIMLER, R., & KUHNNOVA, J. (2018). Optimized Algorithm for Node Address Assigning in a Large-Scale Smart Automation Environment. In Computational Collective Intelligence: 10th International Conference, ICCCI 2018, Bristol, UK, September 5-7, 2018, Proceedings, Part II 10 (pp. 311-321). Springer International Publishing.

- VOJTAS, P., STEPAN, J., SEC, D., CIMLER, R., & KREJCAR, O. (2018). Voice recognition software on embedded devices. In *Intelligent Information and Database Systems: 10th Asian Conference, ACIIDS 2018, Dong Hoi City, Vietnam, March 19-21, 2018, Proceedings, Part I 10* (pp. 642-650). Springer International Publishing.
- MERCL, L., SEC, D., & SOBESLAV, V. (2018). Analysis of Frameworks for Building IaaS Cloud Using by Cloud Computing Providers. In *Advances on P2P, Parallel, Grid, Cloud and Internet Computing: Proceedings of the 12th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC-2017)* (pp. 655-663). Springer International Publishing.
- STEPAN, J., CIMLER, R., MATYSKA, J., SEC, D., & KREJCAR, O. (2017). Lightweight protocol for M2M communication. In *Computational Collective Intelligence: 9th International Conference, ICCCI 2017, Nicosia, Cyprus, September 27-29, 2017, Proceedings, Part II 9* (pp. 335-344). Springer International Publishing.
- SEC, D., MERCL, L., & MIKULECKÝ, P. (2017). Low Cost Architecture of Autonomous Subsystems for Internet of Things. In *PAAMS (Special Sessions)* (pp. 39-49).
- UNIVERZITA HRADEC KRÁLOVÉ. Systém pro monitoring vitálních funkcí zvířat na veterinární klinice, Původci: STUDNIČKA, Filip, R. CIMLER, J. KÜHNOVÁ, J. MATYSKA, J. ŠTĚPÁN, J. ŠLÉGR, D. ŠEC. Univerzita Hradec Králové, 2021. Identifikační číslo: 2021-UHK-PrF-Z-Poloprovoz-001.
- UNIVERZITA HRADEC KRÁLOVÉ. Aplikace s detekčními algoritmy pro ortopedická měření. Původci: STUDNIČKA, Filip, J. ŠLÉGR, R. CIMLER, J. ŠTĚPÁN, D. BUŠOVSKÝ, J. KÜHNOVÁ, J. MATYSKA, D. ŠEC. 2019.
- UNIVERZITA HRADEC KRÁLOVÉ. Cloudový systém pro online analýzu femoroacetabulární impingementu. Původci: STUDNIČKA, Filip, J. ŠLÉGR, J. KÜHNOVÁ, D. ŠEC, J. MATYSKA, R. CIMLER, J. ŠTĚPÁN, D. BUŠOVSKÝ. 2019.

- UNIVERZITA HRADEC KRÁLOVÉ. Systém pro měření ortopedického vyšetření.
Původci: ŠTĚPÁN, Jan, J. MATYSKA, R. CIMLER, F. STUDNIČKA, J. ŠLÉGR, J. KÜHNOVÁ, D. ŠEC, D. BUŠOVSKÝ, D. GLEVICKÝ. 2019.
Identifikační číslo: TG02010020.
- STUDNIČKA, Filip, J. ŠLÉGR, R. CIMLER, J. ŠTĚPÁN, J. KÜHNOVÁ, D. ŠEC.
Zařízení pro autodiagnostiku progresu artrózy a rozvoje femoroacetabulárního impingement syndromu u rizikových skupin - závěrečná zpráva.
- UNIVERZITA HRADEC KRÁLOVÉ. Zařízení pro sledování mikropohybů živých organismů, Původci: CIMLER, Richard, F. STUDNIČKA, J. ŠLÉGR, J. ŠTĚPÁN, J. MATYSKA, J. KÜHNOVÁ, D. ŠEC, P. ŠEBA 2019. Číslo patentu: 33574.
- CIMLER, Richard, J. KÜHNOVÁ, F. STUDNIČKA, D. ŠEC, J. MATYSKA, J. ŠLÉGR.
Závěrečná zpráva projektu CHOPN.
- CIMLER, Richard, F. STUDNIČKA, J. MATYSKA, J. ŠTĚPÁN, J. KÜHNOVÁ, J. ŠLÉGR, D. ŠEC. Závěrečná zpráva projektu Smart Furniture.
- UNIVERZITA HRADEC KRÁLOVÉ. Cloud system for gathering data from wearables and sending questionnaires. Původci: CIMLER, Richard, V. TICHÝ, J. KÜHNOVÁ, D. ŠEC. 2018.
- UNIVERZITA HRADEC KRÁLOVÉ. Cloudový systém pro sběr senzorických dat. Původci: CIMLER, Richard, J. ŠTĚPÁN, J. KÜHNOVÁ, F. STUDNIČKA, D. ŠEC, J. ŠLÉGR, J. MATYSKA, D. GLEVICKÝ. 2018.
- UNIVERZITA HRADEC KRÁLOVÉ. Modul precizního sigma-delta převodníku. Původci: ŠTĚPÁN, Jan, J. MATYSKA, R. CIMLER, J. ŠLÉGR, F. STUDNIČKA, J. KÜHNOVÁ, D. ŠEC. 2018. Identifikační číslo: TG02010020.
- UNIVERZITA HRADEC KRÁLOVÉ. Modul pro ovládání relé. Původci: ŠTĚPÁN, Jan, J. MATYSKA, R. CIMLER, J. ŠLÉGR, F. STUDNIČKA, J. KÜHNOVÁ, D. ŠEC. 2018. Identifikační číslo: TG02010020.

UNIVERZITA HRADEC KRÁLOVÉ. Ovládací modul pro LED pásy. Původci: ŠTĚPÁN, Jan, J. MATYSKA, R. CIMLER, J. ŠLÉGR, F. STUDNIČKA, J. KÜHNOVÁ, D. ŠEC. 2018. Identifikační číslo: TG02010020.

UNIVERZITA HRADEC KRÁLOVÉ. Podpůrná aplikace pro pacienty s CHOPN. Původci: CIMLER, Richard, D. ŠEC, D. GLEVICKÝ, J. MATYSKA, J. KÜHNOVÁ, F. STUDNIČKA, J. ŠLÉGR, J. ŠTĚPÁN. 2018.

CIMLER, Richard, F. STUDNIČKA, J. MATYSKA, J. ŠTĚPÁN, J. KÜHNOVÁ, J. ŠLÉGR, D. ŠEC. Průběžná zpráva projektu Smart Furniture Q1/2018.

CIMLER, Richard, F. STUDNIČKA, J. MATYSKA, J. ŠTĚPÁN, J. KÜHNOVÁ, J. ŠLÉGR, D. ŠEC. Průběžná zpráva projektu Smart Furniture Q2/2018.

15 Seznam projektů a podíl autora na jednotlivých projektech

SPEV 2017 FIM – Smart Solutions for Ubiquitous Computing Environments (řešitel:
Doc. Krejcar)

- člen týmu, řešení úkolů z oblasti IoT

Exceclence FIM 2017 – Modelování a simulace procesů v socioekonomických systémech
a inteligentních prostředích

- člen týmu, řešení úkolů z oblasti IoT

Grant PřF TAČR GAMA 2017 – programátor - RNDr. Filip Studnička, Ph.D.

- tvorba řešení pro zpracování dat na speciálním hardwaru

GA 15-11724S DEPIES FIM – Decision Processes in Intelligent Environments (řešitel
prof. Mikulecký)

- Výzkum v oblasti řízení inteligentní domácnosti. implementace serverové části komunikace, tvorba pravidlového systému a systém poskytování dat.

UHK specific research project 2017 FIM – Computer Networks for Cloud, Distributed Computing, and Internet of Things II (řešitel: prof. Mikulecký)

- Výzkum v oblasti adresace zařízení a tvorba simulačního nástroje ověřujícího funkčnosti navrženého řešení.
- Výzkum v oblasti sběru surových dat z nositelných zařízení. Implementace systému pro sběr vitálních dat psů z bezdrátových senzorů a jejich poskytování pro vyhodnocení.

TAČR EPSILON TH03010415 (5615) PřF – Vývoj inteligentního systému elektronického řízení specializovaného nemocničního lůžka pro pacienty v kritickém stavu. (RNDr. Filip Studnička, Ph.D.)

- Technický pracovník zajišťující podpurná měření a zpracování dat.

TAČR TJ02000155 ZETA PřF – Smart Vet

- Tvorba a implementace systému pro měření a vyhodnocení dat ze senzorů

TAČR GAMA TG02010020 PřF – Zařízení pro diagnostiku femoroacetabulární impingementu. Systém pro automatické rychlé stanovení klinicky významných analytů ze senzorů a) Mikrofluidních systémů, případně technologie Lab On Chip b) DNA čipové technologie c) Molekulárních sensorů umístěných na těle pacientů.

- Návrh a implementace systému

C2P s.r.o. PřF – (2301)

- Výzkum v oblasti zpracování a vyhodnocení medical dat.

TAČR GAMA TG02010020 Health React (9403) PřF – výzkum v oblasti sběru a zpracování dat z nositelných zařízení.

- Vývoj systému zpracování dat ze služeb Fitbit, Garmin a Polar. Poskytování dat pro další analýzy tvorba pravidelných reportů.

OP PIK Inovační voucher CZ.01.1.02/0.0/0.0/16_045/0010984 PřF – Vývoj systému pro sběr dat z wearable zařízení

- Systém pro sběr dat ze Smart zařízení Android Wear.

OP PIK Inovační voucher CZ.01.1.02/0.0/0.0/17_205/0015892 PřF – Vnitřní monitorovací systém NEXARS

- Vývoj SW platformy pro řízení a zobrazování veličin z měřeného prostředí

Smluvní výzkum pro OSU CZ.02.1.01/0.0/0.0/16_019/0000798 PřF – Healthy Aging in Industrial Environment HAIE – rozvoj multioborového výzkumu, zaměřeného na zkoumání vlivů vybraných faktorů životního prostředí, životního stylu a pohybové aktivity na zdraví a stárnutí populace. Do projektu jsou zapojena 4 VaV centra.

- Vývoj platformy pro sběr poskytování a vyhodnocení dat.

FV40231 MPO Trio (5104) PřF – Inovativní platforma pro stanovení bioaktivních látek

- Návrh a vývoj systému pro ukládání nově vyvinutých biochemických sloučenin v oblasti zdravotnictví.

TAČR GAMA TG02010020 PřF – Smart Furniture

- Sběr dat ze senzorů a tvorba vyhodnocovacího SW

GAMA TG02010020 PřF – Diagnostický systém monitorování fitness s vizí využití pacienty CHOPN

- Sběr dat ze senzorů, implementace systému, vytváření online reportů

ZÉTA TJ02000155 – Smart Vet

- Návrh systému, zpracování dat ze senzorů a tvorba vyhodnocovacího SW, Implementace edge node a cloudové části aplikace.

16 Přílohy

Příloha 1: Seznam dostupných šifer protokolů TLSv1.2 a TLSv1.3

```
Testing server's cipher preferences
-----
Hexcode Cipher Suite Name (OpenSSL)      KeyExch.  Encryption  Bits      Cipher Suite Name (IANA/RFC)
-----
SSLv2
-
SSLv3
-
TLSv1 (server order)
-
TLSv1.1 (server order)
-
TLSv1.2 (server order -- server prioritizes ChaCha ciphers when preferred by clients)
xc030  ECDHE-RSA-AES256-GCM-SHA384           ECDH 256  AESGCM     256      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
xc02f  ECDHE-RSA-AES128-GCM-SHA256           ECDH 256  AESGCM     128      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
xcca8  ECDHE-RSA-CHACHA20-POLY1305           ECDH 256  ChaCha20   256      TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
xc028  ECDHE-RSA-AES256-SHA384               ECDH 256  AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
xc027  ECDHE-RSA-AES128-SHA256               ECDH 256  AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
xc014  ECDHE-RSA-AES256-SHA                  ECDH 256  AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
xc013  ECDHE-RSA-AES128-SHA                  ECDH 256  AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
x9d    AES256-GCM-SHA384                     RSA      AESGCM     256      TLS_RSA_WITH_AES_256_GCM_SHA384
x9c    AES128-GCM-SHA256                     RSA      AESGCM     128      TLS_RSA_WITH_AES_128_GCM_SHA256
x3d    AES256-SHA256                         RSA      AES         256      TLS_RSA_WITH_AES_256_CBC_SHA256
x3c    AES128-SHA256                         RSA      AES         128      TLS_RSA_WITH_AES_128_CBC_SHA256
x35    AES256-SHA                             RSA      AES         256      TLS_RSA_WITH_AES_256_CBC_SHA
x2f    AES128-SHA                             RSA      AES         128      TLS_RSA_WITH_AES_128_CBC_SHA
TLSv1.3 (server order -- server prioritizes ChaCha ciphers when preferred by clients)
x1302  AEAD-AES256-GCM-SHA384                ECDH 253  AESGCM     256      TLS_AES_256_GCM_SHA384
x1303  AEAD-CHACHA20-POLY1305-SHA256         ECDH 253  ChaCha20   256      TLS_CHACHA20_POLY1305_SHA256
x1301  AEAD-AES128-GCM-SHA256                 ECDH 253  AESGCM     128      TLS_AES_128_GCM_SHA256
x1305  TLS_AES_128_CCM_8_SHA256               ECDH 253  AESCCM8    128      TLS_AES_128_CCM_8_SHA256
x1304  TLS_AES_128_CCM_SHA256                 ECDH 253  AESCCM     128      TLS_AES_128_CCM_SHA256

Has server cipher order?      yes (OK) -- TLS 1.3 and below
```

Příloha 2: Informace o TLS certifikátu

Testing robust forward secrecy (FS) -- omitting Null Authentication/Encryption, 3DES, RC4

```
FS is offered (OK)      AEAD-AES256-GCM-SHA384 AEAD-CHACHA20-POLY1305-SHA256 ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-CHACHA20-POLY1305
AEAD-AES128-GCM-SHA256 TLS_AES_128_GCM_SHA256 TLS_AES_128_GCM_SHA256
ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA
Elliptic curves offered: prime256v1 X25519
TLS 1.2 sig_algs offered: RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384 RSA-PSS-RSAE+SHA512 RSA+SHA256 RSA+SHA384
RSA+SHA512 RSA+SHA224 RSA+SHA1
TLS 1.3 sig_algs offered: RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384 RSA-PSS-RSAE+SHA512
```

Testing server defaults (Server Hello)

```
TLS extensions (standard) "renegotiation info/#65281" "server name/#0" "EC point formats/#11"
"session ticket/#35" "status request/#5" "next protocol/#13172"
"supported versions/#43" "key share/#51" "max fragment length/#1"
"application layer protocol negotiation/#16"
Session Ticket RFC 5077 hint 83100 seconds, session tickets keys seems to be rotated < daily
SSL Session ID support yes
Session Resumption Tickets: yes, ID: yes
TLS clock skew Random values, no fingerprinting possible
Certificate Compression none
Client Authentication none
Signature Algorithm SHA256 with RSA
Server key size RSA 2048 bits (exponent is 65537)
Server key usage Digital Signature, Key Encipherment
Server extended key usage TLS Web Server Authentication, TLS Web Client Authentication
Serial 04E7B96E0C39D141F36BC4570579FF2D3FE6 (OK: length 18)
Fingerprints SHA1 1833A1FE21C1AA735E17D067AF3C88566F2BDF83
SHA256 3EA0A01528FE3759D88EDAC8FD1AF21CF2D1E32A4DDFD9748A2D4694ED9C9293
Common Name (CN) vetsapp.online (request w/o SNI didn't succeed)
subjectAltName (SAN) vetsapp.online broker.vetsapp.online
Trust (hostname) Ok via SAN (SNI mandatory)
Chain of trust Ok
EV cert (experimental) no
Certificate Validity (UTC) 66 >= 30 days (2023-06-25 18:54 --> 2023-09-23 18:54)
ETS/"eTLS", visibility info not present
Certificate Revocation List --
OCSP URI http://r3.o.lencr.org
OCSP stapling offered, not revoked
OCSP must staple extension --
DNS CAA RR (experimental) not offered
Certificate Transparency yes (certificate extension)
Certificates provided 3
Issuer R3 (Let's Encrypt from US)
Intermediate cert validity #1: ok > 40 days (2025-09-15 16:00). R3 <-- ISRG Root X1
#2: ok > 40 days (2024-09-30 18:14). ISRG Root X1 <-- DST Root CA X3
Intermediate Bad OCSP (exp.) Ok
```

Příloha 3: Přehled nastavení prahových hodnot a zasílání notifikací

Detekce anomálií (24 hodinový přehled)

HR: 40 - 80;BR: 10 - 20 [Upravit](#)

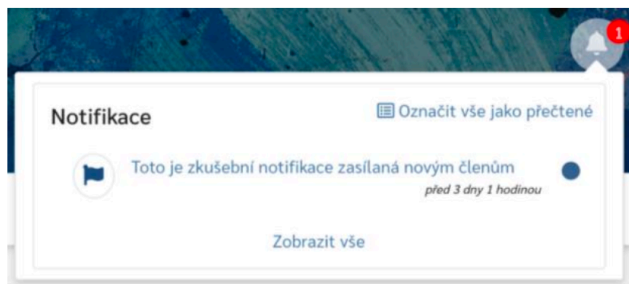
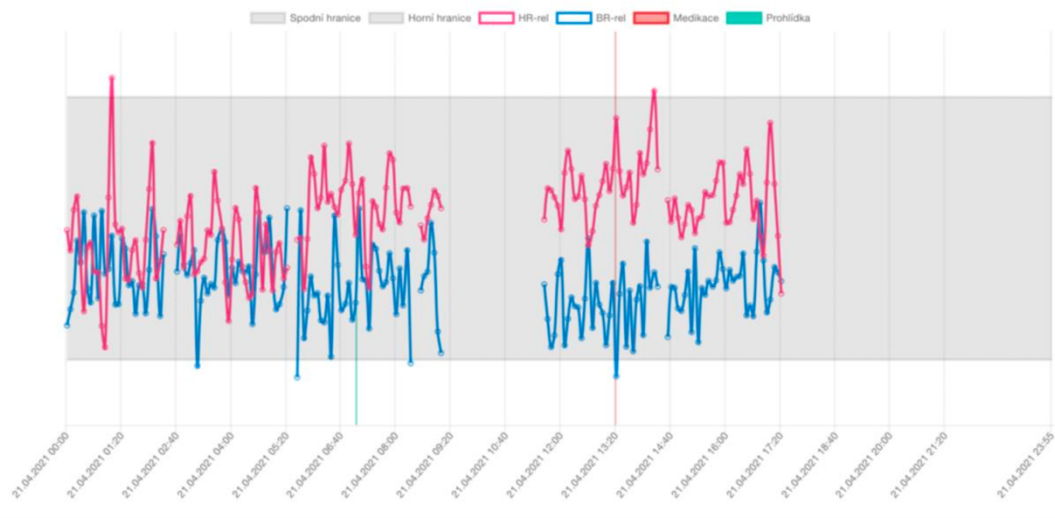
HR
Mezi 40 a 80 BPM

BR:
Mezi 10 a 20 nádechy za minutu

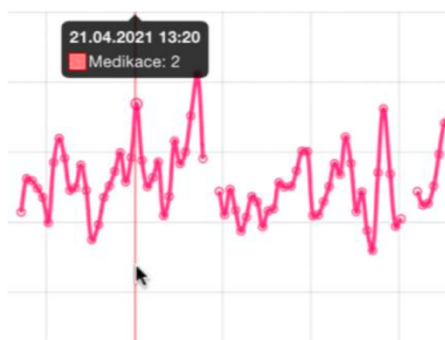
[Uložit](#)

Detekce anomálií (24 hodinový přehled)

HR: 40 - 80; BR: 10 - 20 Upravit



Příloha 4: Vkládání záznamů o medikaci



Medikace časová osa

- Medikace**
 Biocan T (Bioveta) 2.0 mL
 18.04.2020 10:55, Administrátor
- Inspekce**
 Vizuální kontrola, vše v pořádku. 🙌
 8 hodinami, Administrátor
- Medikace**
 Biocan DHPPI+L (Bioveta) 2.0 mL
 1 hodinou, Administrátor
- Medikace**
 Caniverm (Bioveta) 38.0
 1 hodinou, Administrátor

Medikace

Druh: Medikace

Datum: 📅

Obecný název:

Označení výrobce:

Množství: Zvolte jednotky

Inspekce

Druh: Inspekce

Datum: 📅

Popis:

Druh: Vyberte jednu z možností

- Medikace
- Inspekce