VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra kybernetiky a biomedicínského inženýrství

Vestavěný biometrický systém pro identifikaci osob ve zdravotnickém zařízení založený na principech otisku prstu

Embedded Biometric System for Personal Identification in Medical Facility Based on Fingerprint Analysis

2018 Bc. Matouš Procházka

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra kybernetiky a biomedicínského inženýrství

Zadání diplomové práce

Student: **Bc. Matouš Procházka**

Studijní program: N2649 Elektrotechnika

Studijní obor: 3901T009 Biomedicínské inženýrství

Téma: Vestavěný biometrický systém pro identifikaci osob ve zdravotnickém zařízení založený na principech otisku prstu
Embedded Biometric System for Personal Identification in Medical Facility Based on Fingerprint Analysis

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Analýza oblasti zpracování biometrické obrazové informace se zaměřením na otisk prstu.
2. Rozbor současné problematiky identifikace osob ve zdravotnických zařízeních.
3. Návrh vestavěného systému pro identifikaci osob pomocí otisku prstu s použitím bezdrátové technologie WiFi a síťového datového úložiště typu NAS.
4. Realizace a testování vestavěného systému pro identifikaci osob pomocí otisku prstu s použitím bezdrátové technologie WiFi a síťového datového úložiště typu NAS.
5. Analýza výsledného systému a srovnání se zjednodušeným prototypem vestavěného zařízení pro identifikaci osob.
6.Zhodnocení dosažených výsledků a stanovení užitečnosti v praxi.

Seznam doporučené odborné literatury:

[1] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* 1. vyd. Praha: Grada, 631 s., 32 s. obr. příl. Profesionál. ISBN 978-8024723655.
[2] FRISCH, P., S. MIODOWNIK, P. BOOTH, P. CARRAGEE a R.N.M. DOWLING. Patient centric identification and association. In: *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society* [online]. IEEE, 2009, s. 1722-1725 [cit. 2017-02-16]. DOI: 10.1109/IEMBS.2009.5333558. Dostupné z: http://ieeexplore.ieee.org/document/5333558/.
[3] ŠČUREK, R. *Biometrické metody identifikace osob v bezpečnostní praxi.* studijní text. Ostrava: VŠB - TU Ostrava, 2008, 34-43 s.
[4] OMAR, Hangaw Qader, Abdulqadir KHOSHNAW a Wrya MONNET. Smart patient management, monitoring and tracking system using radio-frequency identification (RFID) technology. In: *2016 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES)* [online]. IEEE, 2016, s. 40-45 [cit. 2017-02-16]. DOI: 10.1109/IECBES.2016.7843411. Electronic ISBN 978-1-4673-7791-1. Dostupné z: http://ieeexplore.ieee.org/document/7843411/

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Zdeněk Macháček, Ph.D.**

Konzultant diplomové práce: doc. Ing. Martin Augustynek, Ph.D.

Datum zadání: 01.09.2017

Datum odevzdání: 30.04.2018

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky 1D16 OSTRAVA

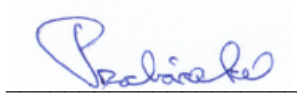
doc. Ing. Jiří Koziorek, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě, dne: 27. 4. 2018



Bc. Matouš Procházka

Poděkování

Mé poděkování patří především vedoucímu Ing. Zdeňku Macháčkovi, PhD. za odborný dohled, cenné rady a kvalitní vedení diplomové práce. Za věcné připomínky a vstřícnost při konzultacích chci také poděkovat MUDr. Františku Jurkovi a týmu z IT oddělení FNO zejména Ing. Miroslavu Krupovi MBA.

Abstrakt

Cílem této diplomové práce je vytvoření komplexního vestavěného zařízení a systému, který by zajišťoval bezpečný proces identifikace pacienta v rámci léčebných postupů a každodenních rutinních činností personálu. Ve své práci se zaměřuji především na popis principu moderních metod identifikace osob, technologií zpracování obrazové informace se zaměřením na otisk prstu a také se věnuji síťovým prostředkům a komunikačním rozhraním, související se síťovým úložištěm, databází a Wi-Fi modulem pro bezdrátový přenos osobních informací pacienta mezi koncovým systémem a databází. Výsledkem práce je fyzický přístroj, který je plně přenosný a umožňuje provádět biometrickou identifikací pacientů, kteří jsou registrovaní v centrální databázi. Tu je možné plně editovat skrz vytvořenou aplikaci pro stolní počítače a pracovní stanice umístěné na zdravotnických odděleních. Účelem této práce bylo navrhnout a vytvořit moderní a bezpečnější identifikační nástroj, který by byl schopen plně nahradit stávající řešení v podobě zápěstních náramků ať už ručně psaných s čárovým kódem nebo RFID čipem. Celý systém je navržen tak aby co nejlépe splňoval nově přijaté nařízení EU o ochraně osobních údajů tzv. GDPR.

Klíčová slova

Identifikace osob, papilární linie, biometrie, senzory otisku prstu, daktyloskopie, FAR, FRR, bezdrátové sítě, NAS server, databáze, MySQL, C/C++, PHP, Arduino, TCP/IP, HTTPS, záloha informací, RAID, IEEE 802.11b/g/n, Wi-Fi modul ESP-07, GDPR, mikrokontrolér, obrazová segmentace a skeletizace

Abstract

The subject of this diploma thesis is to create a complex integrated device and system that will ensure a secure process of patient identification within the therapeutic procedures and everyday routine activities of the medical employees. In my own work I primarily focuse on description of principles for modern methods of personal identification, fingerprint image processing technology and I also devote on network equipment and communication interfaces related to the network storage, database and Wi-Fi module for wireless transmission of patient's personal information between end system and databases. The result of the work is a physical device that is fully portable and allows the biometric identification of patients who are directly registered in the central database. This can be fully edited through a desktop application and a workstation located in healthcare departments. The purpose of this work was to design and create a modern and safer identification tool that would be able to fully replace existing solutions in the form of wristbands either manually typed with a barcode or RFID chip. The whole system is designed to best meet the newly adopted EU Privacy Act, the so-called GDPR.

Key Words

Personal identification, papilar lines, biometrics, fingerprint sensors, dactyloscopy, FAR, FRR, wireless network, NAS server, database, MySQL, C/C++, PHP, Arduino, TCP/IP, HTTPS, information backup, RAID, IEEE 802.11b/g/n, Wi-Fi module ESP-07, GDPR, microcontroller, image post-processing

OBSAH

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

A/D (AC/DC)	analogově digitální převodník
AES	standard pokročilého šifrování
AFIS	mezinárodní systém a databáze otisků
AP	přístupový bod bezdrátové sítě
ARM	označení architektury mikroprocesorů
ASCII	kódová tabulka definující znaky anglické abecedy a znaky používané v informatice
AT	označení příkazů ovládající modemy a síťové prvky
Bd	jednotka modulační rychlosti
CAN	sběrnice, využívaná nejčastěji pro vnitřní komunikační síť senzorů v automobilu
CCD	elektronická součástka používaná pro snímání obrazové informace
CE	označení výrobku, který má doložené posouzení o shodě před uvedením na trh EHS
CELP	kódovací algoritmus pro hlasové záznamy
CMOS	technologie výroby integrovaných obvodů (čipů)
CNC	číslicové řízení obráběcích strojů
COM	hardwarové označení pro počítačový vstup
CSS	jazyk pro popis způsobu zobrazení elementů na internetových stránkách
ČTÚ	český telekomunikační úřad
DAS	datový nosič přímo spojený s počítačem, který k němu přistupuje
DES	symetrická šifra používaná v kryptografii
DHPC	protokol umožňující nastavovat stanicím v počítačové síti IP adresu
DLNA	standard podporující sdílení multimediálních souborů v rámci sítě
DNA	deoxyribonukleová kyselina – nositel genetické informace
DPS	deska plošných spojů
EEPROM	elektricky vymazatelná počítačová paměť
EER	míra vyrovnaných chyb
FAR	chybné přijetí osoby při identifikaci
FLASH	elektricky programovatelná počítačová paměť
FMR	míra chybné shody
FNMR	míra chybné neshody
FRR	chybné odmítnutí osoby při identifikaci
FTA	míra neschopnosti snímat biometrický otisk
FTE	míra neschopnosti registrovat biometrický otisk
FTP	protokol pro přenos souborů mezi počítači pomocí počítačové sítě
GDPR	obecné nařízení EU o ochraně osobních údajů
GND	elektrické uzemnění
GPIO	piny pro uživatelsky nastavitelné hardwarové rozhraní
GPS	globální polohový systém
GSM	standard pro mobilní telefony a telefonní sítě
HDD	zařízení k dočasnému nebo trvalému uložení většího množství dat
HTML	jazyk používaný pro tvorbu webových stránek
HTTP(s)	internetový protokol pro výměnu hypertextových dokumentů ve formátu HTML
IEC	mezinárodní elektrotechnická komise
ID	symbol identifikace ve výpočetní technice
IoT	síť označující vzájemné datové propojení elektronických zařízení skrz internet
IP	logická adresa identifikující síťové rozhraní
I2C	počítačová sériová sběrnice pro připojení nízko rychlostních periferií
JBOD	označení způsobu uložení dat na síťových úložištích
JPEG	metoda ztrátové komprese používané pro ukládání počítačových obrázků
LAN	označení pro počítačovou síť, která pokrývá malé geografické území
LCD	tenké a ploché zobrazovací zařízení

LED	polovodičová elektronická součástka emitující světlo
LoRa	řešení pro bezdrátový přenos dat, kdy je hlavním cílem co nejnižší spotřeba výkonu
LTE	technologie určená pro vysokorychlostní internet v mobilních sítích
MAC	fyzická adresa síťové karty
MAN	rozlehlá počítačová síť, obvykle zasazená do města
MCU	integrovaný obvod, obsahující mikroprocesor a periferie
MySQL	systém řízení báze dat uplatňující relační databázový model
mAh	jednotka akumulátorové kapacity, která dodává proud do obvodu za jednotku času
NAS	síťové datové úložiště
Ni-Mh	nikl-metal hydridový akumulátor
OFDM	širokopásmová modulace využívající frekvenční dělení kanálu
PDA	palmtop, malý kapesní počítač
PGP	počítačový program, který umožňuje šifrování a podepisování
PHP	skriptovací jazyk, určený pro programování dynamických internetových stránek
PIN	identifikátor, pomocí kterého je možné se autorizovat
POP	internetový protokol pro stahování e-mailů ze vzdáleného serveru na klienta
PVC	polyvinylchlorid
PWM	diskrétní modulace pro přenos analogového signálu pomocí dvouhodnotového signálu
QR	kód pro automatizovaný sběr dat
QVGA	termín používaný pro počítačovou obrazovku s rozlišením 320 × 240
RAID	metoda zabezpečení dat proti selhání pevného disku
RC	technologie pro ovládání zařízení pomocí rádiových vln
RFID	identifikace na rádiové frekvenci
ROM	typ elektronické paměti, jejíž obsah je dán při výrobě
RX	elektronický pin pro příjem dat
SAN	datová síť, která slouží pro připojení externích zařízení k serverům
Sb.	označení sbírky zákona
SCSI	standardní rozhraní a sada příkazů pro výměnu dat mezi externími počítači a sběrnicí
SD	paměťová karta používaná v přenosných zařízeních včetně
SDRAM	paměť typu DRAM se synchronním způsobem přenosu dat
SFTP	protokol a program pro bezpečný přenos souborů pomocí počítačové sítě
SMS	telefonní služba pro posílání zpráv
SMTP	internetový protokol určený pro přenos zpráv elektronické pošty
SPI	sériové periferní rozhraní
SRAM	polovodičová paměť typu RAM realizovaná bistabilním klopným obvodem
SSD	typ datového média, které neobsahuje pohyblivé mechanické části
SSL	protokol poskytující zabezpečení komunikace šifrováním a autentizací
SSH	zabezpečený komunikační protokol v počítačových sítích
SSID	identifikátor bezdrátové sítě Wi-Fi
SQL	strukturovaný dotazovací jazyk, pro práci s daty v relačních databázích
TCP/IP	sada protokolů pro komunikaci v počítačové síti
TTL	standard používaný pro implementaci integrovaných obvodů
TX	elektronický pin pro odesílání dat
USART	synchronní / asynchronní sériové rozhraní pro komunikaci mezi zařízeními
USB	univerzální sériová sběrnice, moderní způsob připojení periferií k počítači
U-FL	typ konektoru pro připojení koaxiální antény
V	jednotka elektrického napětí
VoIP	technologie, umožňující přenos digitalizovaného hlasu
WAN	počítačová síť, která pokrývá rozlehlé geografické území
WLAN	bezdrátová počítačová síť, která spojuje dvě nebo více zařízení
WEP	označení pro zastaralé zabezpečení bezdrátových sítí
WPA	obchodní označení pro zabezpečení bezdrátových sítí
Wi-Fi	označení pro několik standardů IEEE 802.11 popisujících bezdrátovou komunikaci

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK A GRAFŮ

ÚVOD

Biometrie jako prvek moderních informačních technologií je v dnešní době důležitou a nedílnou součástí bezpečnostních aplikací určených pro správu veřejného sektoru a kontroly osobních informací. Stále častěji se s ní můžeme setkat v oblasti osobních mobilních aplikacích pro účely autentizace daných technologií a jejich majitelů. Hovoří se také o rostoucí tendenci lépe zabezpečovat zneužitelná data, firemní a osobní informace nebo například platební transakce. Ještě před dvaceti lety byla biometrická identifikace pouze okrajovou záležitostí výpočetní technologie, tehdy byly veškeré osobní informace ukládány v převážné většině do papírových dokumentací, které dnes již nejsou vyhovujícím standardem v nakládání s citlivými údaji. Velkou zásluhou na vývoji a začlenění moderní biometrie do běžného života patří vznik polovodičových senzorů detekující obrazové informace, miniaturizace komplexních součástek, vznik programových algoritmů pro analýzu a extrakci obrazových dat nebo také modernizace počítačových sítí. Hlavní úlohou této diplomové práce je sjednotit nejmodernější dostupné prvky biometrických aplikací současně s výpočetní technikou a vytvořit ucelený systém, který je schopen identifikovat a zároveň zobrazit základní osobní anamnézu pacientů ve zdravotnických zařízeních.

Diplomová práce je rozdělena na dvě základní části, a to na teoretickou a praktickou. V první části se věnuji komplexnímu popisu základních biometrických pojmů spolu s biometrií otisku prstu a vysvětlením identifikačních a autentizačních procesů. Značnou část tvoří podrobný popis anatomické oblasti složení všech kožních i podkožních struktur prstu jako je epidermis, dermis a tela subcutanea včetně fyziologických funkcí pokožky. Další kapitoly se orientují na historii snímání otisků prstů včetně představení prvních zakladatelů moderní daktyloskopie jakožto nejčastěji používané kriminalistické technice. Otisk prstu coby klíčové téma teoretické části je podrobně popsán také v dalších kapitolách zabývajících se celým identifikačním procesem jako je snímání, počítačové předzpracování a extrakce obrazových markerů z šablony otisku. Toto téma těsně souvisí s popisem základních principů fungování biometrických senzorů na otisky prstů, které rozděluji na snímače kontaktní a bezkontaktní. Poslední kapitoly teoretické části jsou směřovány k části praktické, která popisuje samotný vývoj a sestavení fyzického zařízení a softwaru. Jsou tak objasněny pojmy z oborů zdravotnických systémů pro kontrolu pacientů, bezdrátových technologiích pro přenos informací nebo strukturu síťových datových úložišť.

Druhá, praktická část diplomové práce je orientována především na návrh a následnou realizací fyzického vestavěného zařízení s importovaným softwarem pro komunikaci mezi senzorem otisku prstů, řídícím modulem, databází pacientů a uživatelskou aplikací pro stolní počítače. Konkrétně jsou popsány síťové komunikační protokoly a software jak pro desktopový systém Windows, vestavěné zařízení tak i pro samotný optický senzor otisků. Nemalou část tvoří detailní popis všech použitých komponentů jako je základní vývojová deska, biometrický senzor, bezdrátový síťový Wi-Fi modul, dotykový LCD displej a akumulátorové obvody pro napájení zařízení. Jelikož je tato diplomová práce určitým navázáním na mou bakalářskou práci, porovnávám technické a funkční zpracování prototypového systému s nově sestaveným modernějším a sofistikovanějším zařízením. Další kapitolu praktické části tvoří podrobná charakteristika všech ovládacích scriptů naprogramovaných v jazycích C/C++, Wiring, MySQL a PHP. V několika posledních kapitolách se věnuji, testování funkčnosti celého systému, statistickým výpočtům rychlosti a přesnosti biometrické identifikace pacientů a výdrži bateriového zdroje napájení. Vlastní poznatky, výpočty a realizace funkčních součástí vestavěného zařízení podkládám obrázky, grafy a tabulkami společně s řešeními konkrétních problémů.

TEORETICKÁ ČÁST

1 BIOMETRIE JAKO VĚDNÍ DISCIPLÍNA

1.1 ÚVOD DO BIOMETRIE

Pod pojmem biometrie rozumíme vědní disciplínu, která se zabývá studiem a poznáváním biologických organismů, především lidských anatomických a fyziologických příznaků. Slovo biometrie má původ ve dvou řeckých slovech a to „bios“ což znamená život a „metron“ tedy měřítko. V oblasti informačních technologiích se biometrický systém využívá k rozpoznávání vzorů lidské identity jako je např. obličej, otisk prstu, sítnice nebo duhovka. Tyto vzory jsou charakterizovány anatomickými rysy a jsou nejčastěji používaným prostředkem pro identifikaci osob. Opakem mohou být rysy behaviorální, ty jsou zaměřeny na chování člověka, pohyb nebo styl písma. Jiný úhel pohledu na obor biometrie může mít oblast biomedicíny, která se zabývá např. statistikou v medicíně, biologii nebo také antropometrii. Antropometrie má velmi blízko k biometrii. Má za úkol měření, záznam a vyhodnocování lidských fyziologických rozměrů, které můžeme dále využít pro identifikaci či verifikaci osoby. [1, 3]

K nesporným výhodám biometrie řadíme jedinečnost a unikátnost biologických znaků člověka, které nejsou ve velké většině zaměnitelné, biometrie také zvyšuje zabezpečení důležitých osobních údajů a odrazuje tak potencionální útočníky od jejich odcizení. Dále zvyšuje pohodlí uživatele biometrických systémů a díky vysoké technologické přesnosti eliminuje možnost popření identifikace člověka. Biometrický systém má samozřejmě také své nevýhody, kterými může být napadnutelnost neoprávněnou osobou zvenčí, díky tomu pak nezachovává stoprocentní soukromí. Dalším případem jsou vysoké náklady na výrobu a vývoj takového systému, který ve výsledku nemusí být přesný a spolehlivý. Jak již bylo zmíněno, biometrický systém má i své určité nevýhody. Mezi jednu z největších nevýhod patří zmanipulování identifikačního nebo verifikačního systému přímo na vstupu procesu. Tento jev je nejčastější a týká se podvrhu s uměle vytvořeným biometrickým vzorem, jako je falešný otisk prstu. V systému se dále může vyskytovat ohrožení v podobě napadení komunikace mezi senzorem a extraktorem markantů (biometrických vzorů), jde o tzv. replikaci dat. S tím souvisí i upravení samotného extraktoru a upravení jeho funkčního principu k vlastním potřebám. Dalšími problémy pak jsou přímé změny uložených dat v databázi, modifikace šablony nebo blokace komunikace mezi databází a rozpoznávacím senzorem. Posledním slabým místem může být výsledek, který je zaslán aplikaci. Ten může být buďto upraven nebo kompletně změněn. [1, 3]

Ve zjednodušené formě se biometrický systém skládá ze dvou částí i když díky realizaci jsou obě části spojené v jeden software s případným hardwarovým zařízením (senzory a snímače). V obou částech systému se nachází biometrický senzor, který nám získává biometrická data od skenovaného objektu a převádí analogové signály (obraz) na digitální (matice bitů). Následuje algoritmus, který má za úkol vyhledat a určit konkrétní biometrické markanty, tedy extrahované biometrické rysy člověka, díky nimž můžeme porovnávat předlohu se snímaných objektem. Tyto jednotlivé vzorky jsou uloženy v databázi ať už přímo do biometrického modulu nebo externě na datové úložiště a při identifikaci jsou porovnávány se zkoumaným objektem. Doposud se jednalo o registrační model biometrického systému. Druhou částí je identifikační a verifikační model. Ten na začátku obsahuje stejné prvky jako model registrační nicméně již neukládá nasnímaná data do databáze, ale naopak načítá data z ní. Následuje to nejdůležitější čímž je porovnávání identifikujícího se objektu s již dříve uloženými vzorky markantů.

Důležitým aspektem jsou biometrické charakteristiky. Typické rozdělení těchto charakteristik je možné zařadit primárně do dvou kategorií. První je anatomicko-fyziologická oblast, ta je využívána pro identifikaci nebo verifikaci osob a je spojena s vědeckými poznatky týkajících se např. oční sítnice, oční duhovky, tváře, otisku prstu, rozmístění žil a tepen ve dlani, geometrii ruky a prstů nebo skladbě DNA. Tyto charakteristiky jsou unikátní, vždy přítomné, člověkem neovlivnitelné a časově velmi stálé, proto také nejčastěji slouží jako primární identifikátor osoby v biometrických systémech. Tato oblast se v odborné literatuře nazývá statická nebo také neměnná. Druhá kategorie je zaměřena na behaviorální charakteristiky s dynamickými vlastnostmi, ty jsou spojeny s pohybem organismu z místa na místo, tzv. lokomoce. Behaviorální identifikace může být reprezentována např. lidským hlasem, mimikami obličeje a rtů, dynamikou psaní souvislých textů, psaní na počítači a v první řadě chůzí. [3, 6]

Spolu s biometrickými charakteristikami a jejich vlastnostmi lze systémy obecně diferencovat na unimodální a multimodální. Unimodální systém je technicky zkonstruován tak, aby využíval pouze jednu zkoumanou biometrickou vlastnost např. otisk prstu. Tyto systémy v komerční oblasti převažují nad multimodálními. Jejich výhodou jsou nižší výrobní náklady, naopak jsou méně spolehlivé. Opakem je systém multimodální, v dnešní době nazývaný také jako dvou faktorové ověřování, ten využívá dvou nebo více snímaných biometrických vlastností. Typická je kombinace rozpoznávání tváře spolu se skenem oční sítnice. Takto spojené rozpoznávací systémy mají zvýšenou spolehlivost, jsou odolnější proti pokusům o útok nebo falšování osobních údajů. [3]

Při samotném průběhu rozpoznávání člověka hrají velkou roli charakteristiky biometrických metod. Ve většině případů patří mezi hlavní ukazatele při rozhodování, který biometrický systém je vhodný pro danou činnost. Mezi důležité ukazatele patří jedinečnost, ta nám říká, s jakou šancí je možné nalézt a následně úspěšně rozpoznat dvě osoby, které mají stejné (případně velmi podobné) biometrické rysy. Čím menší tato šance je, tím je biometrický systém přesnější a méně napadnutelný. Neméně důležitým faktorem je konstantnost, která určuje, zda daná biometrická vlastnost zůstává neměnná v čase. Příkladem jsou oční sítnice a duhovky, ty se začínají vytvářet již ve 22. týdnu vývoje plodu a od narození zůstávají v průběhu života neměnné. Třetí charakteristikou je získatelnost, jakožto důležitý ukazatel v mnoha ohledech. Jednak nám říká, jak náročné je biometrickou vlastnost získat a zároveň jestli je taková vlastnost kvalitativně měřitelná. S tím souvisí i finanční náklady, které jsou úměrné technologii snímání a použitých hardwarových a softwarových komponent. Nejdražšími jsou v dnešní době systémy pro rozpoznávání oční sítnice, duhovky a 3D obrazu tváře. Tyto systémy je možné vidět v soukromých technologických firmách, bankách nebo v letištních halách. Pro uživatele biometrického systému je rovněž důležitá praktičnost. Identifikační metoda musí být co nejvíce praktická ve smyslu nejmenšího možného kontaktu snímané osoby se zařízením, a zároveň by měla trvat co možná nejkratší dobu. Systém by měl vyžadovat pouze minimální množství úkonů a znalostí uživatele. Biometrická technologie musí splňovat jednoduchost ovládání a ukládat pouze hlavní měřené charakteristiky. [1]

Poslední charakteristikou je imunita proti zneužití a falšování, a to ať už z pohledu softwarového oklamání systému nebo vnucení jiné biometrické vlastnosti, např. napodobení hlasu, vytvoření umělého otisku či tváře. Existuje i mnoho dalších aspektů, kterými je důležité se řídit např. dostupnost, velikost nebo spolehlivost. Ta definuje kvalitu systému podle toho, zda je biometrický senzor náchylný na světlo, změnu teploty nebo fyziologické změny vzhledu člověka. Je třeba také zohlednit místo kde bude systém používán, konkrétní skupinu uživatelů či náklady na údržbu. [1, 2]

Tab. 1 Biometrické metody a jejich základní charakteristiky [1,2]

Biometrická Metoda	Jedinečnost	Konstantnost	Získatelnost	Finanční náklady	Odolnost proti falšování	Snímání (Technologie)
Oční sítnice	1:1 000 000	Velmi dobrá	Nízká	Vysoké	Vysoká	Optické-Laser
Oční duhovka	1:6 000 000	Velmi dobrá	Střední	Vysoké	Vysoká	Optické
Tvář	1:5000	Dobrá	Vysoká	Vysoké	Nízká	Optické/Infračervené
Otisk prstu	1:1 000 000	Velmi dobrá	Střední	Nízké	Vysoká	Optické/Kapacitní
Hlas	1:10 000	Proměnlivá	Střední	Nízké	Nízká	Elektroakustické
Geometrie ruky	1:10 000	Dobrá	Vysoká	Střední	Střední	Optické/Infračervené
Žíly na dlani	1:12 500	Dobrá	Střední	Střední	Vysoká	Infračervené

1.2 ZÁKLADNÍ POSTUPY V BIOMETRICKÝCH SYSTÉMECH

Průběh biometrického zpracování dat se skládá z pěti na sobě závislých procesů. Z obecného hlediska mezi ně patří snímání biometrických znaků, přenos dat ze senzoru do řídící jednotky a databáze, převedení analogového obrazového signálu na digitální s následným předzpracováním a segmentací obrazu. Dále následuje proces pro analýzu a extrakci biometrických rysů. Posledním a nejdůležitějším procesem je klasifikace a rozpoznávání biometrických markantů s následným vyhodnocením a uložením dat do databáze. Celý proces začíná prvním krokem tedy získáváním biometrických dat. Je to děj, při kterém se inicializuje měření anatomicko-fyziologických nebo dynamických rysů člověka. Jak již bylo zmíněno, pro budoucí proces identifikace či verifikace hraje důležitou roli jedinečnost biometrických markantů, měřitelnost nebo časová stálost, která zaručuje možnost opakování procesu. Při snímání musí uživatel umožnit ať už vědomě nebo nevědomě zpracovat své biometrické údaje pomocí zvoleného snímače. Tím je většinou CCD snímač s příslušnou optikou pro detailní záběry, mikrofon, kapacitní a optický snímač pro otisk prstu nebo infračervené kamery a senzory. Každý senzor by měl být maximálně vyladěn a zkonstruován s ohledem na konkrétní biometrické měření. Zároveň musí splňovat technické aspekty pro správné snímání, tím je myšleno odpovídající umístění senzoru vůči snímané osobě nebo správné nastavení úhlů mezi plochou senzoru a snímaným člověkem. [2, 6]

Následuje technická část, kde jsou nativní obrazová data odesílána k procesu předzpracování. Ideální prezentací přenosu dat je komunikační systém, ten je složen z pěti částí: informační zdroj (v našem případě senzor), vysílač, přenosové médium, přijímací člen a cílové zařízení (mikrokontrolér, server nebo počítač). Jako zdroj informací je při zpracování obličejové identifikace považován obrazový standard JPEG, u technologií pro otisk prstu je to algoritmus WSQ a pro hlasové audio záznamy systém CELP. V dnešní době se z bezpečnostních důvodů upouští od ukládání zdrojové informace společně s identifikačními údaji osob na jedno společné místo. Tím, že jsou data posílána na vzdálené cílové zařízení (nejčastěji databázový server nebo počítač) jsou data před odesláním zkomprimována, aby nedocházelo ke zpomalování datového přenosu díky objemným souborům. Zdrojová informace je odeslána buďto přímo k předzpracování nebo je vysílačem zpracována na signál vhodný pro vzdušný přenos. Tímto signálem je například satelitní vysílání, rádiové vlny, laserové světlo. Přijímač následně provede opačnou operaci k těm, které prováděl vysílač tedy rekonstruuje zdrojovou informaci pro další zpracování v cílovém zařízení. [6]

Poté co jsou zdrojová data ve formě digitálního signálu doručena do jednotky pro finální úpravu dat, nastupuje fáze extrakce a analýza biometrických příznaků. Při extrakci je důležité získat všechny potřebné biometrické charakteristiky ze zdrojových informací vytvořených na senzorech. Dále je nutné odfiltrovat všechny rušivé složky signálu jako je šum nebo nadbytečné informace v signálu a využít jen

ty, které nesou jednoznačné biometrické markanty. Proces extrakce je v dnešní době automatickou činností softwaru a jeho úkolem je nalezení a určení konkrétních identifikačních rysů. Tento software je neustále zdokonalován matematickými algoritmy, které si firmy důkladně střeží. Výsledným produktem extrakce je tzv. šablona. Je to soubor informací, který jasně identifikuje danou biometrickou vlastnost. V takovéto šabloně se nachází informace zakódovány do bodů v matici, množiny nebo funkční závislosti a slouží jako vizitka osoby. Šablona je ideálním nástrojem při identifikaci osob, jelikož splňuje všechny specifikace pro biometrickou autentizaci a zároveň odráží fyzické podstaty biometrického obrazu. Výhodou těchto šablon je nemožnost zpětné rekonstrukce snímaného obrazu z markantních bodů. Má tak důležitý význam jak z etického, tak právního pohledu. Šablony jsou pouze reprezentativním vzorkem k reálnému obrazu a nejsou tak informačně spojeny s konkrétními identifikačními údaji o osobě, navíc každý autor takovéhoto systému má jiný algoritmus na vytváření šablon, a proto ani není možné přenášet šablony mezi různě navrženými typy senzorů či systémů. Tím je zaručena ochrana osobních údajů, která je dána zákonem č. 101/2000 Sb. [6]

Proces extrakce biometrických markantů pokračuje fází výstupní kontroly vytvořené šablony. Tato kontrola může probíhat již během prvotního snímání a získávání šablon. Funkce kontroly kvality extrahovaného nebo snímaného obrazu je důležitá, jelikož potřebujeme vědět, jestli je snímek použitelný k dalšímu zpracování nebo identifikaci osoby. Pokud nejsou vytvořené charakteristiky v požadované kvalitě (rozostřený obraz, překrývající se biometrické linie aj.) pro zpracování, je po osobě vyžadováno nové snímání. U některých osob se stává, že nemohou nikdy poskytnout kvalitní vzorek biometrických dat pří snímání obrazu, v takovém případě systém hlásí selhání snímání tzv. failure enroll. Biometrické vzorky či šablony vyhodnocené jako dostatečně kvalitní jsou předány k porovnávacímu procesu. Výsledné porovnávání je prováděno s již dříve vytvořenou a uloženou šablonou v databázi, a právě snímanou osobou požadující identifikaci. Účelem porovnání je ztotožnění snímané osoby s jednou nebo i více uloženými šablonami. Tyto šablony představují známé osoby s identitou, která je oprávněna přistupovat do objektu (počítače, budovy, aplikace). U konkrétních osobních údajů jako je např. jméno, příjmení, rodné číslo atp. je ukládání do databáze z bezpečnostních důvodů prováděno odděleně, není tak spojeno s databází referenčních šablon, která je z pravidla uložena v samotném senzoru. [5]

1.3 BIOMETRICKÁ IDENTITA, IDENTIFIKACE A VERIFIKACE

Lidé každý den rozpoznávají u ostatních osob obličej, vzhled postavy, chování, hlasovou intonaci či pohyby těla. V takovém to případě se jedná o automatické identifikování člověka, které se děje v našem mozku a jde výlučně o subjektivní hodnocení. Konkrétně lze definovat jednoznačné charakteristiky člověka jako fyzickou identitu, kterou má každý jinou a nezaměnitelnou s nikým na světě (DNA). Opakem je elektronická identita, ta již jednoznačná není a každý si může vytvořit identit mnoho, jedná se o účty na sociálních sítích, e-mailech apod. Podstatným prvkem pro správné určení identity člověka je spolehlivost systému, díky němuž jsme schopni jednoznačně rozlišit hodnověrnost uživatele. Hodnocení o případné oprávněnosti osoby závisí na překročení pomyslného prahu identifikace, jako jednoduchý příklad může být použití uživatelského jména a hesla při přihlášení do aplikace, kde systém pouze provádí jednoduché porovnání údajů s databází, složitější úlohy rozpoznání identity se nachází v biometrických systémech. V mnoha teoretických i praktických řešeních těchto systémů se můžeme setkat s pojmem autentizace, který je s biometrií velmi úzce spojen. Je však nutné umět rozlišit pojem autentizace a autorizace. Odlišné pojmy podobného názvu je možné nalézt v různých odvětvích. [1, 5]

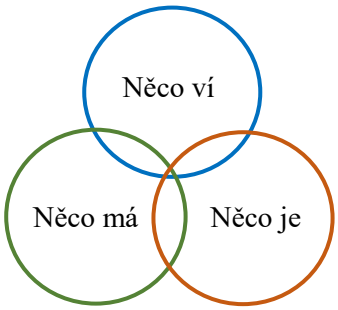
Autentizace (ověření): pojem pocházející z oblasti řízení bezpečnosti, který znamená ověření identity určitého subjektu nejčastěji osoby. Autentizace se řadí mezi bezpečnostní prvky zajišťující ochranu před potencionálním neoprávněným přístupem k osobním údajům. Využívá se všude tam kde je potřeba ověřit identitu člověka (e-mail, datové úložiště, firemní software). V praxi se setkáváme nejčastěji se třemi typy autentizace uživatele a dělíme je podle toho jaké jsou potřeba prostředky pro úspěšné ověření.

1. Autentizace podle toho, *co člověk zná*: tato metoda pracuje s neveřejnou tedy tajnou informací, jejíž majitelem je osoba, která se chce autentizovat. Podstatou tohoto přístupu je dostatečně velká a lehce zapamatovatelná informace. V dnešní době je to nejrozšířenější a nejméně nákladný proces, nicméně se jedná o metodu s nejnižším zajištěním bezpečnosti. Typickými příklady jsou hesla, piny nebo přístupové fráze.

2. Autentizace podle toho, *co člověk má*: také označována jako autentizace uživatelů pomocí předmětu (tzv. tokenu). Ten je vyžadován vždy při ověřování identity. Nejčastěji se využívají platební a identifikační karty, autentizační kalkulačky nebo klíče. Výhodou je obtížná padělatelnost a rychlá identifikace, naopak nevýhodou je možnost odcizení a nutnost nosit token stále u sebe. Bez tokenu není možné uživatele autentizovat.

3. Autentizace podle toho, *čím člověk je*: jedná se o typ autentizace, která využívá jednoznačných biometrických znaků člověka. Jeho hlavní výhodou je skutečnost, že sám člověk je nositel autentizační informace, kterou nemůže zapomenout nebo ztratit. V minulosti byla využívána ve specializovaných aplikacích (kriminalistika), dnes jde o nejefektivnější metodu k identifikaci osob ve veřejném sektoru (informační technologie, bankovnictví).

Každý jednotlivý systém má svá specifická slabá místa. Díky tomu se mimo již zmíněné typy autentizace setkáváme s pojmem vícefaktorová autentizace. Jde o kombinaci dvou nebo i více typů autentizačních metod. Úkolem je eliminovat možnost jednoduchého napadení systému pouze pomocí odcizeného hesla nebo tokenu. Příkladem může být spojení platební karty a pinu nebo mobilního telefonu a autorizační SMS. Čím vyšší je kladen důraz na zabezpečení systému, tím je třeba použít silnější autentizaci a kombinaci hesel. [1, 5]



Obr. 1: Příklad typů autentizace, potřebné k úspěšnému ověření identity. Kombinace všech tří prvků vytváří vícefaktorovou autentizaci.

Autorizace (oprávnění): je proces navazující na autentizaci a znamená schválení k určitému zásahu do systému nebo jeho úpravě, například vytvoření nového informačního záznamu o pacientovi ve zdravotnickém systému. Tato metoda má za úkol ověřit přístupová oprávnění uživatele a zjistit, zda subjekt požadující editaci systému má na něj právo a v jakém rozsahu. K tomuto účelu se stejně jako u

autentizace využívají tokeny a identifikační karty, které mají za úkol ověřit identitu subjektu a jeho pravomoci v přístupu do informačních systémů. [5]

Identifikace (ztotožnění): jde o postup kdy kontrolovaná osoba zadává do identifikačního systému pouze své biometrické vlastnosti a úkolem je zajistit porovnání, rozpoznání a ztotožnění identity subjektu s ostatními biometrickými vzorky uloženými v databázi. Výsledkem celého procesu je buďto nalezená nebo nenalezená identita. Jedná se o časově a výkonnostně velmi náročný postup, zejména díky obsáhlým databázím se stovkami až tisíci registrovanými osobami. V takovém případě jsou databáze rozděleny do menších podskupin, které zajišťují rychlejší zpracování výsledku. Typickým příkladem jsou daktyloskopické systémy AFIS, zde jsou otisky prstů rozděleny podle jejich typů a teprve při jejich určení dochází k identifikaci.

Identifikaci lze rozdělit na dva typy podle toho, zda je ověřovaný subjekt opravdu ten, za kterého se vydává, nebo naopak potvrdit, že neoprávněný subjekt není tím, za kterého se vydává. Tyto typy jsou pojmenovány jako pozitivní a negativní identifikace. Cílem pozitivní identifikace je znemožnění identifikovat se pomocí identity jiné osoby. Pokud tedy v procesu rozpoznávání osoby za pomoci biometrické šablony není nalezena identická šablona v databázi je subjekt odmítnut. Protikladem je nalezení shody šablon, a tedy i kladné přijetí osoby. Příkladem pozitivní identifikace může být kontrola přístupu do počítače s nainstalovaným snímačem otisku prstu, kdy je pouze oprávněné osobě umožněno se přihlásit. Opačným případem je negativní identifikace, zde se jedná o odmítnutí jakéhokoliv přístupu, pokud byla nalezena shoda snímané šablony s šablonou v databázi. Tento typ identifikace se využívá všude tam, kde je nutné hlídat vícenásobné přihlašovaní, neoprávněné použití jiné identity u voleb nebo opakované nárokování sociálních a humanitárních služeb. [5]

Verifikace (porovnání): je proces při kterém dochází ke kontrole snímané osoby vůči její vlastní elektronické předloze identity. Na začátku je osoba vyzvána k předložení identifikačních údajů (PIN, ID Karta), které jsou následně vyhledány a porovnány s daty v databázi. Pokud již při této operaci není nalezena shoda je okamžitě osoba zamítnuta. Pokud jsou však obě identity nalezeny může dojít k samotnému porovnání biometrických šablon uložených v databázi, tedy dat od snímané osoby a dat spojených s elektronickou identitou. Verifikace je mnohem rychlejší a méně náročná na výkonnostní a časové zpracování nežli identifikace. Oproti identifikaci, jinak označované jako porovnání 1: N, kde N představují všechny uložené šablony v databázi, se verifikaci říká porovnání 1:1. [1]

1.4 HODNOCENÍ PŘESNOSTI BIOMETRICKÝCH SYSTÉMŮ

Při vytváření finální verze technického zařízení je třeba si položit několik otázek týkajících se kvality, výkonu, přesnosti, bezpečnosti a spolehlivosti metody, která zaručuje úspěšné provozování takového to zařízení. V případě systémů pracujících na biometrických metodách je důležité vnímat aspekty, které ovlivňují budoucí výběr a zavedení systému do praxe. Příkladem pro jednoznačné a bezchybné určení identity člověka jsou systémy, které splňují klasifikační charakteristiky. Těmto charakteristikám se říká míry chybného přijetí, odmítnutí, shody, neshody a další. Všechny tyto aspekty vycházejí z předpokladu určení prahové hodnoty, která definuje kdy je prokázaní identity člověka úspěšné a kdy naopak není. Celý proces získání identity však začíná již při extrakci biometrických rysů. Extrahované rysy vytvoří obrazovou šablonu, která je pak v budoucnu využita k porovnání se snímaným subjektem. Výsledkem porovnání je skóre definující shodu obou šablon. Hodnota skoré je číslo ležící

v intervalu od <0,1> nebo <0 %, 100 %>. Pokud tedy skóre leží za již zmíněnou prahovou hodnotou je systém povinen přijmout tvrzení o identitě, jestliže není výsledek je opačný. Z výsledku se následně určuje závěr rozhodnutí. To může nabývat dvou hodnot, buďto správné nebo chybné rozhodnutí. Příklad výsledného rozhodnutí (identifikace/verifikace) biometrického systému: [1]

- Petr je identifikován jako Petr → Oprávněné přijetí (Správné přijetí)
- Petr je zamítnut jako Jiří → Oprávněné odmítnutí (Správné odmítnutí)
- Petr je identifikován jako Jiří → Neoprávněné přijetí (Chybné přijetí)
- Petr je zamítnut jako Petr → Neoprávněné odmítnutí (Chybné odmítnutí)

Míra chybného odmítnutí (FRR – False Rejection Rate): v různých publikacích označována jako chyba prvního typu (Type I Error Rate), je pravděpodobnost určující chybné odmítnutí oprávněné osoby. V praxi se jedná o chybné vyhodnocení rozhodnutí o oprávněnosti subjektu, který však je v systému zaregistrován s příslušnou šablonou biometrických rysů. FRR lze vypočítat z poměru celkového počtu chybných odmítnutí a počtu pokusů oprávněných osob o identifikaci či verifikaci. Z bezpečnostního hlediska se nejedná o příliš nežádoucí jev, nicméně v komerčních aplikacích chybné odmítnutí způsobuje problémy při praktickém využívání systému a snižuje spolehlivost a kvalitu. [1, 3]

$$FRR = \frac{Celkový\ počet\ chybných\ odmítnutí}{Počet\ pokusů\ orávněných\ osob}\ [\%]$$

Míra chybného přijetí (FAR – False Accept Rate): taktéž nazývána jako chyba druhého typu (Type II Error Rate), je pravděpodobnost určující chybné přijetí neoprávněné osoby biometrickým systémem. Ten nesprávně ztotožní dvě odlišné šablony rysů a tím umožní potenciálnímu útočníkovi narušení objektu, odcizení identity či nežádoucí činnost. Jedná se o významnou bezpečnostní chybu, kterou je třeba omezit na minimum. FAR se vypočítá z podílu celkového počtu chybného přijetí a počtu neoprávněných osob pokoušejících se o identifikaci. [1]

$$FAR = \frac{Celkový\ počet\ chybných\ přijetí}{Počet\ pokusů\ neoprávněných\ osob}\ [\%]$$

Míra chybné shody (FMR – False Match Rate): je indikátor určující pravděpodobnost, že bude přijata neoprávněná osoba. Jedná se o relativní množství chybných pozitivních identifikací. V dnešní době je FMR spíše marketingová než technicky objektivní informace. Míra chybné shody je definována jako integrál od 1 do T, kde T je práh rozhodnutí o přijetí, P určuje hustotu pravděpodobnosti výroku umístěného v závorce, S je skóre na porovnávacím intervalu a H_1 je tvrzení o odlišnosti původu šablony a vzoru. FMR se podobá FAR nicméně se liší tím, že do výpočtu nezahrnuje neúspěšné pokusy, které byly prováděny před snímáním. [1,3]

$$FMR\ (T) = \int_T^1 P(S|H_1)ds$$

Míra chybné neshody (FNMR – False Non-Match Rate): určuje hlavní podíl všech vzorů od oprávněných osoby, kterým bylo chybně deklarováno že jejich vzor není totožný se šablonou od stejné osoby předkládající biometrický vzorek. Konkrétně se tedy jedná o podíl osob s chybně nepřijatou identitou. Výpočet je podobný FMR nicméně navazuje na FRR. Míra chybné neshody se vypočítá jako integrál od 0 do T, kde T je rozhodovací úroveň, P určuje hustotu pravděpodobnosti výroku umístěného v závorce, S je skóre na porovnávacím intervalu a H_0 je tvrzení o shodě původu šablony a vzoru. [1,3]

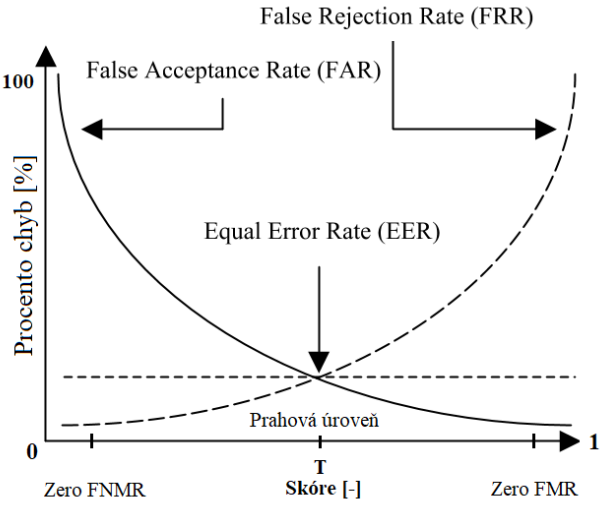
$$FNMR\ (T) = \int_0^T P(S|H_0)ds$$

Míra vyrovnaných chyb (EER – Equal Error Rate): jedná se o index definující vyrovnanost míry chybné shody a neshody kde platí, že FMR(T) = FNMR(T). Pomocí tohoto indexu je možné stanovit rozhodovací práh na takovou úroveň, kde bude současně chybně přijat i odmítnut stejný počet lidí. V praxi se tento index využívá k přesnému nastavení prahové úrovně dle požadavků budoucího systému. K indexu EER také patří neméně důležité pojmy jako ZFMR (Zero FMR) určující dolní mezní hranici FNMR, kdy FMR je nulové a ZFNMR (Zero FNRM) určující dolní mezní hranici FMR, kdy naopak FNMR je nulové. [1]

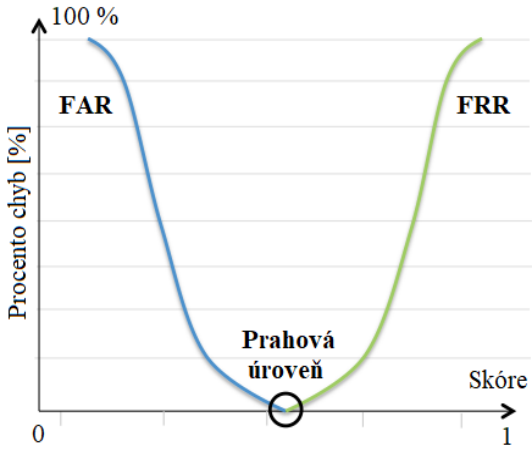
Míra neschopnosti snímat (FTA – Failure To Acquire): je velmi důležitý ukazatel týkající se schopnosti kvalitního zpracování a zaznamenání obrazové informace daným biometrickým snímačem. Fakticky se jedná o podíl počtu identifikačních pokusů, u nichž systém selže při snímání biometrické informace k celkovému počtu pokusů o identifikaci. Výsledkem této chyby je odmítnutí snímané osoby, přičemž sama osoba je schopna předložit biometrickou informaci. Pokud je míra neschopnosti snímat vysoká, není vhodné senzor dále využívat. Ukázka: při zápisu uživatelů do systému pomocí otisku prstu bylo z celkového počtu 100 pokusů 5 osob odmítnuto a biometrické informace se nepodařila uložit. FTA je pak rovna (5/100) *100 = 5 %. [1]

Míra neschopnost zaregistrovat (FTE – Failure To Enroll): tento ukazatel se týká posledního kroku v procesu ukládání nasnímané biometrické informace. FTE určuje procentuální podíl osob, které se systém není schopen naučit při dokončování registračního procesu. Chybné míry FTE se vyskytují u systémů, kde je instalována kontrola kvality nasnímaných biometrických charakteristik.

Na základě všech těchto chybových mír jsme schopni určit spolehlivost, kvalitu a přesnost systému. Pokud je hodnota FRR vetší než FAR, pak se takovéto systémy využívají k zjištění identity pomocí verifikace 1:1, je-li tomu naopak pak se tyto systémy používají k identifikaci osob 1: N. Určit bezpečnostní měřítko biometrického systému lze z míry FAR, dle platné normy ISO/IEC 15480, která definuje základní bezpečnostní stupeň s hodnotou FAR $<10^{-2}$, střední stupeň pro FAR $<10^{-4}$ a vysoký stupeň, kde je hodnota FAR menší než 10^{-6}. [2]



Obr. 2:Příklad reálného biometrického systému



Obr. 3: Příklad ideálního biometrického systému

2 ANATOMICKÁ A FIZIOLOGICKÁ STRUKTURA PRSTU

Kůže (lat. Integumentum commune nebo také cutis) je z hlediska velikosti a plochy jedním z největších orgánů lidského těla, je skladebně velmi členitá a vývojově složitá. Jakožto orgán nacházející se na hranici mezi vnitřním a vnějším prostředím vykonává nespočet funkcí. Hmotnost kůže průměrně dosahuje hodnot přibližně 5 až 9 % z celkové hmotnosti těla a plocha se pohybuje v rozmezí od 1,5 do 2,0 m^2 v závislosti na výšce a váze člověka, z čehož na hlavu a krk připadá 11 %, na trup 30 %, na horní končetiny 23 % a na dolní končetiny 36 % z celkové plochy kůže. Kůže má proměnlivou tloušťku, která závisí na několika faktorech. Jedním z nich je anatomické umístění na těle, jiná tloušťka kůže bude na dlani a jiná na břišní stěně. Průměrně však tato tloušťka činí od 0,5 mm (oblast očních víček) do 4 mm (záda). Další roli hraje kondice a věk jedince spolu s výživou a hydratací. Jedním ze znaků je barva, ta je výsledkem působení mnoha vnějších i vnitřních činitelů. Barvu tak ovlivňuje množství melaninu, prokrvení kůže, hydratace, velikost rohové vrstvy nebo obsah betakarotenu.

Kůže má členitý nikoliv hladký povrch, na kterém se nachází brázdy, záhyby a rýhy vytvářející celkový reliéf kůže, který je segmentován na menší polygonální útvary. Příkladem detailního kožního reliéfu je systém papilárních linií nacházejících se na bříškách prstů horní a dolní končetiny. Tomuto reliéfu se odborně říká Purkyňovy kresby neboli dermatoglyfy. Jejich přesné rozložení a zahnutí je dané díky uspořádání papil koria, kolagenních a elastických vláken dermis. Výsledkem jsou dermatoglyfické obrazce s hlavními vzory typu smyčka, oblouk a závit. Uspořádání, velikost a kombinace těchto vzorů je jedinečná u každého člověka již od narození a neexistuje totožná kombinace u jiné osoby. Této přednosti se hojně využívá v biometrii, forenzní antropologii či kriminalistice. Kůže je složena ze tří na sebe navazujících vrstev: epidermis (pokožka), dermis (škára), tela subcutanea (podkoží). [2, 8]

2.1 ANATOMICKÁ STAVBA KŮŽE

Epidermis (pokožka): je svrchní vrstvou kůže s nejmenší tloušťkou, která neobsahuje cévy ani kapiláry. Představuje zevní ochranou vrstvu kůže, kterou tvoří vrstvený rohovějící epitel dlaždicového tvaru a tenký emulzní film ektodermového původu. Tloušťka se odvíjí od místa umístění, nicméně se pohybuje v rozmezí od 0,2 do 1,5 mm. Nejtenčí je na očních víčkách, kde epidermis dosahuje tloušťky pouhých 0,1 mm, naopak nejsilnější je na chodidlech a zádech. Buňky dlaždicového epitelu se neustále mitotický dělí a vytváří tak stále novou kožní vrstvu. Tato vrstva se periodicky posouvá směrem k povrchu kůže a zároveň se zplošťuje až nakonec odpadne v podobě odumřelých buněk. Tento proces trvá 28 dní a začíná v bazální vrstvě, kde se keratinocyty mění v tzv. korneocyty. [2, 12]

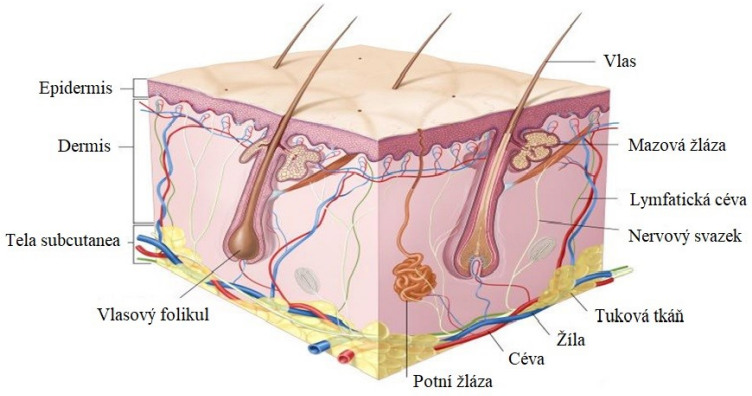
Samotný epidermis se skládá z pěti vrstev. První vrstvou je Stratum bazale. Jde o zárodečnou a nejhlouběji se nacházející vrstvu v epidermis. Tvoří ji několik palisádově uspořádaných keratinocytů cylindrického tvaru, zrnka melaninového pigmentu a malé množství bazofilní cytoplazmy. Keratinocyty jsou navzájem spojené pomocí výběžků tzv. desmozomů, které navíc také spojují keratinocyty s bazální membránou, která představuje hranici mezi škárou a pokožkou. Druhou a zároveň nejtlustší vrstvou je Stratum spinosum, která navazuje na bazální vrstvu a je složena z mnoha polygonálních oplošťujících se keratinocytů. Ty jsou navzájem opět spojeny desmozomy a extracelulární prostor vyplňuje tkáňový mok sloužící k dopravě živin do buněk. Třetí je vrstva Stratum granulosum, která je tvořena 1 až 3 řady zploštělých buněk s tmavě zbarvenými zrny keratohyalinu obsahující protein profilagrin. Ten se postupem času mění na filagrin a zajišťuje spojení vláken keratinu. V této části kožní vrstvy se již buňky

mitoticky dále nedělí. Následuje velmi tenká a světlá eosinofilní přechodová vrstva Stratum lucidum, která je dobře viditelná v tlustších částech kůže. Tvoří ji tzv. tranzitní keratinocyty ztrácející své jádro a organely. Poslední a zároveň zevní vrstvou kožní bariéry je Stratum corneum. Tuto zrohovatělou vrstvu tvoří 1,6 x 10^6 korneocytů/cm^2 a každý den se z povrchu kůže odloučí 6 až 14 g těchto buněk. [2]

Dermis (škára): je střední vrstva kůže mezenchymálního původu nacházející se mezi epidermis, kde je spojena pomocí bazální membrány a podkožního vaziva. Je složena z pojivové tkáně obsahující zvlněné elastické kolagenní vlákna, která jsou propletena v plsťovité snopce. Její tloušťka se mění v závislosti na lokalitě a dosahuje hodnot od 0,6 do 3 mm a tvoří tak 70 až 95 % z celkové tloušťky kůže. Škára se dělí na dvě podvrstvy. První je jasně zbarvená povrchová vrstva je tzv. Stratum papillare obsahující velké množství vazivových buněk, ve kterých jsou rozmístěny nervové zakončení, buněčné elementy, termoreceptory, hmatová tělíska a bohaté sítě krevního řečiště. Druhou podvrstvou je Stratum reticulare. Jde o silnější a hlubší část škáry obsahující menší množství buněk a elastických fibril. Naopak se zde ve velkém množství nachází hlavní složky škáry jako je elastin a kolagen. Tyto vlákna jsou uspořádány do větších snopců, které se navzájem proplétají a dále kříží ve směru mechanického zatížení v kožní krajině, zároveň jsou zodpovědné za pružnost a sílu kůže. Důležitou součástí škáry jsou lineární výběžky, které prostupují do svrchních pater pokožky a vytváří tak jedinečné kličky tzv. papilární linie, díky nimž jsme schopni identifikovat osoby.

Ve škáře se nachází několik druhů přídatných kožních útvarů. Jedním z nich jsou mazové žlázy. Ty jsou uloženy v horní části škáry a nachází se na většině povrchu těla s výjimkou dlaní a chodidel. Celkový počet mazových žláz se pohybuje okolo 300 tisíc. Velké množství těchto žláz je umístěno v oblasti obličeje a zad. Mazové žlázy ústí do vlasových kanálků neboli folikulů, ze kterých vyrůstají k povrchu pokožky vlasy. Za den se tak ve škáře vytvoří asi 2 gramy mazu, který se následně rozprostře na povrchu epidermis a vytvoří tzv. mazový film sloužící k první ochraně pokožky. Druhým útvarem jsou potní žlázy. Ty dělíme na velké a malé. Malé neboli apokrinní žlázy, jsou uloženy hlouběji než mazové žlázy a jejich úlohou je vyrovnávání teploty mezi vnitřním organismem a vnějším prostředím. Denně se z potních žláz vyloučí 500 až 1000 ml potu. Velké potní žlázy (aromatické) jsou umístěny v podpaží a okolo prsních bradavek. Nachází se hluboko ve škáře a mají samostatný vývod do vlasového folikulu. Ve škáře jsou rozprostřena i další adnexa jako jsou kořeny vlasů a nehtů či nervová vlákna. [8]

Tela subcutanea (podkožní vazivo): je nejhlouběji uložená část kůže, která spojuje dermis s povrchovou fascií či periostem. Pochází z období mezodermu a skládá se ze sítí lamelárně uskupených elastických a kolagenních vláken, mezi nimiž jsou rozesety vazivové buňky. Z velké části se zde nachází podkožní tuk obsahující tukové buňky neboli adipocyty. Podkožní vazivo je z velké části prorostlé lalůčky tuku, ze kterých vzniká tukový polštář (panniculus adiposus). Jeho velikost je závislá na výživě, hormonálních vlivech a somatickém typu člověka. Tukové vazivo je důležité pro ukládání zásobní energie. Má také ochrannou a termoregulační funkci. Největší část tukového vaziva je umístěna na břiše, stehnech a hýždích kde dosahuje šířky od 8 do 25 mm. U žen je tato šířka dvakrát větší než u mužů a nejčastěji se nachází v oblasti prsou, ledvin a boků. V místech, kde je kůže vystavena mechanickému namáhání, vznikají v části podkožního vaziva tzv. tíhové váčky, které toto namáhání tlumí. Váčky jsou svou strukturou podobné synoviální tekutině. Podkožní vazivo je bohatě vázané na krevní řečiště a díky tomu je také prvním místem, kde se ukládá přebytečná energie a vitamíny A, D, E a K. Na druhou stranu je rovněž jako první využita při absenci výživových látek v krvi. Nachází se zde také jeden z důležitých mechanoreceptorů tzv. Vater-Paciniho tělísko, potřebné k vnímání dotyku a tlaku na kůži. [7, 8]



Obr. 4: Histologický řez stavby kůže

2.2 FYZIOLOGICKÉ FUNKCE KŮŽE

Jakožto největší aktivní orgán, zastává kůže mnoho nepostradatelných metabolických procesů potřebných k životu. Tyto fyziologické funkce přímo souvisí s anatomickým složením konkrétních receptorů a jejich umístěním na povrchu těla. V naprosté většině jsou funkční procesy kůže regulovány nervovým systémem a nezáleží na tom, zda jsou projevy na kůži fyziologického nebo patologického původu. Veškeré funkce umožňující spojení se zevním prostředím jsou řízeny z mozkové kůry a nervového autonomního systému. Jednotlivé funkce kůže lze rozdělit do několika skupin. [7]

Obraná funkce je prvním a hlavním faktorem rozlišujícím, které biologické složky budou propuštěny do organismu a které se naopak zadrží nebo zničí. V obrané funkci lze definovat několik bariér bránících vstupu nežádoucích vlivů. První je bariéra fyzikální, ta je zodpovědná za mechanickou ochranu ve smyslu udržení pevnosti a pružnosti kožního krytu. Této ochraně významným způsobem přispívá proces keratinizace, hydratace pokožky či podíl podkožního tuku a vaziva. S fyzikální bariérou přímo souvisí schopnost regenerace pokožky trvající přibližně 28 dní. Díky neustálému obměňování těchto buněk je rohová vrstva schopna ochránit kůži před ultrafialovým zářením ze slunce. Úkolem fotoprotektivních mechanismů je zajistit odraz světla od pokožky, rozptyl dopadajícího světla nebo absorpce světelné energie proteiny. Poslední obrané funkce představují chemické a biologické bariéry. Obě spolupracují na acidorezistenci keratinu, autodezinfekci a detoxikaci kůže. Biologická bariéra je navíc díky aminokyselinám, potu a kyselině mléčné schopna chránit kůži před kyselým a zásaditým prostředím či mikroorganismy.

Metabolická funkce je druhou skupinou ve fyziologických dějích kůže. Výhodou této funkce je uskutečnění metabolismu cukrů jako je glukóza, glykogen nebo kyselina hyaluronová. Dále pak je to vstřebávání aminokyselin (cystin, tyrozin, histidin), cholesterolu a volných mastných kyselin. Metabolismus má mimo jiné velký vliv na výrobě vitamínu D a s tím spojeným biologickým účinkem. Vitamín D vzniká v bazálních keratinocytech přeměnou 7–dehydrocholesterolu a ultrafialového záření na previtamin D_3, ten se během osmi hodin přemění na cholekalciferol tedy vitamín D.

Regulační funkce má na starost řízení tělesné teploty, která je výsledkem svalové činnosti, metabolickými a endokrinními procesy. Jelikož je člověk homoiotermním organismem, je teplota regulována z centrálního místa, v tomto případě z hypotalamu. Díky němu je celková teplota těla udržována na hladině 37 °C a můžou probíhat biochemické reakce. Kůže má nicméně také vliv na regulování teploty, a to pomocí dvou mechanismů. Prvním je odpařování vody z povrchu kůže a potních

žláz. Druhým je vazodilatace, vazokonstrikce a zásobení škáry cévami. V poslední řadě se na regulaci tepla podílejí Ruffiniho tělíska zodpovědné za detekci tepla a Krauseho tělíska detekující chlad. Oba tyto typy receptorů vysílají signály do hypotalamu k dalšímu vyhodnocení.

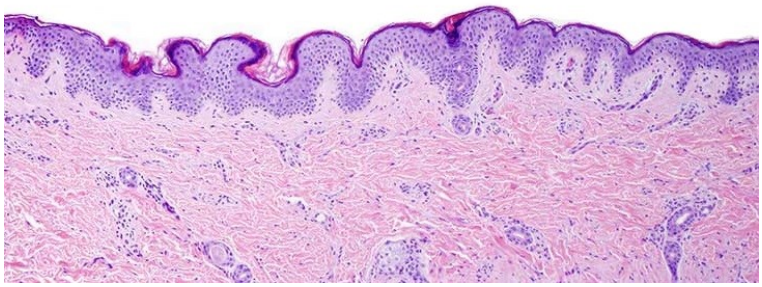
Sekreční funkce kůže, jakožto holokrinní žláza, vykonává vylučování důležitých hormonů a látek potřebných k fungování kožního povrchu. Jedním z nich je keratin, který je hlavním prvkem při růstu vlasů a nehtů. Dalším je pigment melanin, jedná se o polymer metabolitů dopaminu a tyrosinu. Je zbarven žlutohnědě a tvoří se v intracelulární tekutině v melanosomech. Melanin je jedním z prvků důležitých při fotoprotekci a optické filtraci světelných kvant a fotonů. Kůže hraje také velkou roli při vylučování potu, mazu a katabolitů.

Senzorická funkce vytváří z kůže smyslový orgán, který prostřednictvím receptorů umístěných v podkoží informuje mozek o vnitřním a vnějším prostředí. Přenos těchto informací zajišťuje vegetativní nervový systém spolu s cerebrospinálním nervstvem ve škáře. Člověk je díky těmto receptorů schopen vnímat teplo, chlad, bolest, dotyk, brnění a svědění. Nejcitlivější je kůže na povrchu čela, tváře a nosu. Za hlavní receptory se považují tyto: Vater-Paciniho tělíska zprostředkující tlak na posledních konečcích prstů, Meissnerova tělíska pro dotyk a Golgiho tělíska pro detekci tlaku na dlani a uprostřed prstů.

Imunologická a depotní funkce uzavírá seznam všech nejpodstatnějších fyziologických aktivit kůže. Imunologická ochrana kůže začíná při procesu pronikání antigenů do epidermální vrstvy, kde jsou vychytávány pomocí Langerhansových buněk. Následně tyto buňky dozrávají, eliminují antigeny a migrují do spádové regionální uzliny. Do imunitní reakce se také zapojují makrofágy, fibroblasty, T a B lymfocyty. Poslední vlastností kůže je ukládání důležitých výživových látek jako je glukóza, lipidy, voda, krev či NaCl do podkoží. Kombinace těchto živin je potřebná k tkáňovému dýchání, vylučování odpadních látek pomocí potu nebo správné buněčné aktivitě. [7, 8]

2.3 PAPILÁRNÍ LINIE PRSTŮ RUKY

Otisk prstu je jedinečnou a neměnnou dvourozměrnou kresbou vyjadřující strukturu pokožky na každém zakončení prstu. Výška těchto útvarů dosahuje hodnot od 0,1 do 0,4 mm a průměrná šířka je 0,3 mm. Konkrétní velikost a tvar určuje tzv. zárodečná vrstva uložena v nejhlubší části epidermis. Díky této vrstvě je informace o papilárních strukturách velmi obtížné dlouhodobě odstranit. Papilární linie jsou tak odolné proti mechanickému, tepelnému či chemickému poškození. Pokud je však kožní vrstva narušena je jen otázkou regeneračního období, kdy zárodečná vrstva zahájí tvorbu nové papilární linie. Z anatomického hlediska jsou tyto útvary tvořeny hřebenovitými výběžky (papilae) vznikajícími mezi epidermis a stratum papilae. Opačným směrem se nacházejí brázdy (údolí), ve kterých jsou založené epiteliální lišty společně s čepy pokožky. Na otisku prstu jsou hřebeny vyznačeny černou a brázdy bílou barvou. [7, 10]



Obr. 5: Příčný řez strukturou kůže se znázorněním papilárních linií

Velikost a směr vláken podkožního vaziva určující tvar papilárních linií je závislá od toho jakým způsobem je v daném místě namáhána kůže, např. v oblasti kde je potřeba větší a jemnější pohyblivost konečků prstů jsou struktury linií větší. Vznik kožních papil probíhá již ve čtvrtém měsíci embryonálního života. V tomto období se odehrává tvorba základních tvarů papilárních linií, které zůstávají po celý zbytek života neměnné. Individuálně se během života v závislosti na růst člověka mění pouze tloušťka a velikost výběžků společně s prohloubením brázd. Výjimkou je období stáří, kdy jsou struktury papil narušeny vráskami a rohovatěním kůže. Během života se neustále od pokožky odlučují zrohovatělé buňky a ty jsou nahrazovány novými, které vytvoří totožnou strukturu papilárních linií jako ty předešlé. Za dobu 75 let života se od pokožky odloučí přibližně 20 kg těchto buněk.

Existuje několik zákonitostí týkajících se využití papilárních linií a jejich obrazců v biometrii. První se týká jedinečnosti otisku prstu a říká, že díky velkému počtu charakteristických znaků linií a jejich vzájemných kombinací (64 miliard) na světě neexistuje otisk se zcela shodným obrazcem u odlišných osob. Druhé pravidlo říká, že obrazce z papilárních linií zůstávají během života stejné či výrazně podobné. V rámci několikaletých studií byly pravidelně porovnávány otisky prstů u téže osoby s výsledkem neměnných základních biometrických prvků potřebných k identifikaci. Poslední zákonitost popisuje papilární linie jako velice odolnou biometrickou složku, kterou nelze odstranit například spálením, pořezáním nebo odřením. Úplné zničení by bylo možné, pokud by se porušila také zárodečná vrstva. Příklady těchto tvrzení potvrdili na konci 19. století francouzští profesoři Locard a Witkovski, kteří pozorovali na dělnících pracujících s acetonem v továrně na celuloid, že jejich zničené konečky prstů se vždy zahojily a obnovili se také obrazce papilárních linií.

Z celkového pohledu se otisk prstu skládá ze tří základních tříd, tzv. Henryho klasifikací (Edward Henry), někdy označovaných jako singularity. Seskupení papilárních linií tak vytváří obrazce typu oblouk, vír nebo smyčka. Ty se dále dělí na menší kategorie např. klenutý oblouk, spirála, závit, levá a pravá smyčka. V těchto obrazcích se nachází několik klasifikačních bodů a útvarů jako je jádro, delta, typová linie nebo počet papilárních linií. Ve třídách vír a smyčka jsou umístěny body typu jádro a delta. Bod jádro je označení pro střed otisku prstu ležící na vrcholu posledního vnitřního zakřivení hřebenu. Nejedná se však o střed vytvořeného obrazu. Bod delta označuje místo v otisku, kde se rozbíhají nebo setkávají papilární linie ze (do) tří směrů a vytvářejí tak pomyslný obrazec trojúhelníku. Tento typ je nejčastěji umístěn v dolní části otisku a po stranách. Na rozdíl od jádra může být bod delta umístěn na více místech najednou. Dalšími metrikami pro klasifikování otisků je počet papilárních linií mezi dvěma singulárními body a tzv. typové linie definující vzdálenost mezi papilární linií umístěnou ve středu otisku a nejníže umístěné deltě. Obrazec typu oblouk nemá ani jednu deltu a jádro. Naopak klenutý oblouk již má jádro a jednu deltu umístěnou ve vertikální poleze pod jádrem. Závit nebo vír obsahuje dvě delty a jedno jádro. Detailnější popis struktury a klasifikace otisku je popsána v dalších kapitolách. [8, 10]

Obr. 6: Zobrazení tří základních tříd otisků prstu (smyčka, vír, oblouk) a jejich rysů

3 VYUŽITÍ OTISKU PRSTU V PRAXI

Identifikace člověka pomocí otisku prstu je v dnešní době nejčastěji používanou bezpečnostní metodou biometrického inženýrství aplikovanou na desítkách až stovkách typů systémů všude tam, kde je potřeba moderního a efektivního rozpoznáni osob. Příkladem mohou být přístupové systémy jako je kontrola oprávněnosti vstupu osob do budov, skladů, datových center, letištních terminálů nebo trezorů. Rozšířenější jsou však systémy pro kontrolu identity člověka, s tímto příkladem se můžeme setkat na úřadech při vyřizování osobních průkazů, při letištní pasové kontrole ve spojených státech nebo jako nástroj pro náhradu fyzických či elektronických podpisů. V posledních několika letech je tento způsob identifikace přesunut také do sféry informačních technologií. Své využití tak uplatní při kontrole přístupu do mobilních telefonů, notebooků, serverů nebo jako chytrý způsob autentizace při platebních transakcích (TouchID – Apple Pay). Důležitou oblastí je daktyloskopie a obor policejně-soudního vyšetřování, ve kterém otisk prstu slouží jako jeden z hlavních identifikátorů potencionálního pachatele.

3.1 HISTORIE POUŽÍVÁNÍ OTISKU PRSTU

Období od prvních historicky doložených existencí a znalostí využívání otisku prstu u člověka až po současné komplexní biometrické systémy je velice dlouhé. První nalezené zmínky pocházejí z doby indiánských kmenů sídlících v oblasti dnešního státu Indiana v USA. Na počátku 20 století zde byli nalezeny kamenné rytiny tzv. petroglyfy zobrazující lidskou dlaň s papilárními liniemi. Podstatné historické nálezy pocházejí z období Babylonské říše a starověké Číny, přibližně 6 až 7 tisíc let př.n.l. V Babylonské říši za vlády královny Hanimurabi (18 století př.n.l.) se otisky prstů používaly jako identifikační značky. Jedním z prvních spisů dokumentující otisk prstu jako nástroj pro správu veřejného i soukromého charakteru je dílo čínského historika Kio Kung-yen definující novou metodu stvrzující obchodní a manželské smlouvy. Tyto dokumenty byly většinou opatřeny pečetí obsahující autorův otisk prstu. Další historické využití otisku papilárních linií bylo uplatněno ve spisu kriminalistických důkazů při vloupání do domu z období dynastie Sung (11.století n.l.). [9]

V Evropě se za první zmínky o otiscích prsů považují vědecké poznatky z roku 1686. Italský profesor anatomie Marcello Malpighi se v této době věnuje na univerzitě v Boloni detailnímu zkoumání jednotlivých znaků papilárních linií jako jsou smyčky, oblouky nebo třeba velikost hřebenů a údolí. Později po něm byla pojmenována jedna ze základních anatomických struktur kůže tzv. Malpighiho vrstva. Nesporný přínos k rozvoji první daktyloskopie měl český profesor patologie a fyziologie Jan Evangelista Purkyně. Ten ve své habilitační práci „Commentatio de examine physiologico organi, visus et systematis cutanei“ v roce 1823 jako první detailně popsal a rozlišil otisky prstů na devět základních a dodnes používaných vzorů. Definoval je jako nejčastěji se vyskytující obrazce papilárních linií: elipsy, spirály, kruhy, zdvojené vrcholky, mandle, šikmé zálivy a pruhy, podélné pruhy a příčné záhyby. Purkyněho práce však nebyla vnímána jako podklad pro kriminalistickou analýzu, ale zejména jako pohled na teoretickou analýzu anatomických a fyziologických zákonitostí daktyloskopie.

William James Herschel je další významnou osobností v oblasti teoretické daktyloskopie. Tento anglický úředník sloužil od roku 1853 v Indii jako plátce penze indickým vojákům a již při této práci si zakládal seznamy vojáků společně s jejich otisky prstů, aby poznal, kdo již penzi dostal a zabránil tak podvodům při vyplácení důchodů. Během prvních pěti let zkoumání otisků došel k podstatným závěrům, že žádné dva otisky nejsou stoprocentně totožné a navíc, že jsou během života člověka neměnné.

Herschel se teoretické daktyloskopii věnoval přes dvacet let a opakovaně docházel ke stejným závěrům týkajících se jednoznačnosti a neměnnosti otisku. Své znalosti nakonec uplatnil ve věznici, kde využil svou metodu otisků prstů k identifikaci a rozlišení těžkých a lehkých zločinců. Jeho snahou bylo zařadit principy teoretické daktyloskopie do praxe a přivézt tento objev také do Anglie, nicméně se mu nepodařilo dosáhnout výsledku širšího uplatnění. Na jeho znalosti postupem času navazuje H. Faulds a především F. Galton. Henry Faulds byl významný skotský lékař a vědec, který nezávisle na Herchelovi objevil v Japonsku roku 1879 otisky prstů na hliněných prehistorických nádobách. Ve svém bádání se zaměřil především na otisky prstů primátů a osob různých národností. Hlavní objevy přišli v roce 1880, kdy představil možnost spojení otisků prstů a trestních činů. Ve svých poznámkách uvádí návod ke zkvalitnění kriminalistických procesů za pomoci předem odebraných otisků od již trestaných osob a uložit je do sbírky otisků. Ty by mohly v budoucnu zjistit pravou identitu osoby a rychleji objasnit trestné činy. Další využití našel ve spojení s registrací migrantů, identifikaci mrtvol nebo podepisování finančních smluv. Na rozdíl od Herschela, který snímal pouze dva otisky Faulds zavádí snímání otisků ze všech deseti prstů na strukturovaný formulář pomocí inkoustu. [10]

Angličan Francis Galton je označován jako jeden ze zakladatelů praktické daktyloskopie. Ačkoliv byl vystudovaný lékař, medicíně se nevěnoval a své zkoumání přenesl do oblasti identifikačních metod, konkrétně tehdy moderní antropometrické bertillonáži. Výzkum započal roku 1884 a to v rámci konání mezinárodní výstavy o zdraví v Londýně, kde sbíral tělesné a duševní informace pro své budoucí podklady. V roce 1888 byl požádán Královským ústavem, aby přednesl nové techniky Bertillonova antropometrického měření, kterým se věnoval při návštěvě Paříže. Nebylo to však jediné téma, které přednášel, ale pozastavil se i nad tehdy novými metodami identifikace, právě například otisky prstů. Výsledky svého zkoumání vložil do práce „Fingerpints“ (1892), v níž stanovuje nový jednoznačný identifikátor zvaný delta, který vzniká spojením několika linií ve trojúhelníkovou oblast. V návaznosti na tento bod definoval čtyři základní typy otisků: otisk bez delta bodu, otisk s delta bodem doleva a doprava a otisk se dvěma a více deltami. Díky tomuto zařazení bylo možné v roce 1894 zavézt daktyloskopickou metodu identifikace společně s metodou antropometrie do praxe. O rok později Galton ještě zdokonalil klasifikační typy otisků a v práci „Fingerpints Directory“ stanovil nové vzory papilárních linií používané do dnes: oblouk, pravá smyčka, levá smyčka a spirála. [9]

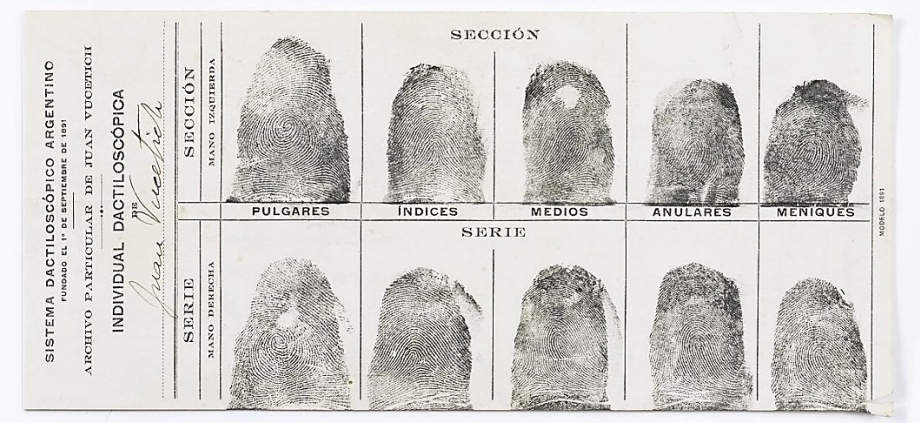
V roce 1895 navštívil F. Galtona v rámci své dovolené po Anglii bengálský policejní inspektor Edward Richard Henry. Ten si nechává od samotného Galtona vysvětlit všechny dosavadní výsledky zkoumání otisků prstů. Po návratu do Indie, začíná Henry vytvářet nové možné návrhy pro uvedení daktyloskopie do praxe. V počátcích se snažil doplňovat antropometrické policejní archívy kartami s otisky prstů, které se rozrostly do sbírky až dvou set tisíc karet. Chtěl tímto způsobem přesvědčit veřejnost a policejní orgány, že antropometrie je již zastaralá metoda a je třeba ji modernizovat pomocí otisků prstů. Povedlo se mu to až v roce 1897, kdy vládě předvedl nedostatky antropometrických identifikačních technik, ta posoudila, že daktyloskopie je výhodnější, finančně méně nákladná a rychlejší z hlediska délky času potřebného k vyřešení trestného činu. Na základě přínosu publikace „Classification and uses of finger prints“ Henryho zařadíme mezi první zakladatele kriminalistické daktyloskopie. Poslední osobou spjatou s historií daktyloskopie byl Chorvat žijící v Argentině Juan Vucetich. Působil jako policejní antropolog ve městě La Plata, kde také jako první zavedl do úplné praxe kriminalistickou daktyloskopii. Významným se však stal poté, co zdokonalil Galtonovu klasifikaci otisků. V jeho nové metodě označoval palce jako písmena od A do D a zbylé prsty jako čísla 1 až 4. Dokázal tak zařadit deltové body podle jejich velikosti a množství do čtyř skupin usnadňující třídění.

3.2 DAKTYLOSKOPIE A DERMATOGLYFIKA

Daktyloskopie je definována jako nauka zabývající se existencí obrazců papilárních linií umístěných na některých částech lidského těla např. vnitřní strana konečků prstů obou rukou, dlaní a chodidel. Na jiných částech povrchu těla se tyto obrazce papilárních linií nevyskytují. Daktyloskopie je začleněna mezi nejstarší kriminalistické metody sloužící k identifikaci osob. Značnou výhodou této metody je skutečnost, že lze jednoznačně určit původu otisků, a to od člověka, jelikož u jiných živočichů, kromě lidoopů se papilární linie neobjevují. Daktyloskopii je možné rozdělit do menších podoblastí zaměřující se na jednotlivá místa snímaní papilárních linií. Příkladem je chireoskopická disciplína zaměřená na otisky dlaní rukou a podoskopie, věnující se otiskům prstů a plosek na chodidlech. Nicméně tyto metody identifikace osob jsou v dnešní době považovány spíše jako okrajová záležitost. Podstatou daktyloskopie je schopnost identifikace neznámé osoby, na základě zanechaní stopy na určitém typu materiálu. Tyto stopy lze dlouhodobě uchovávat ve formě sbírek daktyloskopických karet nebo databází (AFIS). Obecně jsou daktyloskopické objekty (stopy) rozděleny do dvou oblastí, a to na získané stopy a porovnávací materiály. [10, 11]

Získané stopy jsou otisky, které vznikají působením tlaku papilárních linií pokrytých tenkým filmem tekutiny z potních kanálků na pevný nebo plastický povrch. Pokud je otisk vytvořen na plastickém povrchu je označován jako objemová daktyloskopická stopa. Výsledkem je trojrozměrný zrcadlově otočený reliéf struktury papilárních linií, díky kterému je vytvořený otisk časově stálý a snadněji identifikovatelný. Opakem je otisk pevný, označovaný také jako plošná daktyloskopická stopa. Tento typ dvourozměrné stopy je nejčastěji reprezentován odvrstveným a navrstveným otiskem prstu. Odvrstvená plošná stopa vzniká odloučení látky např. prachu, barvy či krve z určitého povrchu pomocí hřebenů papilárních linií, tento typ stopy vznikne za předpokladu existence velmi malé koncentrace potu na konečcích prstů, který je schopen na sebe vázat jiné látky. Druhým typem je navrstvená plošná stopa, ta vzniká nanesením a následným přenosem určité látky pomocí papilárních linií na jiné místo nebo předmět. Velkou roli zde hraje trvanlivost otisku, závisí tak např. na teplotě, vlhkosti, charakteru nosiče, který je buďto odebírán nebo přenášen a době od vzniku otisku do jeho zajištění. [11]

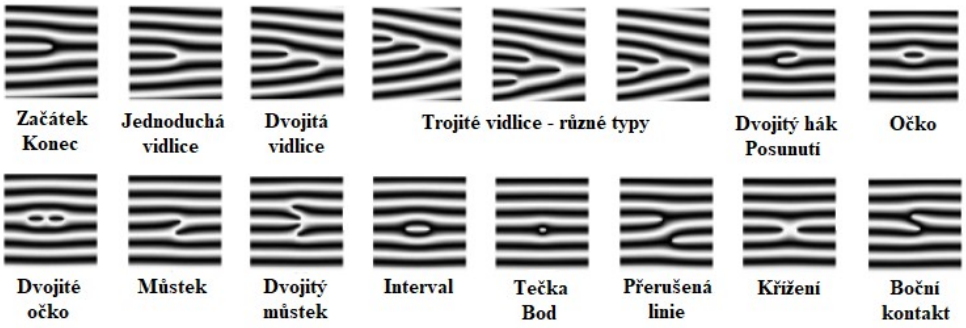
Porovnávací materiály tvoří obsáhlé kartotéky a databáze dříve zaznamenaných a uložených otisků konkrétních osob pro budoucí možné použití. Typickým příkladem jsou otisky zločinců spojených s trestnými činy, podezřelých osob pohybující se v blízkosti místa události a v poslední řadě u mrtvých osob, jejichž identita je neznámá. V moderní společnosti se však tyto materiály ve větší míře vyskytují spíše v oblasti výpočetní techniky (databáze AFIS), mobilních biometrických aplikací (Touch ID) nebo jako digitální zdroje identifikačních procesů při pasové letištní kontrole. Jedna z velkých předností daktyloskopie je možnost rychlého vyhledávání a zařazování karet s otisky prstů do systémů. Systémy uchovávající porovnávací materiály se dělí z hlediska vyhledávání na manuální a automatizované. Manuální jsou takové systémy, u kterých je nutné zařadit karty do předem daných skupin a kategorií, určující daktyloskopické charakteristiky spojené s otisky. Při následném hledání otisku s potencionální shodou, je potřeba vyhledávat právě podle příslušných skupin či kategorií nacházejících se na vzorovém otisku. Tento typ systému má však určité nevýhody jako je např. nízká rychlost vyhledávání a časově náročné porovnávání otisků nebo velikost ručně vytvářených kartoték a databází přesahující reálné fyzické kapacity. Opakem jsou systémy automatizované využívající výpočetní techniku, ty provádějí porovnávání podle předem daných algoritmů, které vyhodnocují vzájemnou korelaci důležitých daktyloskopických markantů se všemi vzorovými otisky. [11]



Obr. 7: Daktyloskopický porovnávací materiál z roku 1912, obsahující otisky prstů jednoho ze zakladatelů daktyloskopie Juana Vuceticha

Při identifikaci a hodnocení daktyloskopických materiálů z hlediska kvality a počtu jednotlivých rozpoznávacích znaků obsažených na otiscích prstů se obrazce dělí do tří kategorií. Tyto kategorie jsou odstupňované podle přesnosti shody potřebné ke správné identifikaci osoby. První a nejpřesnější je tzv. kategorie upotřebitelná k identifikaci. Do této kategorie patří všechny daktyloskopické stopy, které obsahují více než deset identifikačních znaků a mohou tak zároveň sloužit jako důležitý důkazní či procesní identifikační nástroj. Druhá je kategorie vztažena na částečně upotřebitelné otisky. Ty již obsahují pouze sedm až devět shodně orientovaných daktyloskopických markantů, nicméně nemohou být využity jako hlavní důkazní prostředek v kriminalistické daktyloskopii ale jako podpůrný prostředek vylučující ostatní otisky. Poslední a nejméně spolehlivou je kategorie zahrnující stopy neupotřebitelné, na kterých se nachází méně než sedm rozpoznávacích znaků. Příkladem těchto otisků jsou poškozené, rozmazané nebo pouze z části nasnímané stopy. Uvedené počty identifikačních znaků v otiscích jsou přibližné. Konkrétní hranice může záviset na charakteru původu, tvaru a chemického složení otisku. Rozdílné mohou být také požadavky k identifikaci v jednotlivých zemích, např. nejmenší požadavky jsou kladeny v Rusku (7 markantů) naopak nejvíce v Itálii a Velké Británii (16–17 markantů), v České republice je hranice stanovena minimálně desíti znaky.

Identifikace osob je přímo závislá na posouzení typu, velikosti a četnosti daktyloskopických markantů obsažených v každém otisku. Markanty jsou speciální elementární obrazce s vysokou identifikační hodnotou složené z různě spojených a uskupených papilárních linií. Jejich četnost a velikost se u každého člověka může měnit, nicméně základní tvar je vždy zachován. Příklady nejčastěji se vyskytujících markantů v otiscích je zobrazen na Obr. 8. K procesu porovnávaní daktyloskopických markantů se hodnotící osoba nebo systém (algoritmus) dostává až v poslední fázi identifikace. Úkolem algoritmu je nalezení stejného znaku na porovnávacím otisku, který byl dříve uložen do databáze nebo zařazen do kartotéky. Markanty jsou hodnoceny jako kvalitativní vzorky, naopak vzájemná poloha jednotlivých znaků a jejich vzdálenost, která je definována počtem papilárních linií mezi markanty určuje kvantitativní stránku otisku. Tím že existuje nespočet možných variací markantů obsažených v otiscích, je stanovena stupnice určující identifikační hodnotu každého znaku, která je dále využívána k finálnímu vyhodnocení shody dvou otisků. Tato hodnota lze vypočíst ze vztahu: $I = -\log n$, kde I je identifikační hodnota jednotlivého markantu a n označuje četnost výskytu markantů na 1 mm^2. Z experimentálních měření vyplývá, že nejvyšší hodnotu zastávají znaky: trojitá vidlice, křížení a můstek. Nejčastější a zároveň i méně hodnotné jsou dvojité vidlice, začátek, konec a tečka. [10]



Obr. 8: Výběr nejčastěji se vyskytujících daktyloskopických markantů na otiscích prstů (bílá barva představuje papilární linie)

3.3 PRINCIP ZPRACOVÁNÍ A VYHODNOCOVÁNÍ OTISKŮ PRSTŮ

Počítačové zpracování obrazové informace je velice komplexní a náročný proces zahrnující několik etap vývoje otisku. Před zahájením samotné úpravy obrazu je třeba vytvořit adekvátní prostřední pro správnou detekci signálu. Kvalita výsledného snímku je tak závislá na fyzikálních, atmosférických a chemických podmínkách či materiálových vlastnostech snímače. Důležitou roli hrají psychologické a fyziologické aspekty, které zásadním způsobem ovlivňují přesnost snímání a výsledný charakter otisků prstů. Příkladem jsou otisky s vysokou koncentrací obrazového šumu, což je nadbytečná a nežádoucí složka zabraňující správné identifikaci osoby. Obraz otisku rušeného šumem často vykazuje známky špinavého, zkrabatělého, neúplného nebo poraněného prstu. Některé otisky jsou dále zpracovatelné, jiné jako jsou např. mokré a suché otisky narušující strukturu papilárních linií v obraze nikoliv. [13]

Zpracování otisku prstu je přímo závislé na přesnosti a kvalitě biometrického snímače. Základní parametry jsou: snímací plocha, která se pohybuje v rozmezí od 1,5 cm^2 do 3,5 cm^2, nicméně existují i průmyslové senzory s plochou 100 cm^2 (registrace biometrických totožností). Za standard je v dnešní době považován snímač s plochou jednoho čtverečního palce (2,542 cm^2). Dalším parametrem senzorů je jejich rozlišení udávané v jednotkách DPI tedy *Dots Per Inch*. Při využívání biometrického snímače otisku prstu v oblasti kriminalistiky a policejně-soudní daktyloskopie je minimální hranice stanovena hodnotou 500 DPI. V praktické bezpečnostní sféře je však tento požadavek na rozlišení benevolentnější a systémy tak pracují v rozsahu 250 až 650 DPI. Poslední charakteristikou je bitová hloubka obrazu reprezentována hodnotami v jednotkách až desítkách bitů. Typicky je možné se setkat s 8bitovou hloubkou definující černobílou škálu od 0 do 255 odstínů. Existuje i mnoho dalších faktorů ovlivňující spolehlivost a kvalitu senzoru jako je způsob použité snímací technologie, rychlost přenosu dat nebo použitý algoritmus pro detekci markantů. Více k těmto charakteristikám je popsáno v dalších kapitolách.

První etapou při zpracování otisku prstu je zvýraznění kresby papilárních linií a odstranění nežádoucích šumů pro pozdější snadné nalezení markantních bodů. K tomuto účelu slouží tzv. adaptivní prahovací filtr, který má za cíl odstranit šum a zvýšit kontrast v prostorové kresbě otisku. Zmíněná metoda je v odborné literatuře označována jako prostorová konvoluce. Než je však z otisku odfiltrován šum je nutné provézt tzv. normalizaci, ta má za úkol odstranit technickou nedokonalost při snímání otisku způsobující nerovnoměrné zastoupení barevné škály odstínu šedé v obrazové informaci. Výsledkem normalizační standardizace je převedení hodnot stupně šedi do celého spektra, tedy převedený snímek bude obsahovat pixely s hodnotami od 0 až do 255. Účelem je zdokonalit vizuální charakteristiky papilárních linií a zvýšit matematické rozdíly mezi hodnotami pixelů na hřebenech a

údolích. Pokud tato operace není provedena, rozpoznávací algoritmus by v určitých oblastech odmítl vyhodnotit biometrické znaky v papilárních linií nebo by naopak mohl otisk nesprávně identifikovat. V dalším kroku je již možné použít zmíněnou prostorovou konvoluci, při které je otisk rozdělen do pomyslné sítě menších obrazových lokalit, v nichž se podle tónů šedé barvy vypočte směr vektorů papilárních linií. Následně je adaptivní filtr postupně aplikován na celou síť, ve které zvýrazní všechny pixely orientované ve směru vektoru linií a ostatní pixely orientované jiným směrem potlačí. [13]

Filtrovaný snímek otisku prstu nyní obsahuje pouze užitečné informace o papilárních linií a může postoupit ke druhé etapě zvané binarizace. Tento děj je důležitý z hlediska dalšího možného zpracování, jelikož nativní snímek zobrazuje otisk ve velkém množství odstínů šedé barvy s různými hodnotami kontrastu a jasu, je potřeba sjednotit pouze do dvou jednoznačných odstínů tzv. binárních hodnot. Těmi je bílá barva reprezentující prostor na pozadí kresby a šedá nebo černá barva definující sjednocený odstín papilárních linií dotýkající se snímací plochy. Proces binarizace je opět založen na prahovací úrovni, která stanovuje, zda daná hodnota pixelu (odstín šedé) bude převedena na nulovou tedy černou barvu nebo maximální hodnotu reprezentující bílou barvu. Platí zde však jedna podmínka deklarující správný průběh binarizace. Ta říká, že není možné použít globální práh stanovený pro celou matici obrazových bodů. Tím by vznikala „hluchá“ místa bez adekvátního přínosu pro detekci markantů. Z tohoto důvodu se využívá adaptivní prahování, které se vždy přizpůsobuje dané velikosti jasu v místě lokálních obrazových polí. Výsledek binarizace nemusí být kvalitní a může vytvářet nové miniaturní daktyloskopické markanty typu očko, interval nebo tečka, které nebyly součástí originálního snímku. Těchto nežádoucích znaků se lze zbavit pomocí procesu vyhlazení binarizace založeného na principech blob-coloring a flood-fill. Vyhlazení otisku je uskutečněno dle algoritmu, jehož úkolem je procházení binarizovaný obraz pixel po pixelu a ukládáním si hodnoty barvy aktuálního pixelu. Následně je pomocí funkce flood-fill v otisku vyhledávána oblast s osamostatněným polem odpovídající hodnotě menší, než je práh určující v tomto místě ostatní pixely na černou tedy minimální hodnotu. Nalezené pole je zaplněno barvou vyskytující se v přímém okolí (na papilárních linií je tato barva černá) a zaniká falešný daktyloskopický markant. [1, 5]

Poslední etapou předzpracování snímku otisku prstu je tzv. proces skeletizace. Z předchozího binarizačního algoritmu se vytvořil dvoubarevný snímek obsahující rozdílné tloušťky papilárních linií, které však nejsou optimálním zdrojem informací pro počítačové zpracování a nalezení markantů. Aby bylo možné získat adekvátní identifikační markanty je potřeba ztenčit tloušťku veškerých papilárních linií na velikost právě jednoho pixelu. Tím se zabrání nežádoucímu efektu bifurkace (zdvojení) daktyloskopických znaků, vznikajících v oblasti větvení a ukončení linií. V praxi se využívá např. Pavlidisův algoritmus tenčení, který pracuje na principu iterativního mazání pixelů v binarizovaném obraze, kde zkoumá osmiokolí bodu a vyhodnocuje, které pixely mohou být smazány a které patří k linii.

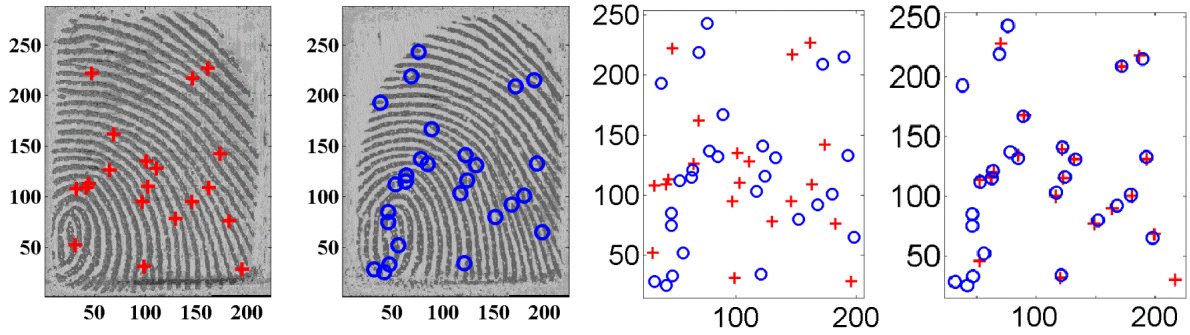
Obr. 9: Technologické kroky při zpracovaní obrazového signálu
Zprava nativní snímek, binarizace, skeletizace, nalezení markantů

V celkovém pořadí druhá, je navazující část na předzpracování, zabývající se automatickou detekcí daktyloskopických markantů v otiscích. Tento důležitý proces má za úkol vytvořit šablonu charakteristických biometrických znaků a uložit ji do počítačové databáze pro pozdější možné identifikovaní s jinými otisky v téže evidenci. Nalezení markantů vychází ze skeletizovaného otisku, který se nejvíce blíží k ideální reprezentaci papilárních linií. Je však nutné podotknout, že veškeré etapy předchozích úprav otisku a jejich kvalita jsou závislé na výpočetním výkonu daného systému. Jelikož nativní snímek může obsahovat až 250 000 pixelů (rozlišení 500 x 500), které jsou potřeba filtrovat, binarizovat a skeletizovat, jsou tyto operace časově náročné a někteří výrobci komerčních systémů tyto výpočetní aktivity úmyslně zkracují na úkor rychlejšího vyhodnocení identifikace. Ve výsledku se však stává, že předzpracovaný obraz není dostatečně kvalitní pro extrakci markantů a může docházet k nesprávným identifikacím identit. [1]

Velká část softwarových algoritmů je založena na vyhledávání základních daktyloskopických markantů, které však mají malou identifikační hodnotu jako je začátek a konec papilárních linií a dvojitá vidlice. Při extrakci těchto markantů se vychází z matematické definice, kdy začátek a konec papilární linie tvoří dva body vytvářející pomyslnou úsečku, dvojitá vidlice se definuje jako tři linie, které se zkříží do jednoho bodu. Ve složitějších aplikacích jsou algoritmy díky modernímu vývoji výpočetní techniky schopné zpracovávat více obrazových bodů např. trojité vidlice, křížení a můstky. Na začátku každého procesu extrakce se nejprve musí odstranit veškeré falešné znaky, které nejsou součástí předem definovaných markantů. Dle statistických pozorování se odstraní znaky jejichž délka neodpovídá průměrným hodnotám vzdálenostem mezi body charakterizující daný markant. Jako příklad je uváděna krátká linie, která má menší vzdálenost mezi dvěma body, než je předem stanovená průměrná vzdálenost pro znak vystihující začátek s koncem, a tudíž se s ní nepočítá. Podobně jsou odstraněny jizvy, papilární linie na krajích otisku a zároveň jejich hraniční body, které ve skutečnosti nejsou konečnými body na prstu ale pouze na obraze. [1]

Poté co jsou nalezeny všechny hledané markanty ve skeletizovaném snímku nastává fáze definování jejich základních charakteristik. Díky těmto reálným charakteristikám je dokážeme navzájem odlišit od jiných znaků v nejbližším okolí. Na začátku se definuje typ markantu, tedy jestli se jedná o začátek, ukončení, zdvojení, křížení a další. Poté jsou nalezeny konkrétní místa daného markantu v obraze, určí se jeho dvourozměrné souřadnice x a y. V poslední řadě je důležité stanovit orientaci makrantu tedy směr vektoru papilární linie. Výsledným produktem je tzv. šablona (minutae map) sloužící k porovnávání ostatních otisků, resp. jejich šablon uložených v databázi. Tvoří ji extrahované markanty v grafické vizualizaci reprezentující vzájemné logické propojení bodů pomocí úseček nebo matematických triangulačních systémů. Šablony obsahující pouze bodové prvky jsou dnes v moderních systémech nahrazovány důmyslnějšími šablonami s polygonálními liniemi vymezující přesné umístění daktyloskopických markantů. Podstatnou výhodu šablon tvoří fakt, že zákon na ochranu soukromí osob zakazuje ukládání originálních snímků otisků v komerčních aplikacích a šablony tedy musí být zpětně nezrekonstruovatelné. Konečný soubor šablony obsahuje přibližně deset až sto markantních prvků. Pro digitální uložení šablony do databáze je v závislosti na počtu možných typů markantů v šabloně potřeba od 1 bitu (pro šablonu rozlišující dva typy) až po několik bitů pro obsáhlý systém. Souřadnice bodu jsou vyjádřeny nejčastěji dvěma 8bitovými čísly (pro rozlišení senzoru 250 x 250 pixelů) a jedním 8bitovým číslem pro uložení orientace bodu. Pokud např. jeden bod v šabloně zaujímá velikost přibližně 25 bitů, tak šablona se sto body bude mít velikost 313 bajtů což v rozsáhlých systémech s tisíci otisky vyžaduje odpovídající výpočetní výkon. V praxi však moderní aplikace dokáží pracovat i s 1 kB šablonami. [1]

Klíčové uplatnění nachází šablona při procesu identifikace či verifikace, kde slouží jako podklad pro porovnávání s ostatními právě extrahovanými otisky se šablonami. Existují tři základní metody na rozpoznávání otisků prstů. Hlavní a ve velké míře používaná je metoda založená na principu detekce markantů v obou šablonách a jejich vzájemné rozložení, kde algoritmus porovnává pozici obou bodů jejich typ a gradient nebo vektor směru natočení. Této problematice se věnují dvě nejčastěji používané metody, a to Hongova a Rathova. Jejich role spočívá ve vytváření globálního zarovnání neboli překryvu šablon a následného hledání lokálních posunů u konkrétních markantů. K přesnému zarovnání pomáhají dva singulární body, kterými jsou delta a střed neboli vrchol otisku. Nalezení těchto bodu se řídí podle úhlové sumarizace papilárních linií, které těsně přiléhají k danému typu markantu, tzv. Poincaré index. Je nutné podotknout, že nalezení stoprocentního vzájemného překryvu u všech bodů není reálné, jelikož při každém novém položení prstu na snímač dojde k odlišnému rozložení kožních struktur. Řešením tohoto problému je stanovení minimálního počtu bodů, které se musí shodovat, aby byl otisk správně identifikován. V kompaktních systémech méně zastoupená je metoda založená na charakteristikách papilárních linií např. tvar, velikost a četnost linií. Důvodem menšího obsazení je softwarová výpočetní náročnost a důmyslnost. Princem identifikace je globální zkoumání otisku jakožto celého obrazu s absencí extrakce markantních bodů. [1, 5]



Obr. 10: Příklad identifikačních šablon dvou totožných otisků ve stádiu extrakce daktyloskopických markantů, první a druhý snímek reprezentuje dva otisky stejné identity s časovým rozestupem snímání. Obrázek vpravo zobrazuje výsledné ztotožnění obou daktyloskopických šablon.

3.4 MODERNÍ TECHNOLOGIE PRO IDENTIFIKACI OSOB

Zásluhou rychlého nástupu vývoje informačních technologií, polovodičových komponentů, výpočetních jednotek a miniaturizací biometrických senzorů je v dnešní době možné využívat tyto komerční systém kdekoliv kde je aktuálně potřeba zjistit identitu osob. Postupem času byla stále častěji realizována výroba autentizačních systémů a přístrojů díky velkým technologickým společnostem jako je Dermalog, Motorola, Printrak nebo Apple a tím se také dostávala do povědomí velké části veřejnosti. Komerční aplikace se určitým způsobem liší od průmyslových systémů pro administrativně-soudní odvětví (AFIS, NAFIS, Eurodac) a to hned v několika aspektech. Prvním rozdílem je fakt, že komerční systémy pracují v režimech identifikace 1:1, případně 1:N, avšak velikost *N* otisků v databázi se na rozdíl od průmyslových systémů, kde se pracuje se stovkami tisíc až milióny otisků, pohybuje v rozmezí desítek až tisíců otisků. Druhou vlastností je zjednodušení algoritmů na předzpracování a extrahování markantních bodů pro celkově rychlejší vyhodnocení identity, přizpůsobené běžným stolním počítačům nebo jednoúčelovým vestavěným zařízením. Posledním odlišným faktem je skutečnost, že u komerčních systémů, pokud dojde k automatickému zamítnutí identifikačního procesu, je možné pokus zopakovat. Zároveň sám algoritmus rozhoduje, zda je konečný verdikt pozitivní či negativní. [1]

Oblast využití komerčních produktů využívající otisky prstů jako hlavní biometrický prostředek pro autentizaci lze rozdělit do čtyř kategorií, které díky trvalému vylepšování informačních technologií a nejvíce prozkoumané problematice biometrik se řadí mezi sféru maximálně preferovaných systémů pro kontrolu a správu osobního majetku či administrativní identifikaci. Jejich značné pozitivum spočívá v několika okolnostech, zaprvé se jedná o dobrou akceptovatelnost jak veřejností, tak uživateli i právními institucemi, zadruhé se stále častěji uplatňuje možnost integrace snímačů do přenosných či vestavěných systémů a mobilních zařízení, a to především díky své malé velikosti a spotřebě. Jako poslední příklad je uváděna spolehlivost a relativně vysoká přesnost daktyloskopických metod. [1]

Tab. 2: Oblasti nasazení biometrických aplikací v praxi

Oblasti technologie biometrických systémů			
Kontrola oprávnění přistupovat k výpočetní a komunikační technice (PC, mobilní telefony, servery, síťové prvky)	Zintenzivnění ochrany osobních identifikačních a platebních karet, případně jiných ID tokenů	Dohled nad povolením vstupovat do soukromých objektů (sklady, výrobní haly, kanceláře)	Ochrana soukromého vlastnictví před zneužitím nebo neoprávněnému použití

Kontrola uživatelů umožňující přistupovat k výpočetní a telekomunikační technice je typickým příkladem využití otisků prstů v praxi. Rozvoj této oblasti komerční biometrie začíná okolo roku 1990, kdy tehdejší světoví lídři předváděli na poli informatiky nové automatizované přístroje s optickými a kapacitními snímači spolu s počítačovým příslušenství jako jsou klávesnice a myši s integrovanými snímači otisků nebo notebooky s tzv. swipe snímači. Na začátku 21. století se ve větší míře začaly objevovat senzory v malých přenosných prostředcích typu PDA jako je HP-IPAQ H 5450 s vestavěným lineárním snímačem. Další velký posun nastal po 11. září 2001 kdy americká vláda přešla na nový sofistikovaný systém US-VISIT s registrací každého nově příchozího do spojených států. Tento systém jako první ve velkém měřítku zavedl skenování všech pěti prstů jedné ruky, a to na optických senzorech s rozměrem snímací plochy 10 x 10 cm. S pokračujícím vývojem technologií vniklo nespočet dalších zařízení v různých oblastech informatiky, pro příklad některé nejvýznamnější produkty: [1, 14]

- Mobilní telefony – *HTC P6500 (2007), Motorola ATRIX 4G (2011), Apple IPhone 5S (2013)*
- Notebooky – *HP NC6320 (2006), Acer Aspire 8372 (2010), Dell E6410 (2010)*
- Klávesnice – *Microsoft se senzorem Digital Persona (2005), Packard Bell 1610 (2007)*
- Myši – *Cezam MK 2 (1999), Siemens IDMouse M4000 (2007), CrucialTec TrackPad (2016)*
- USB Tokeny – *Egistec U2F Dongle (2015), Hypr OTP (2016), Kensington Verimark (2017)*
- Zdravotnictví – *Pacientský monitor Xplore C5 (2007), Uchování léčiv GeneSYS-RX (2015)*

Druhým odvětvím jsou čipové a platební karty podporující biometrickou identifikaci. Tento typ autentizace nebo správně řečeno verifikace je v dnešní době na ústupku a je nahrazován výše uvedenými systémy. Obecně lze čipové identifikační karty rozdělit na dva okruhy. Prvním typem jsou karty jejichž šifrovaný biometrický obsah je uložen v paměti EEPROM na integrovaném obvodu, v odborné literatuře se tato technologie nazývá ToC (Template on Card). Tyto karty se při identifikaci zasouvají do speciálního přístroje a zároveň je prst pokládán na snímací plochu, zařízení je přitom neustále připojeno k PC. Při procesu nastává porovnání snímaného tisku s uloženou šablonou na čipu. Jedná se tak o dvoufázovou autentizaci, jelikož zde využíváme principu něčeho, *co máme* a něco *čím jsme*. Velkou výhodou je fakt, že nepotřebujeme využívat síťový provoz ke čtení osobních údajů z databáze a zároveň

můžeme mít tyto informace ihned při sobě. Druhý typ reprezentují složitější karty označované jako BSoC (Biometric System on Card), tedy systém fungující na kartě. Jde o zatím nejlépe zkonstruovanou technologii zaměřenou na identifikační karty. Nabízí vyšší standardy zabezpečení, pokud jde o potencionální útoky, jelikož získaný obraz otisků prstů, jeho šablona, proces ukládání a rozpoznávání se uskutečňuje zásadně a pouze v rámci jedné karty. Biometrická čipová karta obsahuje veškerou potřebnou elektroniku pro fungování, tedy vestavěný mikročip, senzor otisků, proximity anténu pro magnetický přenos dat a operační systémy jako je základní firmware pro zápis, vytváření a ukládání šablon i jejich rozpoznávání. Modernější verze mohou obsahovat program na šifrování nebo vymazání šablon, pokud jsou zjištěny pokusy s neoprávněnou manipulací. Tento typ karet představuje nejvyšší stupeň zabezpečení díky tří faktorové autentizaci, která využívá všech základních podmínek, kterými jsou fyzický předmět, v tomto případě karta, dále pak pin, jehož tvar víme jen my sami, a nakonec otisk prstu. V praxi se s těmito kartami můžeme setkat v platebním sektoru jakožto nástroj pro zabezpečení a správu účtů nebo čistě jako debetní či kreditní karta. [1, 14]

- Čtečky karet: *Precise Biometrics 100 SC (1999), Silex MUSB 200 Combo (2001), Ewaytek (2006)*
- Platební karty: *Siemens Inferion (1998), NovaCard biosmart (2002), Quardlock (2015)*
- Karetní tokeny: *AXSionics AG (2006), BioMetAccess (2006), Validus BC-25 (2010)*

Velkým podílem na trhu je zastoupena třetí oblast využívající biometrickou identifikaci pomocí otisku prstu k ochraně a kontrole oprávněnosti osob vstupovat do soukromých prostor jako jsou výrobní haly, továrny, specializovaná pracoviště nebo kancelářské budovy. Z technologického pohledu jsou tyto systémy podobné jako u autentizačních zařízení kontrolující přístup k informačním technologiím. Nicméně jsou umístěny do odolnějších krytů na stěnu poblíž vstupních dveří nebo i přímo na dveře v podobě klikových mechanismů. Proces identifikace je ve většině případů nastaven na algoritmus 1:N, tedy porovnávání šablon probíhá s mnoha jinými šablonami, jelikož v systému může být registrováno hned několik oprávněných osob. Zabezpečení je možné zvýšit připojením dalších technologií, např. pomocí čipových karet a hesel. Přístroje, které uplatňují obě tyto technologie mají poblíž snímače na otisk prstu jednoduchou číselnou klávesnicí s displejem a slotem na kartu. Používání hesla či pinu má dvě podstatné výhody. První spočívá ve zvýšení zabezpečení, neboť je použit další ověřovací nástroj. Druhou výhodou je možnost využití časově rychlejšího režimu verifikace (1:1), při kterém je posuzován právě snímaný otisk s dříve uloženým otiskem, jehož šablona je spojena s konkrétním heslem nebo pinem. Není tak potřeba hledat stejnou šablonu v databázi s tisící otisky. [1, 14]

- Zámky dveří: *BioCert FS-100, Fingersec FS 3000, Linpo BioLock BLS-2A, iSmartEye L3 (2016)*
- Docházkový systém: *IDTECK Finger 007, CEM S610f (2008), Biometrix BioLock FU8 (2009)*

Posledním velkým odvětvím využívající daktyloskopické metody jsou přístroje na ochranu soukromého majetku proti jejímu odcizení a zneužití nebo přístupu k nebezpečným mechanismům. Na rozdíl od většiny univerzálních systémů s rozměrově velkými senzory, je v těchto aplikacích kladen důraz na miniaturizaci, odolnost a spolehlivost snímačů otisků, z důvodu umístění do běžných předmětů. Typickým představitelem této kategorie jsou systémy na zabezpečení aut, motorek a lodí proti odcizení nebo trezory, visací zámky a pouzdra k uložení ručních palných zbraní. [14]

- Zabezpečení aut: *Startovací systém Audi Nuvolari se snímačem Inferion (2003), Volvo SCC (2001)*
- Trezory: *Diplomat Safe 070-FPL (2008), Trezor na zbraně Gunvault GVB5900-F (2008)*
- Visací zámky: *iFingerLock LLC (2016), Tapplock (2016), Bio-key TouchLock TSA (2017)*

4 DRUHY IDENTIFIKAČNÍCH SENZORŮ OTISKU PRSTU

V oblasti daktyloskopického snímání otisků ať už digitálního nebo analogového, je kladen důraz především na kvalitu vstupních informací. Dle historického ale také technologického charakteru lze snímání rozdělit do dvou základních skupin. Historicky starší je *klasické* snímání otisků někdy nazývané jako off-line snímání, které využívají z velké části bezpečnostní a kriminální složky. Termín klasické snímání spočívá v metodě manuálního vyhledávání, zviditelňování (pomocí tiskařské černě), fixace a vytváření evidenčních karet s jedním nebo mnoha otisky prstů. V prvotní fázi sběru informací nejde o digitální proces, avšak s vývojem moderních počítačových technologií a velkému počtu evidenčních karet, ve kterých čím dál tím častěji docházelo k časově dlouhodobým identifikacím, bylo potřeba zavézt převedení manuálně vytvořených obrazů do elektronické formy pomocí klasických obrazových senzorů. Na tento typ snímání navazuje dnes již možná jediný způsob sběru dat v komerčních aplikacích a tím je *bezprostřední* snímání otisků. Díky této novější metodě je snímání a vyhodnocování otisků rychlejší, přesnější a také z hlediska hygienického a finančního přijatelnější. S touto metodou je často spjat pojem live-scanning, který ji definuje jako technologii pro snímání a digitalizování obrazových dat v reálném čase s použitím počítačové techniky. Do kategorie live-scanning patří veškeré moderní digitální snímače, které lze rozdělit podle toho, na jakých fyzikálních principech pracují a zda využívají přímého kontaktu papilárních linií se snímačem. Obecně se tyto senzory rozdělují na kontaktní a bezkontaktní. Kontaktní senzory se člení na optické, elektronické, opto-elektronické, kapacitní, tlakové a teplotní. Naopak bezkontaktní senzory se rozdělují pouze na optické a ultrazvukové. [4, 12]

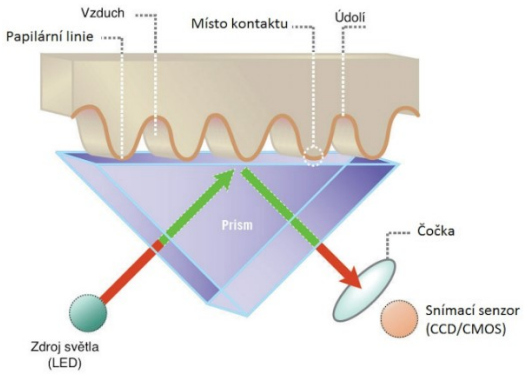
4.1 KONTAKTNÍ SENZORY

Skupina těchto senzorů patří vůbec k nejpoužívanějším na světě, a to především díky přesnosti fyzikální technologie snímání, jednoduchosti odebrání otisků a finanční nenáročnosti. Společným znakem této skupiny senzorů je přímý kontakt papilárních linií a snímací plochy, která může mít různé tvary a velikosti. Hlavní podstata snímání spočívá ve využití plastičnosti povrchu konce prstu, která je dána vystupujícími hřebenovitými výběžky a prostorovými rýhami (tzv. údolí). Značnými nevýhodami jsou horší hygienické podmínky a s tím spojené častější čištění snímací plochy, potencionální zanechání zneužitelného otisku nebo zkreslení otisku při větším přítlaku na snímací plochu. Nicméně i přes určité nedostatky, existuje velké množství kladných charakteristik ovlivňující velké rozšíření těchto senzorů.

4.1.1. OPTICKÉ SENZORY

Optické senzory fungují na jedné z nejstarších metod snímání, vyvíjených od 70. letech minulého století a v dnešní době jde zároveň o nejpoužívanější typ senzoru v komerční sféře. Princip činnosti optického senzoru vychází z techniky FTIR (Frustrated Total Interal Reflection), tedy rozdílné odrazivosti světelného záření, ve smyslu zachycení viditelného světla odraženého od rozhraní plochy hranolu a přiloženého prstu. Jako zdroj vysílaného světla je ve většině případů použita LED dioda nebo laserový paprsek. Dvourozměrný obraz otisku je zachycen na svrchní straně senzoru a dále odražen směrem k maticovému CCD nebo CMOS detektoru, ve kterém je analogový signál digitalizován a dále zpracováván. Pod dotykovým povrchem je umístěna velmi tenká fotocitlivá luminiscenční vrstva, která má za úkol osvětlit a tím i zvýraznit strukturu otisku. Výsledný obraz vznikne tím, že světlo pocházející ze zdroje je odraženo od papilárních linií, v tomto případě pouze od hřebenů těsně přiléhajících k

povrchu průhledného hranolu senzoru. Údolí mezi papilárními liniemi není možné na CCD detektoru zaznamenávat díky absenci těsného kontaktu kůže se snímací plochou a zároveň díky nastavené citlivosti, která je dána tak, aby světlo o definované intenzitě nebylo zaregistrováno. Vývoj optických senzorů byl dlouhý, první prototypy měli velikost 15 x 7,5 x 15 cm. Od konce 90. let se vývoj razantně zlepšil a velikost senzorů již byla srovnatelná s těmi současnými. V dnešní době lze zakoupit optický senzor s velikostí menší než 3 cm^3. Značnou výhodou optického senzoru je vysoká kvalita snímaného obrazu, malá velikost zařízení, rychlost snímání a následné identifikace. Na druhou stranu zde existuje nutnost pravidelného čištění snímací plochy od nečistot ulpělých z povrchu kůže při snímání. [4, 12]



Obr. 11: Princip technologie optického senzoru.

Obr. 12: Optický systém Guardian US-VISIT

4.1.2. ELEKTRONICKÉ SENZORY

Elektronické senzory využívání vlastností elektrického pole mezi dvěma paralelně umístěnými vrstvami, které tvoří povrch kůže přiložený na snímací plochu senzoru a elektricky nabitá destička. Tím, že změníme tvar horní vrstvy senzoru z rovného na zvlněný, díky různorodé struktuře papilárních linií, je rovněž změněna velikosti elektrického pole. Pokud přiložíme prst na povrch senzoru, uzavře se pomocí vodivého kroužku obtočeného podél okraje senzoru elektrický obvod a vlnitou strukturou kůže začne procházet velmi malý proud s referenční hodnotou signálu. Pomocí miniaturních deskových antén umístěných na základní desce senzoru je tento už zkreslený referenční signál snímán a dále předán k zesílení a zpracování pro další použití. Princip detekce rozdílných hodnot elektrického pole spočívá odlišné vodivosti papilárních linií a brázd, ve kterých je signál více potlačen. Velkým pozitivem je odolnost vůči špíně a znečistění povrchu kůže. Senzor je navíc rezistivní proti mokré či suché pokožce.

4.1.3. OPTO-ELEKTRONICKÉ SENZORY

Opto-elektronická senzory jsou složeny ze dvou velmi tenkých rovnoběžných vrstev, které mají technologicky náročné zpracování. Svrchní vrstva senzoru, jenž tvoří těsný kontakt se snímaným prstem, je vyrobena z tenkého polymerového filmu tzv. TFT (Thin-film transitor), který se skládá z matice miniaturních tranzistorových polí sloužících k detekci přiložení kožního reliéfu na povrch senzoru. Reakce na přiložení prstu vyvolá emisi světelného záření z TFT vrstvy. Díky tomu je schopna druhá vrstva ležící pod TFT filmem, zachytit na fotodiodách odražené světlo od papilárních linií. Ty pak následně převádějí dopadající světlo na elektrický signál, který je dále zesilován a zpracováván. Výsledkem převodu je viditelný daktyloskopický snímek. Výhodou opto-elektronického senzoru jsou jeho malé rozměry, vysoká kvalita obrazu a odolnost proti vnějším vlivům jako je teplota a vlhkost. [12]

4.1.4. KAPACITNÍ SENZORY

Kapacitní senzory jsou navrženy ke snímání otisků prstů pomocí zákonitosti měření elektrické kapacity. Hlavní část senzoru je tvořena rozsáhlou maticí z mnoha set tisíc vzájemně odizolovaných kovových plošek velkých jen několik desítek mikrometrů, představující jednu ze dvou vodivých elektrod reálného kapacitoru. Elektrody jsou pokryty velmi tenkým filmem oxidu křemičitého, který slouží k fyzickému oddělení snímacích plošek a přikládaného prstu. Zároveň zastává funkci dielektrika kondenzátoru. Při kontaktu prstu se snímačem dojde pomocí papilárních linií k tzv. přemostění mezi oddělenými vodivými ploškami. Tento děj je snímán a jeho velikost pak odpovídá napětím a kapacitním úbytkům mezi dvojicí plošek. V rámci této metody se neuplatňují brázdy kožních struktur, ty slouží jako vzduchové izolanty. Zesílením a převodem naměřeného napětí získáme digitální mapu kožního reliéfu. Výbornou charakteristikou kapacitních senzorů je možnost vytvoření rozmanitých velikostí snímacích ploch (např. lineární či maticová) a tím i možné uplatnění v mobilních přístrojích. Kapacitní senzor však má hned několik nevýhod. Jedněmi z nich jsou velká citlivost na síťové rušení (60 Hz) a znečištění konečků prstů způsobující změnu vodivosti vedoucí ke zkreslení obrazu. [12]

4.1.5. TLAKOVÉ SENZORY

Tlakové senzory lze obecně rozdělit do dvou technologicky odlišných kategorií. Prvním typem jsou senzory fungující na principu lokálního tlakového působení papilárních linií na snímací plochu, která je tvořena pružnými piezoelektrickými krystaly. Naopak v oblasti brázd je tlak menší a díky tomu jsou odlišné struktury lépe rozpoznatelné. Vliv nepatrného tlaku kožních struktur na piezoelementy je transformován do elektrického napětí reprezentující přesný obraz daktyloskopického otisku. Druhým typem jsou tří vrstvé tlakové senzory. Svrchní plocha je tvořená z velmi tenkého, pružného a elektricky vodivého materiálu, který zastává funkci jedné poloviny elektrody. V prostřední vrstvě je po celé délce senzoru umístěn nevodivý gel. Poslední částí je druhý panel vodivé elektrody. Při umístění prstu na snímací plochu dojde ke stlačení gelu na takovou míru, že papilární linie vytvoří kontakt mezi svrchní a spodní vrstvou senzoru a v místě spojení vznikne elektrický impuls. Tlakové senzory jsou všeobecně považovány za velmi stabilní a schopné snímat jak suchou, tak mokrou kůži. Jedním z prvních, kdo přišel na trh s tlakovým senzorem byla japonská firma JDFS, ta po mnoha letém vývoji představila v roce 2001 unikátní senzor schopný implementace do platební karty, který má zajistit zvýšenou ochranu.

4.1.6. TEPLOTNÍ SENZORY

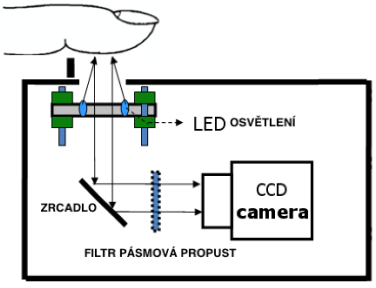
Teplotní senzory vynikají především díky technologické jednoduchosti a malým rozměrům. Princip teplotních senzorů spočívá v detekci teplotních změn mezi papilárními liniemi a brázdami. V průběhu snímání je prst přikládán nebo posouván po senzoru (podle typu) složeného z velkého počtu citlivých senzorů tzv. pyrodetektorů. Papilární linie při snímání těsně přiléhají ke snímací ploše a tím dochází k většímu přenosu tepla na senzory. Na druhou stranu brázdy emitují díky vetší vzdálenosti od senzoru menší teplo a tím je možné znázornit matici rozložení teplých a teplejších míst, ze kterých následně vznikne otisk prstu. Velké zastoupení tohoto typu senzoru tvoří tzv. lineární nebo také swipe snímače, ty pomocí posouvání prstu přes snímač vytvářejí obrazové segmenty dat z naměřených teplot papilárních linií. Jednotlivé segmenty jsou rekonstruovány a spojeny v jeden snímek charakterizující otisk prstu. Výhodu senzoru je absence senzibility na síťové rušení a odolností proti vnějším vlivům.

4.2 BEZKONTAKTNÍ SENZORY

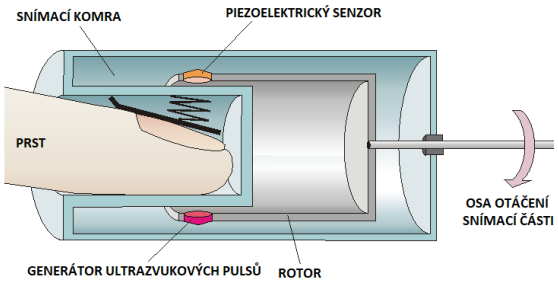
Navazující skupinu tvoří senzory bezkontaktní, které nevyžadují bezprostřední kontakt pokožky prstu se snímací plochou. Díky této technologii je možné předejít určitým specifickým nedostatkům vyskytujících se u kontaktních senzorů jako je značná citlivost na znečištění konečku prstu, znečištění samotného snímače pravidelným používáním nebo neschopnost identifikovat suché a mokré otisky. Bezkontaktní senzory vynikají především v oblasti eliminace nežádoucích zkreslení výsledného otisku, které je většinou způsobeno špatným přítlakem prstu na snímač. Výsledný obraz otisku papilárních linií v obrazu tak může být nesprávně hodnocený. Méně častým, nicméně stále důležitým bezpečnostním problémem, který se objevuje u kontaktních senzorů je zanechávání otisků z předchozího rozpoznávání na snímací ploše, tato záležitost je však u bezkontaktních senzorů vyloučena. K nejvýznamnějším typům bezkontaktních senzorů patří optické a ultrazvukové. [2, 12]

4.2.1. OPTICKÉ SENZORY A ULTRAZVUKOVÉ SENZORY

Princip optických bezkontaktních senzorů vychází z obdobné technologie snímání jako je tomu senzorů kontaktních (optických). Při samotném snímání však nedochází ke kontaktu snímací plochy a prstu. Ten je přikládán ve vzdálenosti tří až pěti centimetrů nad kvalitní CCD nebo CMOS snímač do podpěrné konstrukce, aby se zabránilo potenciálnímu zkreslení obrazu při pohybu prstu a zkreslení papilárních linií působením tlaku prstu na snímací plochu. Pro přesnější detekci kožních struktur se používá několik světelných zdrojů, nejčastěji LED, umístěných po obvodu průhledové části senzoru. Další netradiční způsob snímaní probíhá za pomoci několika kamer rozmístěných v určitých úhlech od prstu, ty následně vytvoří jeden trojrozměrný obraz papilárních linií. Bezkontaktní snímání otisků může způsobovat určité potíže, které je nutné v procesu předzpracování odstranit. Jedná se o nerovnoměrné osvětlení kožních struktur, rozostření obrazu v důsledku pohybu prstu nad senzorem nebo nesprávné nastavení kontrastu kamery. Druhou možností bezkontaktního snímání jsou ultrazvukové senzory. Jde o vůbec nejpřesnější kategorii senzorů. Základ snímače je tvořen válcovou snímací komorou, do níž se umísťuje prst, kolem kterého rotuje ultrazvukový vysílač spojený s přijímačem. Obě zařízení se skládají z piezoelektrických měničů, kde jeden z nich vysílá krátkovlnné akustické svazky (4-24 MHz) směrem k prstu a druhý zaznamenává akustické pulsy odražené od papilárních linií. Doba mezi příchodem odražené vlny od papilární linie a od brázdy se nepatrně liší, nicméně díky této skutečnosti lze vytvořit obrazovou strukturu otisku prstu. Finální otisk je velmi přesný (rozlišovací schopnost 0,1 mm), kvalitní a nezkreslený. Výhodou tohoto senzoru je nezávislost vůči znečištění pokožky a vlhkosti prstu. Velkým pozitivem je bezpečnostní odolnost vůči falešným silikonovým a jiným nalepovacím otiskům. Část svého uplatnění nalezl v oblasti kriminalistiky, konkrétně při odebírání otisků mrtvých osob. [1, 12]



Obr. 13: Princip snímání otisku pomocí bezkontaktního optického senzoru



Obr. 14: Princip rotačního ultrazvukového senzoru s piezoelektrickými měniči

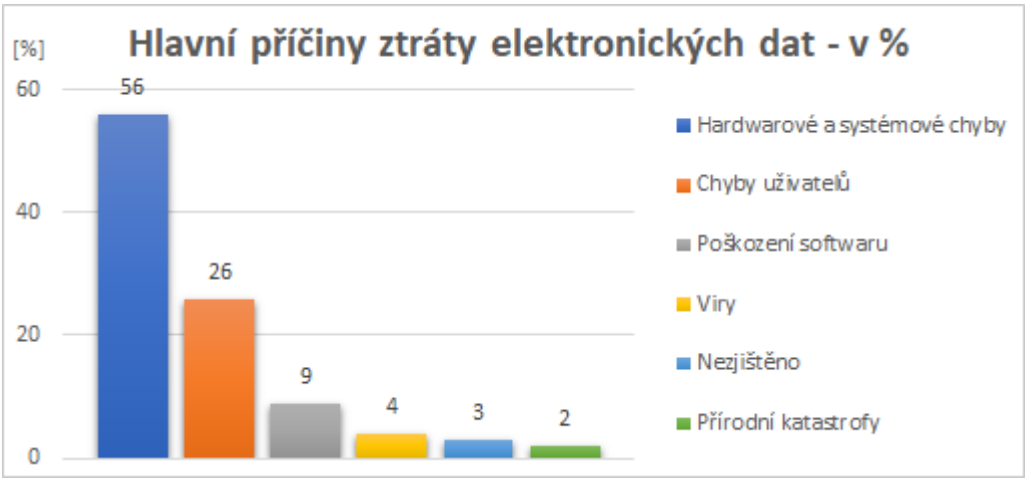
5 SÍŤOVÁ DATOVÁ ÚLOŽIŠTĚ

Počet a velikost datových souborů od firem či domácností se v dnešní době razantně způsobem zvyšuje. Důvodem růstu objemu informací je častější používání a vývoj informačních technologií. Většina fyzických dokumentů, fotografií, filmů a korespondence je převáděna do digitální oblasti, díky níž je možné data skladovat ve velkém počtu na relativně malé ploše diskových polí. S příchodem moderních výpočetních zařízení byl čím dál tím více kladen důraz na schopnost sdílet informace navzájem mezi počítači nebo síťovými úložišti. Současným trendem je ukládání a sdílení datových souborů na serverech, které jsou přístupné z jakéhokoliv místa a zařízení skrz internetovou síť. Dalším podstatným aspektem síťových úložišť je ochrana důležitých informací, které je nutné mít zálohované a zašifrované na různých místech nezávisle na chodu počítače. V teorii síťových úložišť lidé sjednocují dva pojmy, které mají podobný název, avšak rozdílný význam. Prvním je zálohování, což je děj, při kterém jsou vytvářeny bezpečnostní kopie současných datových souborů. Druhým dějem je archivace, při ní jsou pouze přesouvány aktuálně nepotřebná data na jiné volné úložné médium např. kompaktní disk nebo flash disk. Rozdíl obou způsobů ukládání dat spočívá v určení bezpečnostních priorit. [15]

5.1 DŮVODY PRO ZÁLOHOVÁNÍ INFORMACÍ

Záloha (ang. Backup) spočívá v ukládání informací na datové médium vhodné pro zálohování např. externí harddisk nebo síťové úložiště, které v ideálním případě má nulový nebo co nejmenší možný vztah s primárním zdrojem datových souborů. V procesu zálohování je potřeba přesouvat data na média, která mají minimální technickou závislost na stavu zdrojového systému a hardwarových součástí. Zálohy jsou prováděny buďto v pravidelných nebo nepravidelných cyklech. Při pravidelných zálohách je médium kontinuálně připojeno ke zdrojovému systému (princip klient-server), naopak nepravidelné zálohy jsou vytvářeny na médium, které je přenositelné. Ve velkých firmách se značným objemem dat jsou používány komplexní automatizované systémy, jejichž úkolem je účinně zálohovat mnoho zařízení propojených intranetovou sítí (technologie NAS). Bezpečnostní replikace dat může probíhat v online režimu, kdy se proces zálohy uskutečňuje při běžném provozu počítače. Opačným typem je tzv. offline zálohování, při níž je prováděna záloha zařízení mimo standartní chod počítače. [15, 16]

Existuje celá řada podnětů, proč je potřeba data zálohovat. Jedním z hlavních důvodů je zejména obava z možné ztráty nebo poškození důležitých osobních informací. V dnešní době již existuje mnoho sofistikovaných programů a algoritmů, jak případné ztrátě dat zabránit, nicméně velká část veřejnosti stále spoléhá na jedeno úložné místo, v tomto případě harddisk počítače, které obsahuje veškerá osobní data společně s operačním systémem. Ve většině případu je při selhání disku ztráta informací nevratná. Dalším neméně podstatným důvodem zálohování na externí zařízení je limitovaná kapacita aktuálně používaného úložného prostoru, které není určené pro dlouhodobé uchovávání objemných datových souborů. Kvalita a užitečnost síťových úložišť je ovlivněna několika faktory, prvním je velikost pamětí diskových polí, maximální objem dat zapsaný na disk za jednu sekundu, dále pak propustnost a rychlost (tzv. bandwidth, resp. throughtput) síťové infrastruktury v daném místě, operační systém zálohovacího serveru (nejčastěji Linux/Unix) a nakonec konektivita s dalšími síťovými prvky. Všechny potencionální ztráty dat jsou zapříčiněny různými chybami, které lze rozdělit do několika kategorií. Nejčastější chybou jsou hardwarové a systémové selhání. Následují chyby vytvořené samotnými uživateli jako je nechtěné odstranění souborů nebo ztráta zálohovacího média. V poslední řadě to jsou viry a přírodní katastrofy.



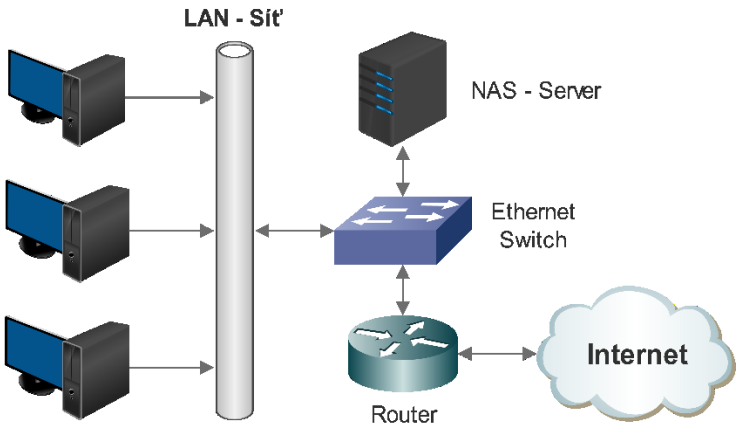
Graf 1: Grafické zobrazení hlavních příčin ztrát digitálních informací [19]

5.2 ARCHITEKTURA ZÁLOHOVACÍCH SYSTÉMŮ

Technologie zálohovacích systémů je rozdělena na tři velké celky, kde každý z nich reprezentuje odlišné řešení pro ukládání dat, nicméně se stejným problémem, kterým je zaručení bezpečné zálohy dat a dostupnost těchto informací v rámci síťové sféry. Výběr konkrétního typu síťového úložiště závisí na detailním zvážení všech technologických aspektů, kterými jsou geografické umístění navrhovaného systému, způsob připojení ke koncovým zařízením, velikost úložného prostoru, princip uchovávání dat nebo také určení oprávněnosti uživatelů přistupovat k datům. Podle rozsahu působení můžeme systémy rozdělit na technologie DAS (Direct Attached Storage), NAS (Network Attached Storage) a v poslední řadě SAN (Storage Area Network). Každá z těchto metod má své specifické oblasti vlivu a užívání. [16]

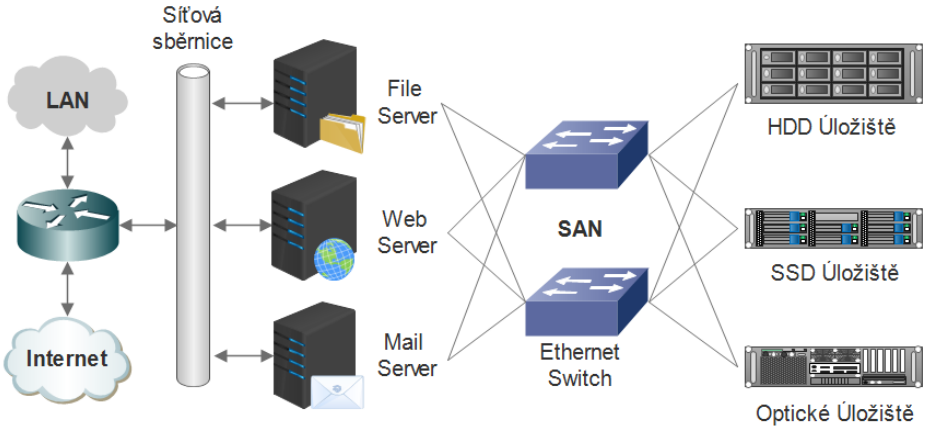
NAS (Network Attached Storage) představuje komplexní systém pro ukládání dat, připojený do společné počítačové sítě, umožňující uživatelům přistupovat v úplné nebo omezené míře k uloženým informacím. NAS je ve skutečnosti server obsahující buďto jeden nebo až desítky pevných plotnových disků zapojených do klasického pole zásobníků přes rozhraní SATA/PCIx. Každý NAS server obsahuje operační systém, nejčastěji některé z forem Linuxu, jehož úkolem jsou bezproblémové procesy s daty. V dnešních moderních NAS serverech zastává operační systém navíc funkci multimediálního prostředí a komunikace mezi uživatelem a virtuálním rozhraním serveru. Komunikaci mezi NAS a jednotlivými koncovými prvky sítě, nejčastěji počítači, zajišťuje protokol TCP/IP. Konkrétně se při komunikaci mezi určitým typem aplikace zajišťující přenos dat po síti a koncovým zařízením používá některý z rodiny protokolů nejvyšší, resp. aplikační vrstvy TCP/IP. Prvním je NFS (Network File System) protokol, který slouží k řízení vzdáleného přístupu k souborům pomocí počítačové LAN sítě. V praxi je pak možné díky NFS protokolu komunikovat se vzdáleným diskem připojeným na server a pracovat s ním stejně jako s diskem v síti LAN. Druhým protokolem je CIFS (Common Internet File System), jehož úkolem je vedení komunikace mezi uživatelem a serverem při žádosti o přístup k sdíleným médiím jako jsou např. tiskárny, sériové porty, externí disky apod. Dalšími síťovými protokoly, které NAS server pro svou komunikaci potřebuje jsou FTP, SFTP, HTTP, POP, SMTP a mnoho jiných. Vzhledem k neustálému vývoji v oblasti datových úložišť nabízejí NAS servery hned několik doplňujících funkcí. Typickou službou je tzv. DLNA server umožňující online streamování multimediálních souborů na jakémkoliv zařízení, které je připojené v síti. Častou možností je také vytvoření web serveru a vlastního cloudového úložiště, které je chráněné přihlašovacími údaji, SSL certifikátem a je přístupné odkudkoliv na světě.

Značnou výhodou technologie NAS je možnost neustálého přístupu všech připojených zařízení k uloženým datům buďto pomocí vzdáleného přístupu přes internet nebo v rámci jedné sítě. Přitom není podstatné, zda jsou nebo nejsou zapnuty všechny osobní počítače připojené do NAS sítě. Další výhody spočívají v nižších pořizovacích nákladech a velikostech oproti velkým datovým serverům, společně s usnadněním a zefektivněním práce s datovými soubory. Díky tomu, že NAS servery neobsahují složité periferie jako tomu je u klasických serverů, disponují jednodušším zabezpečením a menším rizikem výpadku. Opačně existuje i řada nevýhod. Jednou z nich je omezená rychlost zapisování a čtení dat z disků, která je přímo závislá na kvalitě plotnových disků a zároveň na maximální možné rychlosti síťového připojení. Obecně je většina NAS serverů určená pro domácnosti nebo malé podniky, proto při přihlášení a vyřizování požadavků od velkého množství zařízení rychlost ještě více poklesne. Existují však i profesionální NAS servery určené do racků např. od firem QNAP nebo Synology. [15, 16, 17]



Obr. 15: Grafické schéma základní architektury NAS v lokální síti

SAN (Storage Area Network) jedná se o vícečetný navzájem propojený úložný systém, jehož úkolem je zajištění konektivity mezi všemi servery a datovými úložišti v dané dedikované síti a který není nijak přímo připojen k ostatním sítím typu LAN, WAN atp. V praxi se pak jedná o spojení externích úložných zařízení k serverům. Nejčastěji jde o více rozměrná disková pole, elektromagnetické disky nebo optické paměti. Příčinou vzniku sítě SAN byla potřeba zajistit místo pro narůstající požadavky na větší úložné kapacity, zabezpečovací trendy, stabilitu uložených informací a také vytvoření záložních síťových cest. Okruh SAN sítí je v dnešní době často používán jako vysokorychlostní komunikační způsob sdílení dat, nicméně se stále jedná o poměrně nedokonalý a slabý systém, který navíc nezajišťuje plnou schopnost odlišných systémů navzájem spolupracovat. SAN je připojen k standartnímu síťovému rozhraní pomocí klasických komponentů jako jsou L2 switche, routery a Storage routery. Typickým uspořádáním SAN sítě je spojení alespoň dvou serverů k datovým úložištím pomocí minimálně dvou ethernetových či optických switchů. Vzhledem k tomu, že datová úložiště mohou být od sebe vzdáleny desítky i stovky kilometrů, je přenos dat zajištěn díky optickým mnohavidovým nebo jednovidovým datovým kabelům tzv. Fibre Channel. Existuje řada rozdílů a výhod oproti jiným systémům typu NAS, avšak je potřeba tyto systémy odlišit a definovat obě řešení jako možné kooperativní celky. Hlavní výhodou SAN sítí je efektivní využívání paměťové kapacity disků, při které jsou data logicky rozdělena do různých disků na několika místech zároveň tak, aby byly všechny úložiště optimálně zaplněny. Další výhodou je potenciální dynamické zvyšování nebo zmenšování datového prostoru pomocí kaskádování, které garantuje nekonečné přidávání nových disků nebo celých podsítí. Nevýhodou je především vysoká pořizovací cena systému a komunikačních cest, zejména díky technologii optických vláken. [16, 17]



Obr. 16: Grafické schéma architektury SAN sítě pro komunikaci mezi jednotlivými úložišti

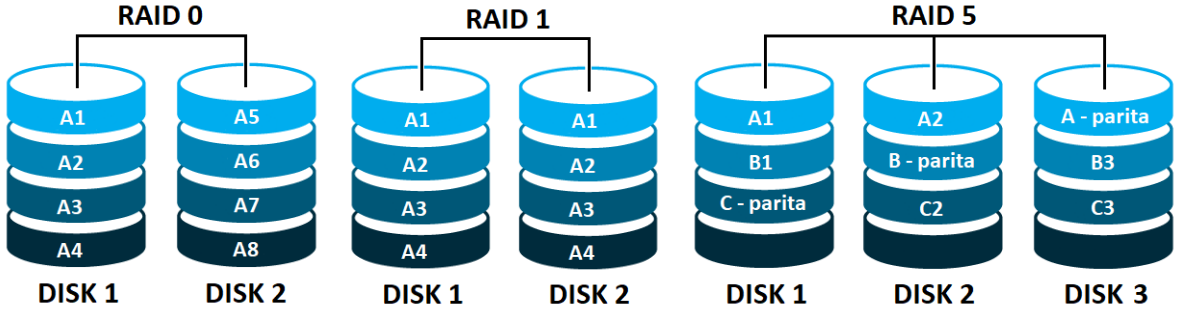
DAS (Direct Attached Storage) je nejjednodušší způsob zálohy informací v síťových úložištích. DAS jsou v podstatě paměťová média, bezprostředně připojená k jednotlivým síťovým zařízením. Může se tak jednat o jednoduché USB flashdisky a externí HDD připojené k počítači nebo složitější disková pole zpravidla opatřena RAID řadiči fungující jako hlavní úložné místo pro servery. Připojení této sítě k serverům je řešeno standartními ethernetovými kabely a rozhraním typu SCSI. Výhodou DAS sítí je jejich jednoduchá administrace a tvorba tzv. datových clusterů. V moderních sítí probíhá správa souborů pomocí webového prostředí. Nevýhodou je rychlost přenosu dat, která závisí na vytížení serveru. [16]

5.3 TECHNOLOGIE DISKOVÝCH POLÍ RAID

RAID (Redundant Array of Independent Disks) v českém překladu se jedná o vícenásobné pole nezávislých disků. Úkolem této metody je dlouhodobé a bezpečné uchovávání dat, které je založené na technologii klasických plotnových disků, které jsou speciálním způsobem uspořádány tak aby při selhání nebo poškození jedné z částí nebyly ztraceny veškeré soubory. Záloha dat je nastavena podle potřeby konkrétního typu RAID režimu, který specifickou formou ukládá soubory na jeden a více nezávislých disků připojených do společné sběrnice PCIx. Při poškození jednoho z disků jsou data uložena na více místech najednou a tím je možné vadný disk vyměnit za nový, na kterém je posléze rekonstruován obsah a chybějící data jsou dopočítána z jiných disků tak, aby systém splňoval kritéria daného RAID označení. Postup ukládání dat je realizován buďto softwarově nebo hardwarově. Při levnějším, softwarovém řešení je obsluha zápisu dat na disk ovládána operačním systémem, který však zbytečně zatěžuje procesor a tím se i snižuje rychlost zápisu a čtení v celém zařízení. Naopak hardwarové řešení využívá speciálních řadičů, které jsou efektivnější a nezatěžují procesor. Velikost bezpečnostní úrovně pro ukládání dat se liší podle toho, jaký je zvolen RAID režim. Nejčastěji se používá RAID 0, RAID 1, RAID 5 nebo 6.

RAID 0 někdy označován také jako Striping nebo JBOD, představuje základní, a tedy i nepřímý úložný systém, jelikož neshromažďuje žádné nadbytečné soubory, které by představovali určitý způsob zabezpečení. Pokud dojde k poškození disku, znamená to nevratnou událost a zároveň i ztrátu informací. Disky jsou zapojeny v sériové logice a každý sektor ukládá rozdílná data. Výsledná kapacita RAID 0 je dána součtem velikostí všech zapojených disků do jedné sběrnice. Spojení mezi jednotlivými disky je uskutečněno dvěma metodami. První metoda je tzv. JBOD nebo také zřetězení, při níž se data ukládají za sebou do té doby, než je zaplněn celý disk. Poté jsou data ukládána na druhý, třetí a další možný disk. Druhou metodou je prokládání, kde jsou data cyklicky a střídavě ukládána na několik disků. [17, 18]

RAID 1 označovaný také jako zrcadlení (mirroring) je efektivní a jednoduchý způsob ochrany uložených dat, využívající principu dvojitého zapisovaní souborů na dva oddělené pevné disky. Během případné poruchy kteréhokoliv z disků je čtení či zapisování automaticky přesunuto na zbývající funkční disk, který obsahuje totožnou kopii původního disku. Poškozený disk lze bez jakýchkoliv problémů vyměnit za nový, na který je následně při iniciaci ihned nahrána kopie obsahu zbylého funkčního disku. Moderní úložné systémy obsahují dva nezávislé hardwarové řadiče, které jsou schopny při výpadku jednoho z nich okamžitě nahradit činnost čtení či zapisování. Tato metoda se nazývá duplexing. Během normální funkčnosti je možné pomocí dvou a více řadičů dosáhnout rychlejšího zpracování dat. Jednou z nevýhod systému RAID 1 je pomalejší zapisování z důvodu dvojnásobného přenosu zapisovaných dat. Dále pak je nutné mít k dispozici sudý počet disků potřebných k procesu zrcadlení což násobí pořizovací náklady úložiště. Výhodou je poměrně vysoká míra zabezpečení dat pro potenciálnímu poruše. [17, 18]



Obr. 17: Ukázka teoretického rozložení uložených dat na dvou (třech) discích v režimu RAID 0, 1 a 5

RAID 5 je již složitější režim ukládání vyžadující minimálně tři diskové jednotky. Z celkové kapacity úložného místa datového serveru, obsazuje jeden celý disk samoopravné tzv. paritní kódy, které jsou střídavě rozdělené v rámci všech připojených disků. Například pokud máme tři disky s maximální kapacitou 2 TB je možné ukládat do výše 4 TB, jelikož zbylé 2 TB jsou využity na samoopravné paritní kódy. Během zápisu jsou data ukládána postupně a parita je rozprostřena do všech disků. Pokud dojde k závadě na některém z disků jsou poškozená nebo ztracená data dopočítána ze zbylých souborů a kontrolních algoritmů. Výhodou režimu RAID 5 je menší zatížení disků z důvodu paralelního přístupu k uloženým souborům. Nevýhodou je naopak pomalejší čtení díky nutnosti výpočtu paritních bitů. [17]

RAID 6 teoreticky navazuje na předchozí metodu ukládání dat s tím rozdílem, že používá dva paritní celky se samoopravnými kódy v rámci každého připojeného disku. Stejně jako tomu je u režimu RAID 5 jsou data ukládána střídavě vždy po určitých částech, a to hlavně kvůli zatížitelnosti paritních údajů na discích. Bezpečnost je zde navýšena odolností proti poškození dvou disků. Z hlediska rychlosti čtení je tento způsob srovnatelný jako u režimu RAID 5 avšak zápis je ještě pomalejší než u předchozího systému, a to zejména díky dvojnásobnému výpočtu paritních celků. Obecně lze RAID 6 vytvořit z alespoň čtyřech disků, nicméně to by znamenalo, že celou polovinu úložného místa zaplní samoopravné kódy. Vzhledem k tomu, že by tato konfigurace byla stejná jako RAID 1, která by byla mnohonásobně levnější, najde své využití až od vyššího počtu zapojených disků, jako jsou průmyslové NAS servery. Existuje i řada dalších variant RAID polí jako jsou vícečetné nebo nestandartní režimy. Typickým příkladem víceúrovňových polí je kombinace dvou diskových celků jako je RAID 0 a 1, ve kterých jsou data ukládána celkem na čtyři disky, přičemž každá dvojice disků tvoří RAID 0. Veškeré soubory jsou zrcadleně proloženy ve dvou logických polích. Výhodou je vyšší rychlost při čtení a zápisu na několik disků zároveň díky rozložení zátěže procesu. Nevýhodou je využití pouze poloviční kapacity pole. [18]

6 BEZDRÁTOVÁ TECHNOLOGIE PRO PŘENOS DAT

Sítě pracující na principech bezdrátového přenosu dat, vytvářejí spojení mezi dvěma subjekty odlišným způsobem, než je tomu např. u metalických tedy kabelových technologií. Existují nicméně i zařízení, která je nutné k bezdrátové síti fyzicky připojit a vytvořit tak připojení s ostatními síťovými prvky. Tato kombinovaná metoda připojení se nazývá hybridní síť. Pro bezdrátový přenos dat se používá několik druhů technologických provedení. Jedním z nich je dnes už zastaralé infračervené záření určené k vysílání informací na krátkou vzdálenost (přibližně jeden metr) a za přímé viditelnosti mezi mobilními a PDA zařízeními, přičemž rychlost přenosu dosahuje maximálních hodnot v jednotkách Mbit/s. Dalším druhem je speciální komunikace využívající laserový paprsek. Ten slouží jako mediátor při přenosu dat mezi pozemními a kosmickými teleskopy. Při ideálních meteorologických podmínkách může rychlost komunikace dosáhnout až 3 GB/s. Nejvyužívanější je však rádiová technologie založená na principu přenosu rádiových vln. Podstatná část rádiových komunikací probíhá na vzdálenost několika stovek metrů až jednotek kilometrů. Důležitým aspektem rádiového přenosu jsou stanovené frekvence, resp. jejich rozsah, který je možný použít. Ten podléhá regulaci a přiděluje jej Český telekomunikační úřad. Značná část vysílacího rozsahu je rezervovaná pro licenční účely jako tomu je u televizních či mobilních sítí. Tato část kapitoly se vymezuje pouze na část nelicencovaného prostoru a tím jsou WiFi sítě, které spadají do rozsahu rádiových vln 2,412-2,484 GHz a 5,150-5,725 GHz. [20, 22]

6.1 VZNIK A VÝVOJ BEZDRÁTOVÉ TECHNOLOGIE Wi-Fi

Historie dnes již nejznámější bezdrátové komunikace se začala psát v 90. letech minulého století konkrétně to bylo 9. května 1985, kdy americký telekomunikační úřad zpřístupnil část rádiového spektra s frekvencí 2,4 GHz pro nekomerční využití bez povinnosti licenčních poplatků. Díky této možnosti byli postupem času vyvinuty také další známé bezdrátové standarty jako je ZigBee, Bluetooth nebo WiMAX, které nepodléhali úředním povolením, pouze dodržovali určité technické specifikace jako je maximální výkon antény atp. Než byl oficiálně představen standard pro sítě Wi-Fi, byla dříve v únoru roku 1980 založena americkou institucí IEEE (Institute of Electrical and Electronics Engineers) nová rodina standardů pro LAN a WAN systémy s názvem IEEE 802 (kde 80 značí rok a 2 měsíc založení). Každé jednotlivé verze ať už metalických nebo bezdrátových protokolů vyvíjeli pracovní skupiny odlišující se koncovým číslem za hlavní verzí 802.x. Vznik a vývoj dobře známého standardu 802.11 neboli Wi-Fi začal v září roku 1990 a první funkční protop byl spuštěn až o sedm let později. Tehdy byla maximální přenosová rychlost pouhé 2 Mb/s a rozsah signálu byl velmi omezený. Nevýhodou byl zastaralý způsob modulace rádiových vln formou FHSS, která spočívá v kontinuálních přeskocích mezi jednotlivými kanály celého pásma a tím pádem zablokovala dalším zařízením přístup do síťové komunikace. Dnes je frekvenční spektrum rozděleno na 13 potenciálních kanálů a používá se komplexnější OFDM modulace.

Velkým průlomem byl rok 1999, kdy byly zároveň představeny dva nové standardy 802.11a a 802.11b. Ty podporovali vyšší rychlost a modernější modulace. První pracoval na frekvenci 5,4 GHz a dokázal přenést až 54 Mb/s což byl tehdy výrazný posun. Druhá varianta nadále podporovala pásmo 2,4 GHz nicméně s rychlostí pouze 11 Mb/s. Další pokrok přišel v roce 2001, tehdy byl uveden standard 802.11g, který již dokázal přenášet data přes 2,4 GHz síť s teoretickou rychlostí 54 Mb/s. Značným pokrokem byl rok 2009, kdy asociace IEEE prezentovala novou, sedm let vyvíjenou verzi 802.11n jejíž hlavním plusem byla kompatibilita jak s pásmem o frekvenci 2,4 GHz tak i 5 GHz. Výhodou byla také

nová metoda vícecestného přenosu zvaného MIMO (Multiple Input Multiple Output). Ta umožňovala efektivnější využití celého frekvenčního pásma tím, že pomocí analogových antén násobila teoretickou rychlost propustnosti. Například zařízení připojené na jeden 20 MHz kanál pomocí jedné antény dosáhlo maximální rychlosti 150 Mb/s ale se čtyřmi anténami se teoretická rychlost mohla zvýšit na 600 Mb/s. Posledním důležitým standardem je 802.11ac uveden na trh v roce 2013. Ten je o něco víc rychlejší a dokáže vysílat i přijímat až na 160 MHz širokém pásmu v osmi svazcích. A jak vlastně vznikl název WiFi? Autorem tohoto názvu je nezisková organizace WECA, která hledala vhodný prodejní název bezdrátové technologie, jelikož pojmenování „802.11b" nebyl tím pravým. Výsledkem byl obchodní název Wi-Fi (Wireless Fidelity) což ve volném překladu znamená bezdrátová věrnost. [21, 22]

6.2 STANDARD IEEE 802.11 A JEHO ZABEZPEČENÍ

Poté co byl v roce 1997 oficiálně představen první standard pro bezdrátovou komunikaci 802.11 se za nedlouho objevila nová norma, která se stala jedním z nejrozšířenějších standardů a také prvním důležitým dodatkem s technologickým vylepšením v rodině WiFi. Tím novým standardem je 802.11b. **IEEE 802.11b** je přesné označení pro tehdejší komerčně používaný standard v bezdrátových sítích. Jde o verzi pracující v pásmu 2,4 GHz, které nepodléhá licenčním požadavkům. V České republice je toto pásmo možné používat od roku 2000, kdy jej ČTÚ poprvé uvolnil pro nekomerční účely. Zařízení připojené na síť 802.11b má dispozici teoretických 13 kanálů v rozmezí od 2,412 GHz až do 2,472 což vytváří 5 MHz rozestupy mezi kanály. Nevýhodou je fakt, že každý kanál dosahuje maximální šířky 20 MHz, čímž se výrazně zmenší počet nepřekrývajících (nerušených) se kanálů na tři. Standard 802.11b také definuje přenosovou rychlost na 11 Mb/s. K přenosu informací vzduchem je použita modernější DSSS (Direct Sequence Spread Spectrum) modulace, která do modulačního signálu aplikuje kódování matematického charakteru. Přenášený signál je tak rozložen do širšího spektra a informační signály jsou posílány v menších souborech, tím je zaručen bezpečnější přenos dat k cíli. Při zhoršení kvality signálu je přenosová rychlost automaticky snížena na 5,5 nebo 1 Mb/s. Ve volném prostranství je možné signál přenášet až na vzdálenost 12 km. Zajímavostí je způsob, jakým byl standard 802.11b rozšířen. Prvním zařízením, které zpopularizovalo WiFi, resp. standard 802.11b byl Access point Air-port od firmy Apple z roku 1999, který obsahoval ethernetovou kartu i možnost bezdrátového připojení. [21, 22]

Druhá a zároveň navazující je norma **IEEE 802.11a**. Ta byla schválena brzy po nástupu verze „b" a je schopná vysílat na frekvenčním pásmu 5 GHz s přenosovou rychlostí až 54 Mb/s, což je oproti předchozí verzi citelný nárůst. Zařízení podporující tuto normu se začala na trhu objevovat v pozdějším období, přibližně okolo roku 2002, na rozdíl od standardu 802.11b. Novou stránkou „áčkové" verze bylo přesunutí pásma do užitečnějšího spektra, které tehdy ještě nebylo tolik zaplněné jako pásmo 2,4 GHz. Navíc poskytovalo mnohem více otevřených kanálů pro bezdrátové vysílání. Nevýhodou se může zdát zpětná nekompatibilita se standardem 802.11b, tedy pokud dvě rozdílné zařízení nepodporovali stejné standardy nebylo možné mezi sebou navzájem komunikovat. Většina dnešních zařízení sice podporuje obě verze, nicméně ty se zahrnují pouze pro účely připojení starších systémů, které jsou dnes na ústupu.

S postupem času vznikaly další nové vyspělejší standardy. Příkladem je třetí nejstarší standard **IEEE 802.11g.** Vznikl v roce 2003 v návaznosti na předchozí úspěšnou verzi „b". Mohl tak nabídnout výrazně vyšší teoretickou přenosovou rychlost 54 Mb/s v pásmu 2,4 GHz a modulaci signálu formou vyspělejší technologie OFDM. Smyslem nového standardu bylo vytvoření jedné komplexní normy, která by byla schopna pracovat se všemi staršími verzemi z rodiny 802.11. Pokud ale v síti „g" je pouze

zařízení umožňující používat standard 802.11b je bandwidth sítě snížen na velikost nejvyššího možného přenosu příslušné normy. V komerční sféře se od roku 2003 začaly objevovat síťové prvky s označením „Tri-Bend“, ty byly schopné fungovat na všech dostupných standardech. Existují však i nevýhody, které vycházejí ze zaneprázdněnosti 2,4 GHz jinými technologiemi jako jsou Bluetooth, bezdrátové VoIP telefony nebo RC modely. Tím vzniká velké rušení celého spektra pásma a omezení přenosové rychlosti. Řešení poskytují tři vyhrazená pásma, která se nijak nepřekrývají a jsou rozdělené po 25 MHz. [22]

Posledním značně rozšířeným standardem mezi uživateli síťových zařízení je **IEEE 802.11n**. Hlavním důvodem pro vývoj dalšího standardu na poli síťových přenosů bylo razantní zvýšení rychlosti až na maximální teoretickou hranici 600 Mb/s. Doposud se však v praxi používá rychlost přibližně 300 Mb/s. První náznaky nové verze síťového protokolu se objevily ještě před oficiálním spuštěním verze „n“ a to v roce 2007, tehdy to byly první zařízení s označením Draft N, které tuto funkci podporovali. Až v roce 2009 byla uvolněna plná verze standardu 802.11n. Ten navíc mohl pracovat jak v pásmu 2,4 GHz tak 5 GHz. Výhodou 5 GHz pásma byla vyšší přenosová rychlost za cenu kratší vysílací vzdálenosti oproti 2,4 GHz síti. Zásadním argumentem, proč nový standard nabízí tak výrazné zvýšení přenosové rychlosti spočívá v technologii MIMO, ta spolu s OFDM modulací zefektivňuje bezdrátové přenosy pomocí zvýšení výkonnosti vyzařovaného signálu díky většímu počtu připojených antén (zpravidla tři a více). Existuje řada dalších standardů z rodiny 802.11 (více než 20) avšak ty nejsou až tak populární nebo byly staženy z funkce. Některé z nich jsou rezervované pro budoucí použití. [22]

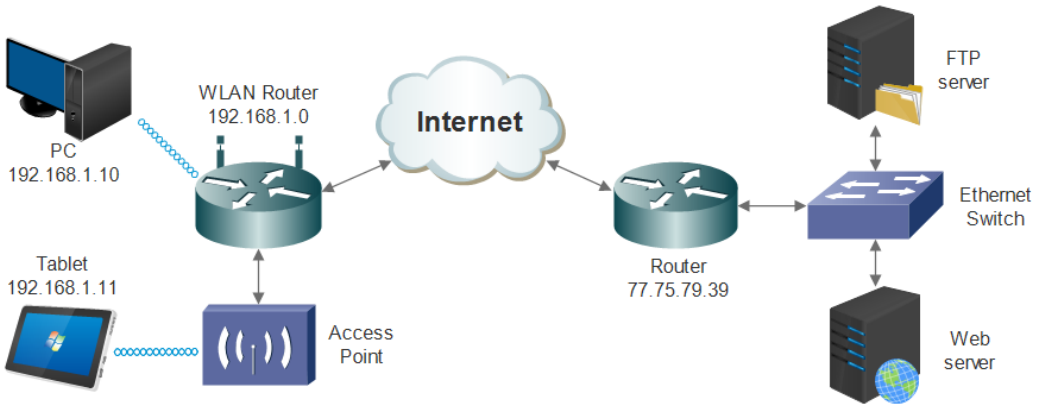
Otázka zabezpečení sítí hraje během bezdrátové komunikace mezi dvěma zařízeními důležitou roli. Vyplývá to z faktu, že informace jsou přenášeny nezabezpečeným médiem (vzduchem), který není možné nijak vymezit. Kvalita zajištění bezdrátového přenosu spočívá ve dvou hlavních aspektech. Těmi je autentizace oprávněné osoby přistupovat do sítě a šifrování posílaných informací. Jedním z mnoha typů zabezpečení v autentizační fázi je zablokování vysílání SSID, což je způsob skrytí broadcastem vysílaný název bezdrátové sítě. Dalším typem je kontrola fyzických MAC adres během připojování se k přístupovému bodu. Zařízení, ke kterému se chce klient připojit obsahuje tabulku tzv. whitelist s MAC adresami, kterým je povolen přístup do sítě. Ostatní zařízení, které nejsou registrovány v tabulce jsou během připojování odmítnuty. Na podobném principu funguje blokace IP adres síťových karet. [21]

V rámci šifrování síťové komunikace existují tři základní doplňky, které brání data před odposloucháváním. Prvním a zároveň nejméně bezpečným (informace zle odposlechnout) je šifra WEP. Ta obsahuje symetrické kódy, které jsou manuálně nastaveny na zdrojových a cílových zařízeních, výlučně pomocí těchto šifrovaných kódů je možné bezdrátový přenos uskutečnit. Modernějším způsobem je šifrování pomocí WPA. Tato funkce dynamicky a v přesném časovém rozmezí mění WEP klíče s dostatečně dlouhým heslem. Není tedy možné vědět nebo odhadnou jak a kdy se šifra změní. Výhodou WPA je zpětné použití u starších zařízení podporující pouze WEP. Posledním a také nejčastěji se vyskytujícím bezpečnostním prvkem je WPA2. Toto zabezpečení aplikuje kvalitnější šifru AES, což je 128, 192 nebo 256bitový symetrický, propracovaný a velice výkonný klíč vycházející z 56 bitové šifry DES. Zatím není známý případ plnohodnotného prolomení, a proto je stále používána v rámci síťových prvků jako jsou např. WiFi routery. Nevýhodou WPA2 je nutnost implementace do zařízení s vyšším výpočetním výkonem. Všechny výše zmíněné zabezpečovací metody se týkají pouze fyzické vrstvy sítě. Tu však lze prolomit. Další techniky autentizace a šifrování dat mohou probíhat na nejvyšší, aplikační vrstvě TCP/IP. Typickým příkladem jsou technologie jako SSL, SSH, PGP a GnuPG. [20]

6.3 ZÁKLADNÍ POJMY A SÍŤOVÉ PRVKY VZTAHUJÍCÍ SE K Wi-Fi

V zásadě je možné bezdrátové sítě rozdělit do dvou hlavních kategorií. První je infrastrukturní bezdrátová síť. Je to klasický případ veřejně používaného způsobu komunikace a přeposílání informací. V infrastrukturní sítí existuje jeden nebo hned několik centrálních uzlů, jejichž úkolem je řízení a správa komunikačních procesů. Na tyto uzly jsou dále větvené další sítě a podsítě typu MAN a LAN až k jednotlivým koncovým zařízením. Opakem je tzv. síť ad-hoc neboli WANET. Jde o decentralizovaný systém, který není nijak organizován a všechny zařízení v této síti jsou si rovny. Neexistují tak některé řídící stanice jako je tomu u sítí LTE, GSM nebo 4G. V rámci těchto systémů jsou uskutečňovány pouze dočasné peer-to-peer komunikace, kde každé zařízení má stejná práva přistupovat k bezdrátovému vysílání. Zmíněný způsob se používá při síťové konektivitě, kterou lze provozovat pouze na velmi malé vzdálenosti všech zařízení. Výhodou je rychlé zprovoznění a minimální konfigurační nároky. [22]

Pro úspěšnou iniciaci a udržení bezdrátové komunikace je nutné implementovat důležité síťové prvky. Na trhu se vyskytuje nespočetné množství vysílacích a přepínacích zařízení, které řídí či směřují tok dat ze zdrojové adresy na cílové místo. Jedním z nich je **Router** (ve Wi-Fi sítích WLAN Router). Jde o aktivní druh síťového zařízení pracující na třetí tedy síťové vrstvě protokolu TCP/IP. Jeho hlavním úkolem je oddělení jednotlivých sítí a tzv. routování neboli přeposílání datových paketů na základě speciální tabulky, která obsahuje IP adresy ostatních routerů a podle nich určuje optimální cestu k cíli. Existuje více typů routerů podle toho, k jakým účelům jsou určené. Největší zařízení se mohou podobat ústřednovým serverů, které se umísťují do rackových skříní a slouží k propojení velkého množství páteřních sítí. Známější jsou však malé domácí routery vybavené multi-portovým switchem, portem pro WAN síť a anténními vysílači. V takovém případě se již jedná o WLAN routeru, který v sobě kombinuje AP (Access Point), router a klasický ethernetový switch. Výhodou je možnost kombinace ethernetového a bezdrátového připojení. **Access Point** (přístupový bod) je síťové zařízení zapojené v infrastrukturním režimu, jehož hlavním úkolem je vysílat a přijímat signály z jednoho nebo více koncových prvků. Takový typ AP se nazývá point-to-multipoint a dokáže přijímat a zároveň vysílat signály na více zařízení najednou. Nejedná se routovací systém, ale pouze zprostředkovává bezdrátovou komunikaci. Typicky obsahuje jeden vstupní a jeden výstupní port pro další zapojení. Pro správný přenos dat po síti jsou také potřebné zařízení typu Switch nebo Hub. **Switch** je aktivní síťový prvek sloužící k přepínání datových toků a propojování podsítí s hvězdicovou typologií. Jeho úkolem je přesměrovávat síťový provoz pouze na zařízení, které jsou oprávněné určitá data přijmout. Opakem je **Hub**. Ten všechna data na vstupu přeposílá na ostatní připojené zařízení a chová se jako opakovač signálu. [22]



Obr. 18: WLAN síť připojená k internetu a klasické ethernetové spojení se servery.

7 IDENTIFIKACE OSOB VE ZDRAVOTNICKÉM ZAŘÍZENÍ

Problematika bezpečnosti a identifikace pacientů ve zdravotnickém zařízení je čím dál tím větší zájmovou oblastí, která je diskutována jak na poli jednotlivých poskytovatelů zdravotní péče, tak i na vyšších orgánech např. ministerstvo zdravotnictví, Rada EU nebo také Světová zdravotnická organizace. Identita každého pacienta je odlišná od ostatních osob pohybujících se v jeho prostředí. Ke správné identifikaci je zapotřebí několika méně či více unikátních znaků, které tuto odlišnost zaručují. Typickým příkladem tak může být jméno a příjmení pacienta, rodně číslo, krevní skupina, fotografie nebo určitý druh biometrické informace. Účelem všech identifikačních systémů je zajištění co nejmenší chybovosti a záměny identity pacienta během procesních úkonů v rámci rutinních činností zdravotního personálu. Obecně lze identifikační systémy ve zdravotnických zařízeních rozdělit na tři základní úrovně, kde každá z nich zaujímá různý pohled na zabezpečení, prezentací informací a technické provedení systému. První a také nejjednodušší formou identifikace pacienta je použití pasivní formy zápěstního náramku. Na druhé úrovni je již použita modernější metoda náramku s pomocí vestavěných RFID čipů nebo pásků s čárovým kódem. Poslední část tvoří aktivní identifikační prvky připojené na nemocniční informační systém. V tomto případě se jedná o finančně a technicky náročné vybavení, které se objevuje spíše ve vyspělých zahraničních státech. Detailní rozbor identifikačních náramků bude vysvětlen v kapitole 7.3.

7.1 PROČ A JAK IDENTIFIKOVAT PACIENTY

Z obecného hlediska je nedostatečná bezpečnost pacienta a zároveň minimální informovanost zdravotního personálu závažným pochybením jak pro veřejné zdraví, tak i pro hospodářskou činnost poskytovatele zdravotnické péče. Z veřejně dostupných statistických modelů je zřejmé, že v určitých případech dochází ke zvýšení přítomnosti nežádoucích událostí ve spojení s poskytováním zdravotní a sociální péče. Tento fakt nutí vedení nemocnic a ministerstva zdravotnictví zamyslet se možností úpravy stávajících bezpečnostních postupů nebo zavedení modernějších a pro pacienta spolehlivějších technik identifikace. Podstatnou skutečností je možnost těmto potenciálně nežádoucím vlivům čelit, jelikož se ve většině případů jedná o chyby způsobené systémovými okolnostmi. S postupným zvyšováním počtu poskytovaných zdravotnických služeb byly Radou EU pro sociální politiku, zdraví a ochranu pacienta spolu s Ministerstvem zdravotnictví ČR představeny dokumenty a metodiky týkající se doporučení o bezpečném zacházení s pacientem (dokument 2009/C 151/01 a metodika MZDR 54595/2009). [23]

Jedním z hlavních důvodů, proč správně identifikovat osoby v nemocnicích a jiných zařízeních je nárůst počtu nežádoucích událostí, které se týkají 8 až 12 % všech hospitalizovaných pacientů. Těmito důvody bývají především chybné podání léčiv např. nesprávná dávka, záměna typu léčiva nebo podání léku jinému pacientovi, než pro kterého byl původně určen. Jistou míru pochybení zastávají i určité diagnostické či terapeutické výkony, které jsou provedeny na nesprávném pacientovi. Dalším rizikem je záměna novorozence bezprostředně po porodu, případně při dalším ošetřování. Výjimečný je případ transfúze krve jinému pacientovi. Určitým smyslem pacientských identifikačních prvků je omezení rizika neočekávaného opuštění nemocničního oddělení nebo celého zařízení. Zavedením optimálních bezpečnostně preventivních opatření pro identifikaci pacientů hospitalizovaných ve zdravotnických zařízeních nebo klientů využívající sociální služby pomocí identifikačních prvků snižuje celkový počet nežádoucích událostí a zvyšuje bezpečnost pacientů. Je důležité se orientovat na rozvoj informačních zdrojů směrem k pacientovi a zintenzivnit vzdělávání zdravotnických pracovníků. [23, 24, 28]

Primární proces během zavádění identifikačního systému do praxe podléhá několika krokům a doporučením, které vydává Ministerstvo zdravotnictví, nicméně je na každé nemocnici, jakou metodiku zvolí. V rámci úvodního procesu je důležité se zaměřit na dvě oblasti. Jednou z nich je volba vhodného typu produktu, který by měl splňovat jak materiálové požadavky, tak i finanční dostupnost. Identifikační prvek musí být pevný, voděodolný, rozměrově vhodný, dezinfikovatelný a schopen zaznamenávat údaje o pacientovi (tyto charakteristiky se přisuzují především páskovým náramkům). V druhé fázi je zásadní získání pochopení od personálu, pacientů a jejich příbuzných. Pro správnou funkčnost je nezbytné, aby byl navržený identifikační prvek logicky sestavený a zajišťoval jednoznačnou identitu pacienta. S tím souvisí pozitivní snaha personálu začlenit tento prvek do běžné pracovní činnosti. Podobné pochopení musí být i na straně pacientů. Tím je myšleno jejich minimální fyzické i psychické zatížení. V poslední řadě je nezbytné klást důraz na vzájemnou podporu bezpečného poskytování zdravotní péče ať už s pomocí samotného zdravotnického personálu či mediální informovanosti. Personál nemocnic je nutné vzdělávat a informovat o metodických postupech, kterými jsou: manipulace s identifikačním prvkem, jeho umístěním, zápisem důležitých údajů ke konkrétní osobě a princip kontroly pacientů. [23, 28]

7.2 IDENTIFIKAČNÍ NÁRAMKY

Identifikační náramky jsou v dnešní době nejvíce zastoupeným prvkem při autentizaci pacientů ve zdravotnických zařízeních. K úspěšné pozitivní identifikací je potřeba alespoň dvou rozdílných faktorů, které jsou schopné nezávisle na sobě určit přesnou identitu pacienta. V zásadě se primárně používá verbální kontrola, při které je pacient dotázán zdravotním personálem na své jméno a příjmení eventuálně jiné údaje jako je rodné číslo nebo trvalé bydliště. Tato okolnost však není postačující pro identifikaci. Teprve ve druhém kroku je pacient ztotožněn se svým identifikačním náramkem, na němž se musí napsané (resp. vytištěné) osobní údaje shodovat s těmi verbálními. V určitých případech jako jsou pooperační stavy, kóma aj. není možné provézt verbální identifikaci pacienta, proto se náramek stává logicky jediným prvkem k identifikaci pacienta. Za velkou chybu se považují informace, které slouží pouze jako jediný možný identifikátor. Typickým příkladem jsou cedule umístěné nad lůžkem nebo číselné štítky pokojů a lůžek ve spojení s místem hospitalizace pacienta případně označení dle stanovené diagnózy. Náramky je možné rozdělit na pomyslné dvě kategorie, a to podle způsobu použití, tedy pro jaký účel jsou vybrány a podle technického zpracování náramku. Škála uplatnění náramků je velice rozmanitá. Nejčastěji se lze s náramkovou identifikací setkat v nemocnicích, poliklinikách, porodnicích, soukromých klinikách, lázních, rehabilitačních centrech nebo třeba v laboratořích. Už ne tak časté je používání náramků záchrannými službami nebo ambulancemi. [23, 24]

Obr. 19 a 20: Příklad identifikačního náramku s možností čtení pacientských dat z čárového kódu

V rámci nemocničních zařízení a poliklinik je zřejmé, že identifikační náramky přímo souvisí s cíli a metodikami bezproblémové péče ve zdravotnictví. Velkou výhodou identifikačních náramků je fakt, že svou existencí nijak nenarušují interní systémy a rutinní činnosti nemocnic a zároveň mohou samostatně plnit cíl bezpečného zacházení s pacientem. Mezi některé další výhody patří jejich pomoc k nadstandardnímu zabezpečení pacienta a usnadnění administrativní činnosti lékařů, sester a veškerého zdravotnického personálu. V porodnicích náramky vytvářejí spojení mezi matkou a novorozencem, tedy veškeré vzájemné osobní údaje matky, resp. novorozence a identifikační čísla s čárovými kódy jsou shodné. V každé sadě se nachází vždy jeden malý náramek pro dítě a jeden nebo i více velkých náramků pro matku případně další osoby. Ostatní zdravotnické zařízení jako jsou rehabilitační a lázeňská centra používají náramky pro zabezpečení správné medikace včetně poskytnutí korektní naordinované péče. Náramek obsahuje základní informace, které jsou nezbytné pro pobyt pacienta, např. typ stravování nebo druhy léčebných procedur. Podle technického zpracování se náramky dělí na tři části. První část tvoří základní papírové nebo PVC náramky opatřené patentovou plombou, na které jsou ručně dopsány důležité identifikační prvky např. jméno, příjmení, dané oddělení, alergie a typ léčby. Některé mohou být také barevně odlišeny, přičemž každá barva specifikuje rozdílná rizika pacienta jako jsou poruchy kožní integrity, rizika pádu nebo nutrice. Druhou částí jsou již moderní náramky viz. obr. 19, které nejenže obsahují základní osobní informace, ale navíc i jednoduchý čárový kód. Při jeho přečtení příslušným čtecím zařízením je možné zobrazit detailní popis pacienta včetně jeho ordinované léčby a medikamentů. Nevýhodou je vysoká pořizovací cena čtečky čárových kódů, zobrazovacího modulu a tiskárny náramků. Posledním a zároveň nejvíce sofistikovaným typem jsou tzv. čipové RFID (Radio Frequency Identification) náramky. Jejich předností je vetší kapacita paměti pro potenciální informace uložené na čipu implantovaném v náramku a téměř nulová chybovost při čtení a zapisování dat. Další využití spočívá v tzv. Trackingu. Tato metoda slouží ke kontrole pohybu pacienta v areálu nemocnice. Ulehčuje tak hledání dezorientovaného pacienta nebo monitoruje čekací doby před vyšetřením. [23]

<u>*Pro koho jsou identifikační metody určené*</u>:

- Pacienti pod vlivem farmakologických látek (analgosedace, umělá plicní ventilace)
- Pacienti s kvalitativní i kvantitativní poruchou vědomí nebo kognitivním deficitem
- Pacienti pod vlivem celkové anestézie (není možná verbální identifikace)
- Novorozenci a dětští pacienti (zabránění záměny či pochybení při poskytování zdravotní péče)
- Ostatní pacienti, u kterých není možné identifikaci ověřit dotazem (jazyková a smyslová bariéra)

7.3 OCHRANA OSOBNÍCH ÚDAJŮ VE ZDRAVOTNICTVÍ

Oblast poskytování zdravotnické péče a zdravotnického práva je jednou z nejvíce hlídaných a kontrolovaných odvětví z hlediska dodržování zákonů, norem a nařízení jak ministerstva zdravotnictví ČR, tak i Rady evropské unie a dnes už také Evropského parlamentu. Korektní respektování ochrany osobních údajů je dáno kompilací hned několika právních norem různé váhy. Klíčovou je pro Českou republiku mezinárodní smlouva týkající se lidských práv ve zdravotnictví tzv. *Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny*. Důležitý je především článek 10, který definuje ochranu na soukromí a právo každého pacienta být v plném rozsahu informován o stavu vlastního zdraví. Existuje i řada dalších mezinárodní dokumentů schválených Radou Evropy jako je *Úmluva o ochraně lidských práv a základních svobod*. V tomto případě je důležitý článek 8, který poukazuje na respektovaní rodinného a soukromého života. Pro domácí politiku je ukotvený zákon 101/2000 Sb. jehož cílem je ochrana osobních a citlivých údajů. Na činnost zdravotnické péče se

vztahuje § 5, který říká že nakládání s osobními údaji musí být v souladu se souhlasem příslušné osoby, nicméně zde existují určité výjimky právě pro možnost zpracování zdravotnické dokumentace bez jejího souhlasu, pokud se jedná o životně důležité zájmy. Nakládat s těmito údaji může dle § 4 pouze správce, kterým je výhradně poskytovatel zdravotních služeb. Důležitou částí je především § 9, který podrobně vymezuje, pro jaké účely je možné se zdravotnickou dokumentací obsahující informace o zdravotním stavu pacienta nakládat a zpracovávat. Jde o případy ochrany veřejného zdraví, zdravotního pojištění a výkonu státní správy pro oblast zdravotnictví. Na zákon 101/2000 Sb. navazuje občanský zákoník (89/2012 Sb.), ve kterém jsou opět stanoveny pravidla pro nahlížení a nakládání se zdravotnickou dokumentací. Jako příklad se uvádí § 109, podle něhož má každý pacient právo na posouzení jeho zdravotního stavu a dokumentace jiným nezávislým lékařem. Paragrafy 2647 až 2650 uvádí, že osobní informace od pacientů není možné použít ve statistických ani vědeckých pracích a je nutné tyto pacienty vždy uvádět jako anonymní případy. Poslední částí je zákon o zdravotních službách 372/2011 Sb., který v § 65 řeší jakým způsobem bude zdravotnická dokumentace ukládána a kdo k nim může mít přístup.

Stále častěji se mluví o obecném nařízení na ochranu osobních údajů tzv. GDPR (General Data Projection Regulation) jehož platnost by měla ve všech státech EU začít od 25. května 2018. Jedná se o nařízení Evropského parlamentu a Rady 2016/679, představující dosud nejucelenější soubor pravidel na ochranu osobních dat. V ČR má nahradit dosavadní právní úpravu, kterou je zákon 101/2000 Sb. GDPR přináší jak změny v povinnostech správce osobních údajů, tak i v právech osob poskytující tyto údaje. Nově bude nutné získat souhlas ošetřované osoby s uložením a zpracováním jejich údajů. Dále bude za potřebí omezit rozsah uchovávaných údajů o pacientech a zároveň stanovit přesnou dobu archivovaných a zpracovávaných dat. S tím souvisí určení konkrétních osob, které budou moci tyto informace editovat a v jakém rozsahu. Pacient bude mít větší práva nahlížet do svých zdravotnických dokumentací. Tento fakt pacientovi umožní podávat žádosti o kompletní výpisy uskutečněných činností během zpracování osobních údajů, tedy kdo, kdy a jakým způsobem s nimi nakládal. Další novinkou je povinnost správce zdravotnických služeb srozumitelně pacienta informovat o tom, že došlo k narušení správy osobních dat a v jakém rozsahu. Existuje celá řada dalších nařízení, tato však jsou nejdůležitější. [23, 25]

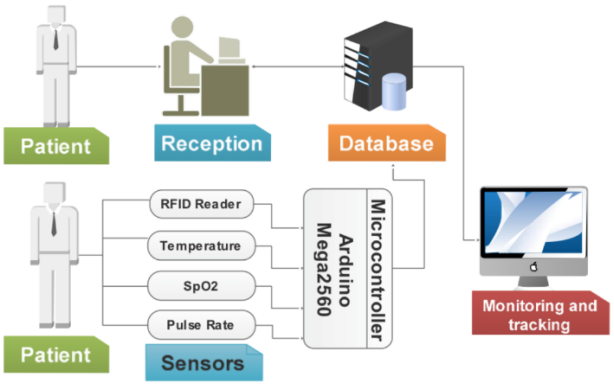
7.4 OSTATNÍ IDENTIFIKAČNÍ METODY

Integrace komplexnějších identifikačních systémů a zařízení je prováděna častěji ve vyspělých západních státech a v oblastech východní Asie, než je tomu v České republice, kde se pacienti setkávají s jednoduchými identifikačními náramky. Tato skutečnost je zapříčiněna mnohonásobně vyšším počtem hospitalizovaných pacientů, obsazeností nemocnic, moderním vývojem a důrazem na bezpečí. Jedním z mnoha případů je nemocnice v Taipei, která disponuje 1084 lůžky a každý den je v ní ošetřeno 5000 nově příchozích pacientů. V posledních několika letech se potýkala s nedostatečnou papírovou metodou pro záznam základních denních informací o stavu pacienta. Úkolem bylo rozšíření staničního systému sester, zavedení elektronických zdravotních záznamů, snížení chybovosti a celkové zlepšení efektivity práce. Výsledkem byl mobilní nemocniční asistent ICEFIRE 2 od společnosti IEI. Jde o plnohodnotný přenosný počítač ve formě tabletu opatřený mnoha doplňujícími periferiemi potřebnými pro správu nemocničního informačního systému. Je vybaven procesorem Intel Atom 1,86 GHz, operační pamětí 4 GB DDR3 SDRAM, paměťovým úložištěm 8 GB mSATA, komunikačním rozhraním WiFi, Bluetooth, USB a GbE LAN. Z uživatelského hlediska obsahuje dvě kamery pro čtení lineárních a dvourozměrných čárových QR kódů z identifikačních pásků pacienta nebo z obalů medikamentů. Doplňující funkcí je technologie RFID, která je v prostředí nemocnice využívána k monitorování pohybu pacientů, sledování

zdravotních nástrojů a dodávek, lokalizaci personálu, sledování krevních vzorků a k zamezení výroby falešných léků. Pro ovládání je k dispozici 10,4 palcový kapacitní dotykový displej, který podporuje jednoduché psaní dotykem prstu ale také detailní psaní pomocí speciálního rezonančního pera. Celkové prostředí přístroje vytváří operační systém Embedded Windows 7 P a doplňující aplikace pro podporu rozpoznávání ručních zápisů a správu pacientských dat. Hlavní výhodou tohoto přístroje je díky velkému množství doplňujících funkcí všestranné využití v rámci nemocničního informačního systému a správu pacientských záznamů. Další předností je také snadná manipulace a přenositelnost. [26]

Obr. 21: Mobilní nemocniční asistent Icefire 2 pro správu zdravotnického informačního systému

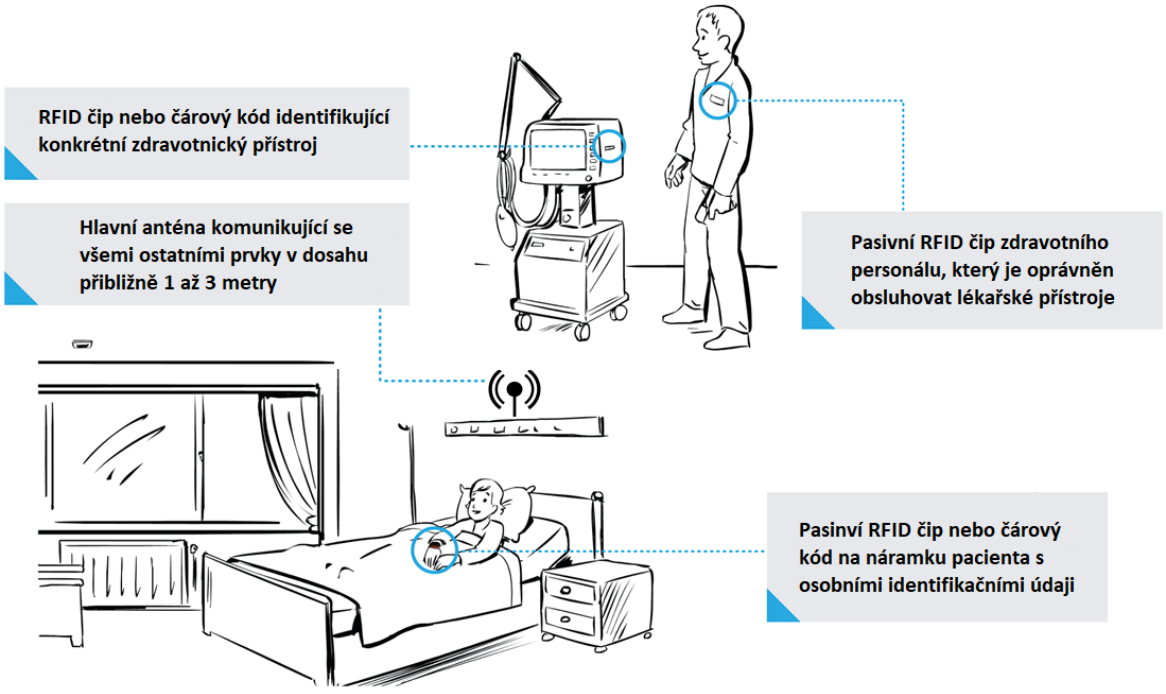
Druhým příkladem je nekomerční identifikační a monitorovací systém publikovaný na vědecké konferenci biomedicínského inženýrství IEEE EMBS v roce 2016. Zabývá se správou a monitorováním základních životních funkcí pacienta. Jde o velice propracovanou komplexní strukturu několika dílčích senzorů a řídících obvodů, které mají za úkol snímat, zpracovávat a přeposílat osobní a zdravotní data o pacientovi. Podstatou této metody je identifikování pacienta a následně korektní přiřazení snímaných dat základních životních funkcí ke konkrétnímu ID. Zásadním prvkem systému je mikrokontrolér, který má za úkol identifikovat pacienta vždy, kdy je zahájeno monitorování fyziologických signálů. Samotná identifikace je pak prováděna pomocí pasivního RFID čipu fyzicky umístěném na kontrolním náramku každého pacienta. Poté co je úspěšně nalezena identita pacienta může probíhat detekce nasycení krve kyslíkem, tepové frekvence a teploty. Důležitou součástí každého biometrického systému je registrace a uložení osobních údajů. Ne jinak tomu je i v tomto případě, avšak zde jsou data uložena na databázový server. Komunikace mezi samotným zařízením, databází a pacientským monitorem probíhá pomocí bezdrátového RN-XV modulu podporující standard 802.15.4. Operační program využívá hned několika dotazovacích a skriptovacích jazyků pro sdílení a zobrazování dat jako jsou SQL, HTML, PHP, CSS aj.



Obr. 22: Zjednodušený princip identifikačního a monitorovacího systému

Naměřená data jsou průběžně ukládána do tabulek vázaných k pacientovým údajům, které jsou spojené se snímáním. Výsledkem je interaktivní online monitor vytvořený ve webové aplikaci Microsoft Power BI, která je schopna zobrazit různé typy grafů, naměřené hodnoty signálů a identifikační údaje potřebné ke kontrole zdravotního stavu pacienta. Tento příklad řešení nemá zastávat primární funkci identifikačního procesu ale upozornit na možnost bezpečného snímání fyziologických dat a dlouhodobě hodnotit vývoj zdravotního stavu pacienta se vzájemnou pomocí moderních identifikačních metod. [27]

Poslední praktická ukázka využití moderních technologií ve zdravotnictví se zabývá efektivním identifikováním pacienta spolu s označením všech aktuálně připojených lékařských přístrojů, jež jsou v přímém dosahu lékařského lůžka. Cílem této vědecké studie bylo vytvořit jednotný a automatizovaný systém identifikace pacienta spolu se správou osobních a fyziologických informací, který by vyloučil chybovost zdravotního personálu při manipulaci s přístroji a naordinovaným dávkováním léčiv. Ve výsledku se úspěšně osvědčilo použití jedné hlavní vysílací i přijímací RFID antény umístěné nad hlavou pacienta přibližně ve výšce jednoho metru. V prostoru bezprostřední blízkosti pacientova lůžka je vytvořena pomyslná signálová obálka, která slouží pro detekci všech přítomných zařízení a zdravotních zaměstnanců. Tyto přístroje jsou opatřeny tzv. odpovídačem (pasivní radiofrekvenční anténa), který je schopen reagovat a komunikovat s hlavní vysílací RFID anténou. Systém tak může poměrně detailně určit jaké typy přístrojů jsou připojené k pacientovy a kdo jej aktuálně spravuje. Výjimkou nejsou ani soustavy alarmů signalizující neoprávněný zásah do přístrojů nebo chybné podání léků. Doplňující technikou jsou již dobře známé čtečky čárových kódů, které mohou posloužit jako záložní metoda pro kontrolu pacienta, přístrojů a léčiv. Jakmile systém automaticky identifikuje všechny součásti na lůžku pacienta nebo v bezprostřední blízkosti radiofrekvenčního pole antény, potvrdí se vzájemné spojení a průběh hospitalizace či jeho obnovení může bezpečně pokračovat. Bez tohoto ověření je zdravotnímu personálu aktivně signalizováno narušení zdravotnické péče. Tato signalizace je realizována pomocí monitorů umístěných na sesternách jednotek intenzivní péče nebo ručních přenosných tabletů, které se přikládají na čelní stranu lůžka. [29]



Obr. 23: Ukázka identifikačního systému využívající technologii aktivních a pasivních RFID čipů

PRAKTICKÁ ČÁST

8 TEORETICKÝ NÁVRH IDENTIFIKAČNÍHO SYSTÉMU

Klíčovými charakteristikami pro optimální sestrojení návrhu na vestavěný biometrický systém pro identifikaci osob ve zdravotnickém zařízení, spolu s jeho softwarovým vybavením a uživatelskou aplikací, jsou jednoznačně definující požadavky na přesnost, spolehlivost, kompaktnost, přenosnost nebo také výdrž. Při zdokonalování existujících nebo vytváření nových metod pro kontrolu pacientů je důležité porovnat současná technická řešení a případně určit jejich nedostatky. Bez tohoto hodnocení není možné vytvořit přesnější, modernější a pro pacienta bezpečnější identifikační systém. V současné době jsou na různých částech kontinentů uplatňovány odlišné metody identifikace, je to především dáno vzdělaností a mentalitou obyvatelstva, politickým vedením zdravotnictví nebo i technickou vybaveností nemocničních zařízení. V Českých nemocnicích jsou již delší dobu zavedeny jednoduché identifikační náramky s ručně psanými osobními údaji každého pacienta. V některých specializovaných centrech je možné se setkat s náramky doplněnými o čárový nebo QR kód, ve kterém jsou všechny důležité údaje uloženy. Tento moderní typ kontroly pacientů je však stále jen otázkou několika vybraných pracovišť.

Ve své praktické části diplomové práce se zabývám návrhem, tvorbou a testováním nového typu vestavěného systému uzpůsobeného k přímé identifikaci pacientů ve zdravotnickém zařízení. Hlavní myšlenkou bylo spojení užitečných informací, z dnes již zavedených biometrických metod a moderních technologií potřebných k sestavení a provozu systému. Každé podobné zařízení musí být upraveno dle budoucího místa použití a způsobu jakým se daná identifikace bude provádět. Mé zařízení a doplňující software včetně uživatelské aplikace je navrhován pro konkrétní začlenění do běžného denního provozu nemocničního oddělení. Hlavní částí spektra koncepcí pro vývoj identifikačního zařízení bylo vytvoření co možná nejjednoduššího ale zároveň pro pacienta nejbezpečnějšího systému, který by byl schopen ve velice krátké době přesně, tedy s co nejmenší chybovostí, určit a zobrazit identitu pacienta. S postupnou evolucí výpočetních technologií, počítačových sítí, biometrických systému a bezpečnostní politiky se ve světě již dnes vyskytují komplexní biometrické systémy, které v plné míře nahradily starší a zároveň nedostatečné náramkové identifikační procesy. Jednou z dalších myšlenek bylo sjednocení všech dílčích zařízení a prvků nutných k samotné identifikaci, příkladem komplikované periferie tak může být použití náramku, jeho tiskárny a čtečky čárových kódů nebo RFID čipů. Všechny tyto části jsem spojil do jednoho celku, který je schopen zpracovávat a zobrazovat nejnutnější, avšak velmi podrobné informace.

8.1 TECHNICKÉ POŽADAVKY PRO ZKONSTRUOVÁNÍ ZAŘÍZENÍ

K tomu, aby bylo možné zahájit realizace návrhu přístroje jsem se v základu zaměřil na stávající biometrické přístroje a systémy, které našli určité uplatnění v komerční sféře. Vycházel jsem částečně z teoretických podkladů a také ze svých praktických zkušeností při tvorbě bakalářské práce. Ze všech možných biometrických senzorů jsem dospěl k závěru, že optimální senzor, který vyhovuje jednak svou velikostí, softwarovou složitostí a pořizovací cenou je optický kontaktní senzor otisků prstů jehož hlavní výhodou je open source prostředí, je tedy možné jej programovat a přizpůsobit vlastním požadavkům. Existuje velké množství senzorů otisků prstů, které mohou vynikat svou špičkovou technickou přesností a miniaturním provedením, nicméně je velice složité takovéto senzory programovat a využívat jejich plný potenciál. Pro účely řešení diplomové práce však bohatě postačuje snímač s odpovídajícím typem

průmyslové klasifikace, jako jsou biometrické parametry pro správnou identifikaci osob FAR a FRR. Mnou použitý senzor má podle výrobce pravděpodobnost určující chybné odmítnutí oprávněné osoby menší než 0,01 % a zároveň pravděpodobnost určující chybné přijetí neoprávněné osoby biometrickým systémem menší něž 0,001 %. Tyto specifikace jsou jasným podkladem k zařazení optického senzoru (GT511-C1R) do tak specifické a bezpečnostně náročné činnosti jakou je identifikace pacientů. Některé typy senzorů je možné připojit a komunikovat s nimi pouze omezeným způsobem, proto bylo potřeba zvolit senzor, který má technologicky nenáročné komunikační rozhraní. Typickým příkladem, který je vhodný pro tuto funkci je asynchronní sériová linka neboli UART. Ta dosahuje ideálního přenosového pásma nutného k rychlé komunikaci mezi řídícím členem a senzorem. Výběr řídící soustavy je taktéž důležitou a nedílnou součástí vestavěného zařízení. Hlavní funkce tohoto prvku by měla spočívat v zajišťování výpočetních, řídících, grafických a komunikačních procesů mezi senzorem otisků prstů, bezdrátovým modulem, databází pacientů a uživatelským displejem. Veškeré technologické a fyzikální principy přenosu dat přímo ovlivňují výběr ideální řídící jednotky. Základní žádané charakteristiky jsou dostatečný výpočetní výkon procesoru, vhodné programovací prostředí, jazykové vybavení systému, úměrně velký paměťový a operační prostor pro uložení vytvořeného programu. S tím souvisí množství a typ vstupně výstupních obvodů pro připojení senzoru otisků a ostatních periferií nutných k celkovému provozu. V poslední řadě hrají významnou roli pořizovací náklady, rozměry řídící desky, dostupnost, vývojové prostředí aplikace ale také především komunita lidí se stejnými nebo podobnými otázkami, kteří si rádi vyměňují názory a rady na možné řešení daného problému.

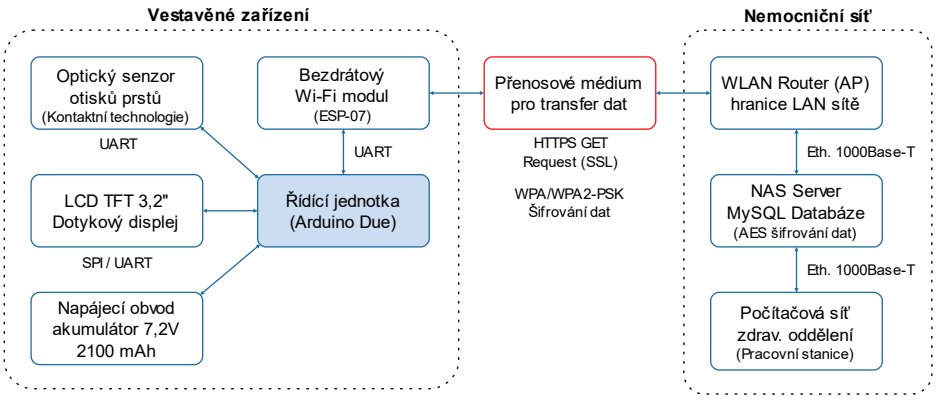
Stejně jako tomu je u jednoduchých pacientských náramků i zde je potřeba vytvořit uživatelské rozhraní kde budou zřetelným a konkrétním způsobem zobrazeny identifikační údaje každého pacienta. Jedná se o sestavení vizuální grafické aplikace integrované do vestavěného zařízení, která bude sloužit k obsluze pacientských dat a jejich ztotožnění při rutinních činnostech zdravotních sester. K tomuto účelu je důležité vybrat displej s ideálním rozlišením, úhlopříčkou, barevnou škálou a podsvícením. Pro pohodlné ovládání nesmí chybět dotyková vrstva displeje. Výběr velikosti displeje by měla záviset na formátu zobrazovaných informací a minimální úhlopříčce displeje pro pohodlné čtení. K přenosu dat mezi vestavěným biometrickým systém a databází pacientů je možné použít několik metod. Ne všechny jsou bezpečné, rychlé a z hlediska síťových infrastruktur optimální. V rámci poznatků teoretických ale i praktických se nejlepším řešením jeví použití bezdrátového komunikačního modulu pro 2,4 GHz sítě Wi-Fi. Právě tento typ počítačových sítí je nejčastější variantou vyskytující se v nemocničních zařízení a působí tak jako ideální zprostředkovatel komunikací. Modul je schopen přenášet šifrovaná data na poměrně velké vzdálenosti s uspokojivou rychlostí. Opět je zde otázka, který typ bezdrátového modulu použít. Dlouhodobým testováním bylo zjištěno, že vyhovují převážně Wi-Fi čipy a karty se snadným projektováním za pomoci AT příkazů s možností připojení externích antén. Podrobnější technické specifikace hardwarových komponentů a funkčních procesů bude popsána v dalších kapitolách.

8.2 BLOKOVÉ SCHÉMA NAVRHOVANÉHO ŘEŠENÍ SYSTÉMU

Srdcem vestavěného systému je řídící jednotka, která zajišťuje veškeré výpočetní a komunikační operace potřebné pro správnou funkčnost zařízení. Principiálně má na starosti řízení a obsluhu optického senzoru otisku prstů, kterému uděluje konkrétní požadavky na zpracování obrazových dat s následným vyhodnocením výsledků identifikace. Optický senzor je k řídící jednotce připojen pomocí dvou párů vodičů umístěných na desce plošných spojů. První pár tvoří jednoduchý napájecí obvod s napětím 5V.

Druhý pár představuje komunikační rozhraní sériové linky (UART), určené k přenosu řídících příkazů. Další připojenou periferií je dotykový LCD TFT 3,2“ displej, který slouží k uživatelské obsluze a práci s pacientskými informacemi. Primární úlohou je zobrazit osobní identifikační údaje každého pacienta, který je ochoten se podrobit procesu kontroly identity. Z hlediska připojení displeje k řídící jednotce je nutné použití velkého množství datových a napájecích vodičů. Na přenos zobrazovaných dat je přiděleno 24 vodičů řídících a 4 napájecí. LCD displej představuje spolu s bezdrátovým Wi-Fi modulem největší odběratele proudu. Je proto nezbytné navrhnout spolehlivé řešení k úměrnému rozložení spotřebované energie a tím i přizpůsobit činnost programu. Třetím prvkem je bezdrátový modul zprostředkovávající komunikaci mezi samotným zařízením a externě umístěným databázovým serverem. Modul je stejně jako optický senzor otisků připojen pomocí dvou párů vodičů sériové linky a napájecího obvodu. Velkou výhodou dnešních modulů využívající podobných síťových technologií je miniaturní provedení, které umožňuje značnou úsporu místa bez ohledu na vysoký výpočetní výkon. Primární úlohou je bezdrátový přenos výsledků z SQL dotazů a PHP scriptů, které slouží jako klíčové nástroje pro správu pacientských údajů. Vyvoláním určitých řídících sekvencí jsou identifikační informace přeposlány z databáze přímo do zařízení a zobrazeny na displeji. Je třeba podotknou, že klíčové informace tzv. metadata, které musí být chráněny, jsou šifrovány podle standartního kryptografického formátu WPA2. Bezdrátový modul operuje na síťových normách IEEE 802.11 b/g/n a vysílací a přijímací obvody jsou připojeny na externí anténu, která zaručuje dostatečně kvalitní spojení s okolní datovou infrastrukturou nemocnice.

Opačnou stranu biometrického systému pro identifikaci pacientů tvoří nezbytné síťové prvky a koncová zařízení, které zajišťují a podporují bezproblémový chod aplikace. K tomu, aby mohla probíhat vzájemná komunikace, musí na protější straně bezdrátového spojení existovat analogická soustava jejíž prioritou je úspěšné doručení odpovídajících datových segmentů. Vzhledem k obecnému faktu, že velká část nemocničních prostor je pokryta různými typy bezdrátových přístupových bodů či WLAN routerů operujících na stejných normách, je ideálním řešením využití právě sítí Wi-Fi. Poté co vznikne vzájemné připojení všech prvků sítě následuje dotazování se databázového serveru na konkrétní údaje spojené jen a pouze s identifikačním číslem každého pacienta. Toto číslo je uloženo ve formě biometrických znaků otisku prstu a je zadáváno při nové registraci na příjmovém oddělení. Pokud zdravotnické informace nejsou předem uloženy v databázi, není možné pacienta úspěšně identifikovat. Pro účely registrace jsem vytvořil intuitivní, avšak plnohodnotnou aplikaci, která může být dostupná z jakéhokoliv nemocničního počítače připojeného v lokální síti. Pouhou nutností je přihlášení oprávněného personálu do systému a sestavení základních údajů, které musí jednoznačně přispět k identifikaci pacienta. Nespornou výhodou je celkové ovládání vestavěného zařízení na dálku, tím zaniká jakékoliv použití propojovacích kabelů.



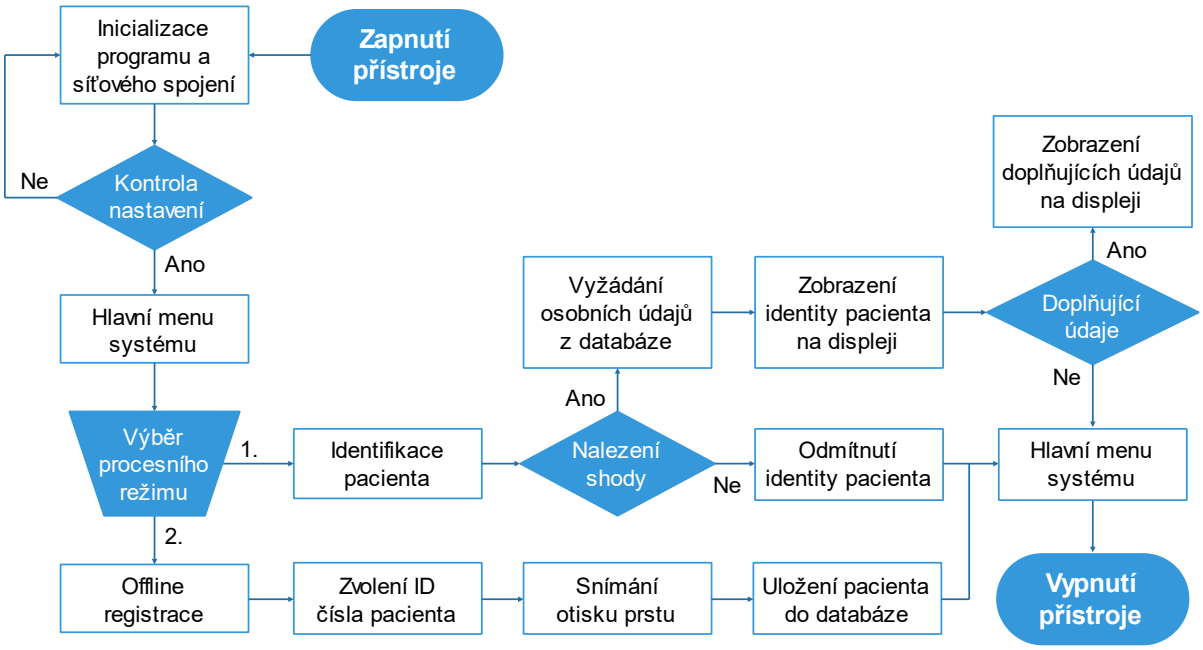
Obr. 24: Zjednodušené blokové schéma systému pro identifikaci pacientů pomocí otisku prstu

8.3 VÝVOJOVÝ DIAGRAM PRŮBĚHU IDENTIFIKACE PACIENTA

V počáteční fázi, kdy je přístroj uveden do běžného provozu, proběhne automatické nastavení a kontrola několika důležitých parametrů a funkcí. Jedná se o inicializaci displeje, senzoru otisku prstů a navázání spojení s bezdrátovou sítí, při které je DHCP serverem přidělena doporučená IP adresa. Dokud není zařízení spárované s nejbližším možným přístupovým bodem sítě, nemůže přijímat online povely od uživatele systému. Doba, která je pro toto nastavení potřebná je vymezena na přibližně 5 sekund. Jestliže jsou všechny parametry nastaveny je zařízení automaticky přepnuto do kontinuálního chodu hlavního menu systému. Zde musí program vyčkat na pokyn uživatele, který zvolí požadovaný režim zařízení. Existují dva primární procesy, které lze s pomocí dotykové vrstvy displeje zvolit. Tyto nabídky jsou znázorněny ve formě velkých tlačítek s charakteristickým označením. Prvním režimem je samotná identifikace pacienta pomocí otisku prstu. Při vyvolání tohoto režimu je pacient informovaně vyzván k přiložení prstu na senzor. Následuje složitý, výpočetně a analyticky náročný proces, během kterého je otisk pacienta identifikován s interní databází senzoru. V té jsou porovnávány již dříve uložené šablony otisků s aktuálně kontrolovaným otiskem. Výsledek může nabývat tří hodnot, avšak pouze dvě se týkají identifikačního procesu. Třetí výsledek upozorňuje na selhání připojení k databázovému serveru.

Nalezením biometrické shody aktuálně snímaného a již uloženého otisku vyvolá novou sekvenci složitých programových operací. Identifikační číslo, které bylo přiděleno výsledku shody je dále využito jako nástroj komunikace s databází pacientů. Pomocí internetového protokolu HTTPS a jeho dotazovací metody GET jsou spuštěny příkazy, které mají za úkol připojení a vyhledání osobních údajů pacienta v databázi. Všechny údaje jsou uloženy právě pod konkrétním identifikačním číslem, které je pro každého pacienta unikátní a neměnné. Nalezené informace v databázi jsou pomocí PHP scriptu přečteny a zpětně poslány v požadované úpravě do zařízení, kde jsou přijatá data spojena do textového formátu vhodného k zobrazení na displeji. Problematickou záležitostí je právě transport dat zpět k Wi-Fi modulu. Bylo tedy zapotřebí sestavit úplně nový komunikační protokol, který by splňoval podmínky pro úspěšný převod dat na řetězec znaků vysílaných do bezdrátového média a naopak protokol, který by tento řetězec převedl zpět na slova a čísla. Doplňující funkcí je zobrazení méně podstatných, avšak stále důležitých informací. Týká se to tří zdravotnických údajů. Jde o preskripci léků, alergie a druhy implantovaných prostředků.

Druhým režimem je tzv. offline registrace pacienta, při kterém vestavěné zařízení není připojeno do sítě. Neznamená to však chybný stav. Tato funkce je navržena pro situace, při nichž je pacient přijat na urgentní oddělení nemocnice a nejsou známy jeho osobní údaje. Proto není zapotřebí použití online aplikace dostupné ze stolních počítačů zdravotnického personálu. Aplikace je určena především k zápisu a uložení konkrétních informací pacienta. Spuštěním režimu offline registrace je displejem zobrazena jednoduchá numerická klávesnice, díky níž může personál pacientovi přidělit identifikační číslo. Dále je proces podobný jako u online registrace (bude vysvětlena dále). Pacient je prostřednictvím grafického uživatelského prostředí celkem třikrát vyzván k přiložení prstu na snímací plochu senzoru otisků. Je to z důvodu optimalizace biometrické šablony, které algoritmus přidělí nejvíce vyhovující vzor papilárních linií. Tento děj trvá přibližně 10 sekund a časově nijak nezatěžuje zdravotnický personál. Šablona otisku se uloží do paměťové databáze zařízení a registrační proces tímto končí. Pacient se při následné identifikaci prokazuje pouze pod svým ID číslem. Během pokračující zdravotnické péče může dojít k objasnění identity pacienta a jeho osobní údaje se doplní k číslu šablony otisku v databázi. Ukončením jakéhokoliv z režimů je ovládání zařízení přeneseno zpět do základního stavu tedy do hlavního menu.



Obr. 25: Vývojový diagram průběhu funkce vestavěného zařízení pro identifikaci pacientů

Jak již bylo vysvětleno dříve, při online registraci pacienta je zapotřebí použít speciální aplikaci dostupnou zdravotnickému personálu z osobních stolních počítačů konkrétního oddělení. Na pracovních stanicích může být aplikace nahrána buďto přímo nebo ji lze spustit vzdáleně z NAS serveru, který však musí být připojen ve stejné lokální síti. Velkou výhodou je především umístění celé MySQL databáze a uživatelské aplikace na jednom místě, resp. na jednom serveru, což usnadňuje případnou správu potíží. Spuštěním aplikace dojde k zobrazení okna pro přihlašování oprávněných uživatelů, tedy zaměstnanců nemocnice, jiné osoby do ní nemají povolení vstupovat. Následně se otevře hlavní grafické prostředí aplikace. V něm je možné provádět řadu operací, nastavení a editací pacientských informací spojených s biometrickými otisky prstů. Při online registraci jsou nejdříve korektně vyplněny základní informace a poté je zahájeno snímání otisku prstu pacienta. Tento proces je obdobný jako u registrování pacienta v offline režimu. Tím je základní konfigurace pro budoucí identifikaci kdekoliv na oddělení hotova a je možné zařízení plně využívat. Pokud nastane potřeba některé informace změnit nebo vymazat, stačí se přihlásit do aplikace, vyhledat pacienta v databázi podle rodného čísla nebo příjmení a provést vybranou editaci. Informace v databázi pacientů jsou aktualizovány a například nově předepsané léky nebo místo přesunu na jiný pokoj či oddělení se při identifikaci automaticky zobrazuje s obnovenými údaji.

Velkou předností celého biometrického systému je bezkontaktní kompatibilita. Tím je myšlena úplná absence jakéhokoliv kabelového připojení. Úpravy a instrukce cílené na zařízení jsou prováděny bezdrátově prostřednictvím lokální Wi-Fi sítě. Doba přenosů informací mezi databázovým serverem, přístupovými body a koncovým zařízením je závislá na typu a místu připojení, nicméně to jsou jednotky sekund. Operace prováděné pouze mezi aplikací a databází jsou prováděny v reálném čase bez zpoždění. Neméně důležitou technickou oblastí je způsob napájení všech obvodů vestavěného zařízení. To je koncipováno na co nejmenší provozní spotřebu akumulátorů. Základní zdroj je tvořen šesti Ni-Mh akumulátory o celkovém napětí 7,2V a kapacitě 2100 mAh, což udává dostatečně velký proudový příkon do zařízení. Vstupní stejnosměrné napětí je pomocí stabilizátoru upraveno na 3,3V a jsou jím napájeny veškeré periferie systému. Tato hodnota napětí umožnuje nižší spotřebu zdroje a vyšší dobu provozu.

9 HARDWAROVÁ REALIZACE IDENTIFIKAČNÍHO SYSTÉMU

Tématem této obsáhlé kapitoly je podrobný popis všech použitých částí, komponentů a řídících systémů. V neposlední řadě je to také vysvětlení funkčnosti a principu, jakým dané elektronické obvody pracují. Hlavním výsledkem praktické části diplomové práce je dokonalé propojení důležitých řídících prvků, které vytváří komplexní a profesionální zařízení schopné bezproblémově identifikovat pacienta pomocí biometrické technologie. Výrobní konfigurace součástek jsou sice stanovena výrobci, avšak vzájemná kombinace už je zvolena podle potřeb konkrétních obvodů. Tím je myšleno například spojení Wi-Fi modulu a řídící jednotky. Nikde není přesně stanoveno, jak se toto zapojení má realizovat a jak programovat. Způsob, jakým jsou vytvářeny finální sestavení všech komponentů již byla má osobní volba a programová část vznikala výhradně pro potřeby specifických obvodů. Celkově jsem použil čtyři různé open source platformy. Jde o řídící jednotku Arduino Due, dotykový LCD TFT displej, bezdrátový Wi-Fi modul ESP8266 ESP-07 a senzor otisků prstů GT-511C1R. Konečné realizaci identifikačního systému předcházelo programovaní a postupem času také samotné testování na nepájivém poli.

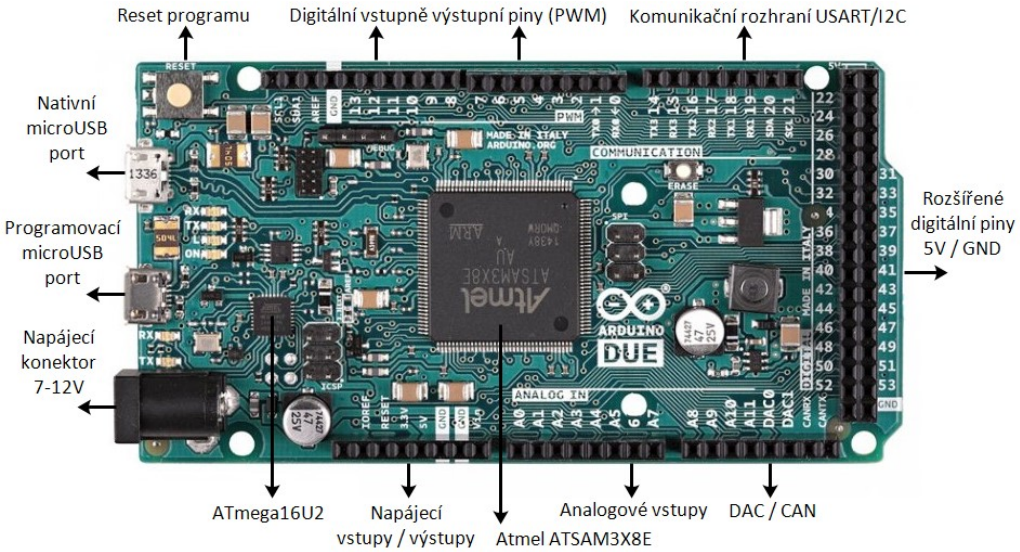
9.1 POUŽITÉ KOMPONENTY K SESTAVENÍ VESTAVĚNÉHO ZAŘÍZENÍ

Krátkým odbočením od technického tématu realizace zařízení je potřeba se částečně zaměřit na fyzickou dostupnost a finanční nákladnost použitých komponentů. Určité typy elektronických součástek a zařízení jsou v České republice obtížně dosažitelné případně cenově mnohonásobně nadsazené. Kromě displeje a konstrukční krabičky byli všechny komponenty pořízeny v zahraničí. Řídící jednotka Arduino Due byla dovezena z amerického obchodu s elektrotechnikou Sparkfun. Stejně tak optický senzor otisku prstů, který je v České republice nedostupný. Cena vývojové platformy Arduino Due činila 1200 Kč a senzor otisků stál přibližně 800 Kč. Naprostým cenovým opakem je bezdrátový Wi-Fi modul. Ten byl dovezen z Číny za 48 korun včetně poštovného. V českých obchodech se jeho cena pohybuje okolo 170 korun. Tento fakt je dán především masivní výrobou, jednoduchým zpracováním, malými rozměry a globálními požadavky na implementaci bezdrátových modulů do IoT systémů. Další komponenty jako LCD displej, konstrukční krabička a zdroj napájení byly pořízeny v českých obchodech s elektronikou. Podrobný rozbor všech prvků vestavěného zařízení je popsán v několika následujících kapitolách.

9.1.1. VÝVOJOVÁ PLATFORMA ARDUINO DUE

Arduino Due je open source vývojová jednodesková platforma založená na procesoru od firmy Atmel. Jedná se o první desku z rodiny Arduino založenou na 32bitové architektuře ARM Cortex-M3 a zároveň o přímého pokračovatele proslulého mikrokontroléru Arduino Mega 2560. Srdcem zařízení je výkonný procesor SAM3X8E s frekvencí 84 MHz. Obsahuje celkem tři typy pamětí. Nejmenší je paměť typu ROM, je součástí hlavního procesoru a slouží pouze pro uložení zavaděče tzv. bootloaderu, který má funkci aktivovaní a jednoznačného stanovení místa posledního uložení operačního, v tomto případě řídícího programu. Dále slouží k přenesení proměnných hodnot do operační paměti. Druhým typem je statická operační paměť SRAM s velikostí 96 kB, ta je ve skutečnosti složena z 32 kB a 64 kB paměti. Poslední a zároveň největší je flash paměť pro ukládání zdrojového kódu. Její velikost je 512 kB a opět je rozdělena na dva menší 256 kB bloky. Arduino Due obsahuje 54 vstupně výstupních pinů pracujících na napěťové úrovni 3,3V. Každý pin může poskytovat signál o velikosti od 3 do 15 mA nebo přijímat signál od 6 do 9 mA. Všech 54 pinů má vytvořené interní připojení k 100 kΩ pull-up rezistorům, které

jsou standardně odpojené. Některé piny mají specializované funkce. Příkladem je dvanáct vyhrazených pinů, které mohou být použity jako 8bitové PWM výstupy pro řízení motorů a jiných analogových obvodů, dalších dvanáct pinů z nich každý může poskytovat až 12bitové rozlišení je rezervováno pro analogové vstupy např. pro digitalizaci signálů ze senzorů neelektrických veličin (teplota, vlhkost atd.). Ve výchozím nastavení je rozlišení čtení vstupních signálů nastaveno na 10 bitů, pro kompatibilitu se staršími deskami Arduino. Maximální vstupní napětí je nastaveno na 3,3V. Při vyšších hodnotách může dojít ke zničení hlavního procesoru. Pro přijímání a vysílání datové komunikaci mezi externími moduly a řídící deskou jsou vyhrazeny hned čtyři hardwarové TTL linky operující na logických úrovních 3,3V. Na desce se kromě těchto sériových linek nachází další komunikační rozhraní jako je SPI, I2C a CAN. Jiný pohled představuje komunikace Arduina s počítačem. Arduino Due je vybaveno dvěma microUSB porty. První je vyhrazen k přenosu zdrojového kódu do flash paměti procesoru. K tomuto účelu slouží jednoduchý čip ATmega16U2, který poskytuje virtuální COM port pro operační systém počítače. Druhý microUSB port je bezprostředně připojen k procesoru SAM3X8E a jeho hlavní funkcí je poskytování CDC komunikace se sériovým monitorem nebo jinými aplikacemi v počítači. Nativní microUSB port může fungovat také jako emulátor pro připojená periferní zařízení, jako jsou smartphony, klávesnice a myši. Před každým nahráváním programu do Arduina předchází kompletní vymazání flash paměti. Je to zapříčiněno pamětí ROM jejíž úkolem je zavedení dat do procesoru, a která je schopná uložit program pouze pokud je flash paměť prázdná. V praxi se před komunikací s počítačem na programovacím portu automaticky nastaví čip ATmega16U2 na datovou rychlost 1200 bps a vytvoří se spojení s konkrétními dvěma piny (erase) procesoru SAM3X určenými pro tvrdé vymazání flash paměti. [30]



Obr. 26: Popis hlavních součástí vývojové platformy Arduino Due

Platformu Arduino Due je možné napájet třemi různými variantami. Nejvíce používanou cestou je napájení pomocí USB/microUSB připojení buďto přímo z počítače, kde je výstupní napětí upraveno na stejnosměrných 5V nebo z externího síťového AC/DC adaptéru. Výhodou připojení Arduina přímo k počítači je absence dvou vodičů, které by musely zastoupit funkci napájecího a datového spojení. Další způsob využívá napájecího "power jacku", který se zasunuje přímo do Arduina přes speciální konektor. Poslední variantou je použití externího zdroje napájení. Jde o často používané připojení, pomocí baterie nebo akumulátoru. Tento zdroj se připojuje na konektory VIN a GND. Zde je znovu výhodou absence připojovacího konektoru, které bezúčelně obsazuje místo potřebné k případnému uložení do konstrukční

krabičky či boxu. Vstupní napětí je omezeno na 6 až 20V. Ideální rozsah je však stanoven na 7 až 12V. Při poklesu napájecího napětí pod hranici 7V může dojít k nestabilní distribuci 5V skrz mikrokontrolér a externí piny. Tento jev je přisuzován stabilizátoru, který pro svou činnost potřebuje o něco vyšší napětí, než na jaké je stanoven jeho pracovní bod. Pokud je vstupní napětí u externího zdroje vyšší, než je 12V může dojít k přehřátí nebo spálení desky, resp. stabilizátoru. Kromě výše zmíněných napájecích pinů a konektorů disponuje Arduino také doplňujícím připojením. Příkladem mohou být piny IOREF a AREF. Ty poskytují referenční napětí pro externí datové moduly nebo analogově digitální převodníky. [30]

Mikrokontrolér	Atmel AT91SAM3X8E
Architektura procesoru	ARM Cortex-M3
Provozní napětí	3,3V
Flash paměť (programové místo)	512 kB (2 x 256 kB)
SRAM	96 kB (64 + 32 kB)
Taktovací frekvence	84 MHz
Analogové I/O piny	12 + 2 D/A převodník
Stejnosměrný proud na pinech (max.)	130 mA (I/O piny), 800 mA (3,3 a 5V piny)
Vstupní napětí zdroje	5 – 12V (limit 6 – 16V)
Digitální piny	54 (z toho 12 pro PWM výstupy)
Rozměry / Váha	53,3 x 101,52 mm / 36 g

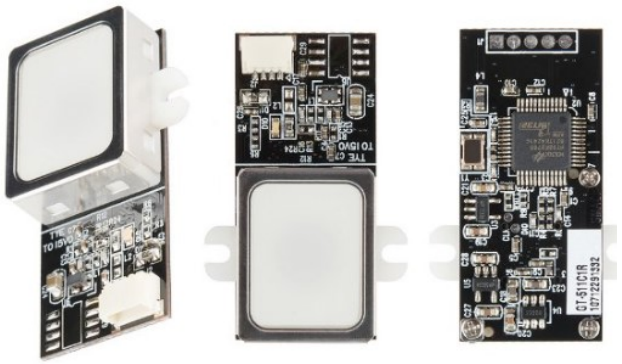
Tab. 3: Technická specifikace vývojové platformy Arduino Due

9.1.2. OPTICKÝ SENZOR OTISKŮ PRSTŮ GT-511C1R

Nezbytnou součástí vestavěného systému zajišťující identifikaci pacientů je senzor otisků prstů. Pro své zařízení jsem zvolil poměrně výkonný senzor GT511C1R od firmy ADH Tech, zaměřující se na vývoj biometrických snímačů, GPS modulů a bezdrátových vysílačů. Tento senzor je přizpůsoben jednoduché konektivitě s ostatními vývojovými platformami podporující sériovou linku. Bez ní by nebyl senzor schopen fungovat. Z mého pohledu je to velké pozitivum použít senzor s UART komunikací, a to z důvodu jednoduchého programování i ovládání. Značné množství vyspělých biometrických senzorů otisků disponuje složitými sběrnicemi, které se jen velmi těžko připojují k vývojovým deskám. Velkou výhodou je také kvalitně zpracovaný datasheet od výrobce, který obsahuje všechny potřebné sekvence příkazů ovládající proces snímání a registrace otisku. Technologie senzoru je kontaktní a optická, jedná se tedy o snímač s přímým dotykem prstu pacienta, který je zvýrazněn viditelným zdrojem světla (LED). V praxi je obraz pomocí optické soustavy drobných čoček zaznamenáván a společně s CCD snímačem dále digitalizován. V rámci postprocessingové úpravy je obraz filtrován, binarizován a jsou extrahovány markantní body. Konečným produktem je šablona unikátních bodů charakterizující konkrétní otisk.

Senzor je vybaven 32bitovým procesorem ARM Cortex M3. Aktivní snímací plocha disponuje rozlišením 240 x 216 pixelů což udává obrazovou hustotu 450 dpi. V závislosti na konkrétním modelu senzoru (existuje jich několik, odlišující se v ceně a rozlišení) je možné do interní databáze uložit od 20 do 3000 rozdílných otisků. Velikost extrahovaného snímku, tedy šablony markantních bodů dosahuje 506 B, originální obraz otisku prstu v rozlišení QVGA pak 52 kB. Senzor podporuje dva biometrické standardy, a to kontrolu pacienta 1:1 nebo 1:N. Rychlost sériové komunikace mezi senzorem a externí řídící jednotkou je stanovena na 9600 Bd. Podstatnou roli hraje přesnost, rychlost uložení a identifikace otisku. Přesnost biometrických systémů je obecně definována mírou chybného přijetí, která je v tomto

případě menší než 0,001 % a zároveň míra chybného odmítnutí pacienta je menší 0,01 %. Verze senzoru GT511C1R umožňuje ukládat otisky po dobou kratší, než jsou tři sekundy. V průběhu této doby jsou registrovány celkem tři obrazové snímky, každý s odlišnou projekcí. Z praktického hlediska je nicméně důležitější čas identifikace pacienta, který je přímo závislý na velikosti a počtu uložených šablon otisků v interní databázi. Při nejmenším počtu uloženým šablon, tedy 20, je doba potřebná k identifikaci menší než 1,5 sekundy. V rámci mnou vytvořeného zařízení je čas o něco málo delší. Je to dáno komunikací s cílovým serverem a přenosem pacientských dat přes několik síťových uzlů s rozdílnou technologií. Doba zobrazení konkrétních informací tak může maximálně vzrůst na 5 sekund. Operační stejnosměrné napětí senzoru je stanoveno v rozmezí od 3,3 do 6V. Při překročení horního limitu napětí může dojít k destrukci procesoru. Odběr proudu je vázaný na aktuální činnost. Maximální hodnota je však 130 mA. [31]



Obr. 27: Optický senzor otisků prstů GT511C1R

CPU	ARM Cortex M3
Technologie	Optická/Kontaktní
Rozlišení	240 x 216 pixelů
Obrazová hustota	450 dpi
Počet otisků (dle typu)	20–3000
Metody identifikace	1:1 a 1:N
FAR / FRR	0,001 % / 0,01 %
Vstupní napětí zdroje	3,3 – 6V DC
Proudový odběr	<130 mA

Tab. 4: Technická specifikace senzoru otisků

Konektivitu s řídícím prvkem systému zajišťuje metoda sériové komunikace tzv. UART. Jedná se o asynchronní přenos dat, který pracuje na principu posílání 8bitových sekvencí jedniček a nul. Celý datový blok je vymezen start a stop bitem. Na začátek posílané zprávy je připojena logická 0 a na konec datového rámce logická jednička. Výsledná sekvence bitů pak může vypadat následovně 0|00110110|1. Fyzické připojení je realizováno pomocí čtyř vodičů a JST-SH konektoru. První dva vodiče jsou určeny pro napájení senzoru a nesou označení VIN a GND. Zbylé dva vodiče RX a TX slouží k přenosu dat v plně duplexním režimu. Pro korektní průběh posílání informací je nutné připojit datové vodiče do kříže a do pinů podporující logickou úroveň 3,3V. Proces přenosu instrukcí a dat mezi jednotlivými prvky zařízení je řízen komunikačním protokolem. Ten může zastávat tři rozdílné funkce. První je příkazový protokol, který slouží k řízení procesů a ovládání senzoru. Formát těchto příkazových paketů je složený z šesti částí. První dva bajty jsou tvořeny hexadecimálním kódem 0x55 a 0xAA, což je série jedniček a nul spojených za sebou udávající začátek posílané zprávy. Následující dva bajty tvoří identifikační číslo senzoru a továrně jsou nastaveny na 0x0001. Pátý až osmý bajt je vyhrazen pro vstupní parametr, který definuje příkazový paket. Další dva bajty určují konkrétní příkaz pro senzor, je charakterizován několika předem definovanými hexadecimálními čísly, které zastupují určitou funkci. Například kód 0x01 slouží k inicializace senzoru, 0x12 spouští LED podsvícení a 0x51 zahajuje identifikaci otisku. [31]

Druhou funkcí komunikačního protokolu je tzv. Response packet. Slouží k odezvě na příchozí instrukce. Tímto se kontroluje činnost proběhlých funkcí. Prvních osm bajtů odpovědi má stejný význam jako v předchozím, příkazovém paketu. Obsahuje tedy určení začátku sekvence, ID číslo senzoru a nově tzv. acknowledge. Ten může nabývat dvou hodnot. Pokud předchozí příkaz vykonal danou instrukci je response paketem odeslán acknowledge s hodnotou 0x30, pokud však došlo k chybě odešle se Non-Ack s hodnotou 0x31. Poslední třetí funkcí je tzv. Data packet. Slouží k odesílání zdrojových informací mezi

senzorem a řídící jednotkou. Jde opět o totožný průběh protokolu jako v předchozích případech. Jediná změna se týká pátého bajtu a dále. Ten je rezervován pro konkrétní data charakterizující šablonu otisku prstu. Na konci každého rámce protokolu je připojen součtový bajt tzv. Check Sum, jehož úkolem je kontrola, zda všechny odeslané bity dorazily do cíle. V rámci svého vestavěného zařízení používám dvě základní operace, které senzor umí provádět. Jsou to procesy identifikování a ukládání otisků. V prvním případě jsem uplatnil předdefinované příkazy pro biometrickou identifikaci jako jsou *IsPressFinger* – detekuje přiložený prst na snímači, *CaptureFinger* – vytváří digitální obraz otisku a *Identify*, který slouží k finálnímu rozhodnutí, zda aktuálně snímaný otisk je totožný s otiskem uloženým v databázi senzoru. V druhém případě jde o první registraci/uložení otisku do paměti senzoru. Na tuto činnost jsou přiděleny příkazy jako *EnrollStart* – nastavující unikátní identifikační číslo otisku prstu a *Enroll* – zahajující čtení struktur papilárních linií. Tato funkce je rozdělena do třech kroků kvůli zkvalitnění výsledného otisku.

9.1.3. BEZDRÁTOVÝ KOMUNIKAČNÍ WIFI MODUL ESP 8266 ESP-07

Modul ESP 8266 v pokročilé verzi ESP-07 je nízkonákladový Wi-Fi mikrokontrolér podporující kompletní TCP/IP síťový protokol. Výrobcem je čínská firma Espressif Systems se sídlem v Šanghaji. Díky výkonnému a vysoce integrovanému 32bitovému SoC Tensilica L106 s jádrem Xtensa pracujícím na frekvenci 80 MHz umožňuje vytvářet spojení a komunikovat s okolními prvky přes bezdrátovou síť IEEE 802.11b/g/n. Modul pracuje v pásmu 2,4 GHz a může fungovat také jako access point nebo klient. Obsahuje kompletní sadu bezpečnostních standardů typicky WPA/WPA2 s šifrováním WEP nebo AES. Paměťové místo reprezentují tři typy pamětí, ROM, SRAM a Flash paměť. První dvě paměti ROM a SRAM jsou součástí integrovaného procesoru Xtensa. Velikost SRAM paměti je 96 kB, ale uživatelsky použitelné je jí méně (přibližně 36 kB), protože velkou část zaujímá samotný Wi-Fi stack. Veškerá další volná paměť se připojuje zvenčí. Tímto výrobce umožňuje rozšíření libovolně velkého místa pro vlastní aplikace. Z výroby je však modul vybaven flash pamětí s velikostí 1 MB. Modul bývá často označován za nadstandardně výkonný oproti většině jiným mikrokontrolerům podobné velikosti. Je to dáno hlavně rozsáhlou sítí periferií jako jsou A/D převodník, GPIO, UART, SPI, I2C sběrnice a mnoho dalších. [32]

Verzi ESP-07 je možné připojit k ostatním mikrokontrolerům díky sériovému rozhraní pracující v plně duplexním režimu. Je důležité, aby přenosová rychlost byla konfigurována na 115200 bd. Jiné nastavení není podporováno. Procesor také obsahuje mnoho GPIO pinů, většina z nich je na rozdíl od předchozích verzí dostupná a nejsou použity pouze k propojení procesoru a vnitřních periferií modulu. Velkým technologickým pozitivem modulu ESP-07 a obecně všech ESP8266 procesorů je konstrukce integrovaných obvodů uvnitř čipu. Ta je uzpůsobena tak, aby zahrnovala jak analogovou část pro příjem a vysílání signálu tak i digitální integrované obvody pro zpracování a řízení průběhu datového přenosu. Kontakt s vnějším prostředím sítě zajišťuje keramická anténa, která je vyvedena ze stíněného pouzdra procesoru na povrch desky. Kromě této antény je na modulu umístěn U-FL soket pro připojení externí antény zaručující hodnotnější zesílení signálu. V rámci mého zařízení bude použita pouze externí anténa s koaxiálním vývodem. Důvodem je zabudování modulu dovnitř hliníkové konstrukční krabičky, která by signál zeslabovala. Pro základní funkčnost není potřeba mikrokontrolér přímo programovat. Systém obsahuje tzv. AT firmware, který lze ovládat předdefinovanými příkazy. Jedná se o průmyslový standard zahrnující základní sadu příkazů podporovanou většinou výrobců, jednotlivé modely síťových zařízení mohou mít příkazy rozšířené či pozměněné. Z obecného hlediska jsou tvořeny krátkými sekvencemi písmen, znaků nebo čísel. Každý AT příkaz má jiné označení a vytváří jinou činnost. Odesílání příkazů

a ovládání modemu (v mém případě bezdrátového modulu) je řízeno pomocí komunikačního programu, nejčastěji terminálu. AT příkazy začínají ve tvaru AT + "daný kód", který má provézt charakteristickou operaci v modulu. Výsledkem je realizace síťového nastavení a odezva procesoru se zprávu OK. Pokud modul neodpovídá, je chyba obvykle na straně spojení nebo může být nesprávně nastavena přenosová rychlost 115200 bd. Standartní zapojení modulu je provedeno pomocí šesti vodičů. První pár má funkci napájecího obvodu. Modul tak může být napájen od 3 do 3,6V. Při vyšším napětí dojde k destrukci čipu. Třetí vodič připojuje zdrojové napětí na pin CH_PD, což je zapínací switch, který udržuje kontinuálně zapnutou Wi-Fi část. Druhý pár (RX a TX) tvoří klasickou sériovou komunikaci. Posledním vodičem je bootovací uzemňovač, který jednoznačně definuje, do jakého režimu se má modul nastavit. Pokud tedy není pin GPIO15 uzemněn, modul nebude schopen zahájit bootovací sekvenci firmwaru. [32]

Obr. 28: Bezdrátový Wi-Fi modul ESP-07

Mikrokontrolér	ESP 8266 SoC Tensilica L106
Bezdrátový standard	2,4 GHz 802.11 b/g/n
Módy komunikace	Access point / Klient / Obojí
Síťové protokoly	TCP / IP Stack
Zabezpečení	WPA / WPA2 + AES / WEP
Pracovní napětí	3 – 3,6V DC
Typická spotřeba	80 mA (max. 350 mA)
Ovládání	AT příkazy
Periferie	SPI / UART / I2C / GPIO / PWM
Typ antény	Interní keramická + U.FL

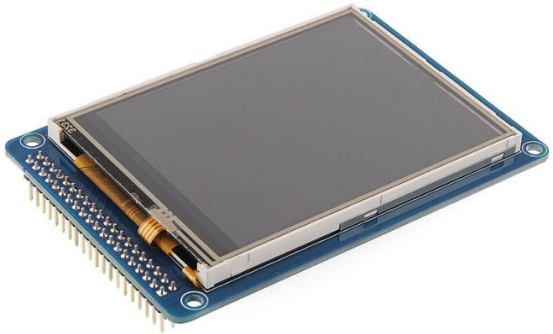
Tab. 5: Technická specifikace bezdrátového Wi-Fi modulu

9.1.4. LCD 3.2" DISPLEJ S DOTYKOVOU OBRAZOVKOU

Podstatou většiny pokročilých vestavěných systémů využívající grafické rozhraní je optimálně velké zobrazovací vybavení s kvalitním rozlišením, které bude schopno přehledně poskytnout informace odpovídající uživatelským požadavkům. V dnešní době moderních displejů s různými velikostmi, tvary a funkcemi se již nevyplatí realizovat zařízení, které bude obsahovat mechanické spínací nebo přepínací prvky. Je zde možnost využít dotykové vrstvy displeje a vhodného programu, díky němuž všechny tyto nutnosti zaniknou. Z hlediska řešení interakce mezi zdravotnickým personálem a pacientem jsem zvolil dobře známý 3,2 palcový dotykový LCD displej od společnosti SainSmart poskytující rozlišení 320 x 240 pixelů. Displej umožňuje zobrazit velká i malá písmena, číslice, ale také ostatní speciální znaky z ASCII tabulky nacházející se v prvních 128 řádcích. Obecně se jedná o výkonný a multifunkční grafický modul podporující komunikaci přes sériové rozhraní přizpůsobené displeji. Kompletní rozhraní tvoří 40 pinový konektor (2x20), nicméně ne všechny piny jsou obsazeny nebo vyčleněny k zobrazování. [33]

Prvních šestnáct pinů s označením DB0 až DB 15 slouží k připojení datových vodičů, které mají za úkol paralelně přivádět grafické informace z řídící jednotky do displeje. Šířka přenosové informace může být nastavena buď na 8 nebo 16 bitů. Dalších pět pinů je typických pro připojení řídících obvodů. Jde o piny RS: register select, WR: write or read, RD: read data, CS: chip select a REST: reset displeje. Piny GND a VCC slouží k napájení 5V. Posledním důležitým pinem je LED_A, na který se připojuje napětí 3,3V a díky němu může být displej podsvícený. Kromě napájení, musí být všechny ostatní piny připojeny na obvody s logickou úrovní 3,3V. Podstatnou výhodou displeje je implementace dotykové vrstvy umístěné na svrchní části LCD panelu. Díky ní je možné emulovat virtuální dotyková místa, která se budou chovat jako klasické spínací prvky. Připojení dotykové vrstvy je vytvořeno díky SPI sběrnici

spojující řídící desku Arduino Due s displejem. Zapojení je realizováno pomocí pěti vodičů. První čtyři tvoří SPI rozhraní (MISO, MOSI, CLK a CS) a pátý vodič má funkci přerušení. V rámci programování grafické podoby uživatelského rozhraní jsem využil dvou základních knihoven sestavených výrobcem vztahující se přímo k hardwarovému řadiči SSD 1289 umístěném na plošném spoji displeje. Knihovny se nazývají UTFT a URTouch. První z nich poskytuje popis základních funkcí týkajících se vypisování znaků a geometrických tvarů na LCD displeji nebo nastavení fontu písma spolu s jeho velikostí. Druhou knihovnou je URTouch, ta charakterizuje způsoby ovládání dotykového panelu a sensitivitu konkrétní plochy displeje s reakční citlivostí na dotyk. Doplňujícím atributem je možnost připojení SD karty ze spodní strany displeje, z ní tak lze zobrazovat uložené obrázky, videa či jiná grafická data. Pozitivem je otevřenost vůči jiným open source platformám podporující mikrokontroléry s architekturou AVR, 8051 nebo STM32. Určitým negativem je velké množství připojovacích konektorů, které omezují výběr všech možných vývojových desek na ty, které mohou tento displej připojit a ovládat. [33]



Obr. 29: TFT LCD 3,2" dotykový displej

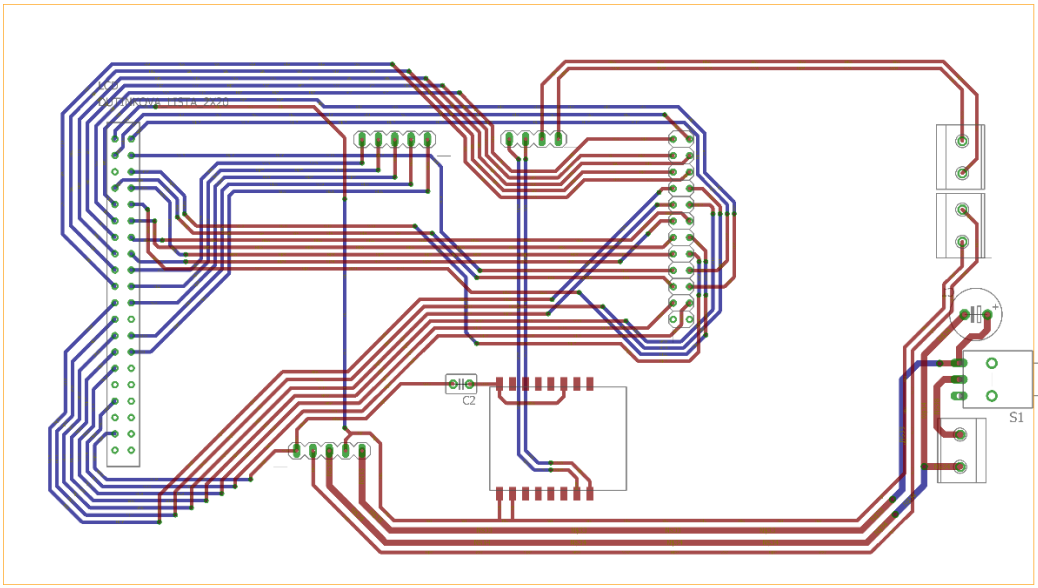
Rozlišení displeje	320 x 240 pixelů 3,2"
Počet barev RGB	262 144
Řadič LCD displeje	ILI9341
Řadič dotykové vrstvy	SSD1289
Provozní napětí	3,3V / 5V napájení
Formát přenosu dat	16bitový RGB 565
Konektivita	2x20 pin header 2,54
Podpora MCU	STM32, AVR, 8051

Tab. 6: Technická specifikace dotykového LCD displeje

9.1.5. DPS SHIELD PRO VZÁJEMNOU KONEKTIVITU PERIFERIÍ

Vývoj vestavěného zařízení odhalil mnohá technická úskalí, která bylo potřeba vyřešit. Jedním z nich je propojení všech výše popsaných periferií do jednoho fungujícího celku. Již během sestavování prototypového zařízení v nepájivém poli vešla ve skutečnost nutnost eliminovat značný počet datových a napájecích vodičů, z důvodu praktického umístění do konstrukční krabičky. Počet vodičů se pohyboval okolo třiceti, což mě vedlo k požadavku vytvořit si vlastní desku plošných spojů, která by tento problém vyřešila. Díky znalosti vývojového prostředí Autodesk Eagle jsem byl schopen navrhnout dvouvrstvou desku tzv. shiled umožňující propojení všech použitých komponentů vestavěného zařízení. Bylo nutné vytvořit patice pro dotykový displej, Wi-Fi modul, senzor otisku prstů, a především řídící prvek Arduino Due. Rozměr DPS jsem stanovil na 90 x 160 mm což přesně odpovídá vnitřním rozměrům konstrukční krabičky. Vodivé cesty na desce jsou rozděleny do několika částí. První z nich je napájecí obvod, který přivádí zdroj napětí z akumulátorů na svorkovnice umístěné na desce, ty pak rozvedou potřebnou energii do řídící jednotky. Další dva typy tvoří signálové spoje. Vzhledem k jejich množství bylo zapotřebí je rozdělit a vézt jak na svrchní, tak i spodní straně desky za použití prokovených otvorů. Šířka signálových cest je nastavena na 0,5 mm a napájecích na 0,8 mm. Izolační vzdálenost mezi cestami, prokovy a pady je minimálně 0,4 mm. V softwaru Eagle se tyto cesty nazývají Top a Bottom. Ukončení vodivých spojení je provedeno pomocí kolíkových a dutinkových lišt s roztečí 2,54 mm. Na DPS se také nacházejí dva kondenzátory, tantalový a elektrolytický s kapacitou 100nF a 470uF. První realizuje funkci blokovacího kondenzátoru pro vyhlazení kolísavého napájení Wi-Fi modulu. Druhý pak slouží k vyhlazení vstupního napájení z akumulátoru. Uvedení desky do provozu zajišťuje dvoupolohový páčkový přepínač s aretací,

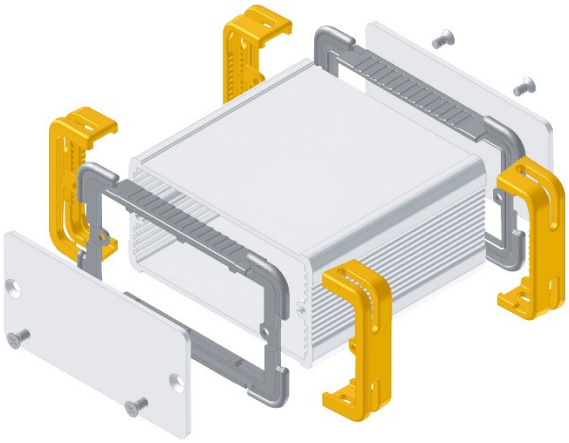
který je přímo připojen ke vstupnímu napájecímu okruhu. Vzhledem ke skutečnosti, že výroba společně s technologickou přípravou v českých podnicích stojí přibližně 1900 korun, rozhodl jsem se kontaktovat profesionálního výrobce DPS přímo v Číně. Společnost SJPCB se sídlem v čínské provincii Guangdong mi byla schopna vyrobit desku v počtu pěti kusů za 800 korun včetně poštovného. Charakteristiky desky potřebné k výrobě: tloušťku desky jsem stanovil o něco málo vyšší na 1,6 mm, jako finální proces úpravy jsem zvolil žárové pokovování plošných spojů tzv. HASL (Hot air solder leveling), materiálem substrátu je skelný laminát nasycený epoxidovou pryskyřicí a plátovaný měděnou fólií tzv. FR4, počet vrstev dvě (oboustranné), zelená nepájivá maska na obou stranách desky a tloušťka měděných cest 35 um. Reálným návrhům DPS předcházela tvorba schémat teoretického zapojení součástek, v rámci kterého jsem musel realizovat nové knihovny pro svorkovnice, kolíkové a dutinkové lišty, spínač a Wi-Fi modul. Zdrojová data byla výrobci poskytnuta ze softwaru Autodesk Eagle ve formátu *.brd.



Obr. 30: Grafický návrh DPS shieldu pro vzájemnou konektivitu periferií vestavěného zařízení

9.1.6. KONSTRUKČNÍ KRABIČKA PRO ELEKTRONICKÉ SOUSTAVY

Posledním článkem vestavěného zařízení je konstrukční krabička či box, který má fungovat jako praktické místo pro uložení všech použitých komponentů. Výběr ideálního produktu splňující technické a konstrukční požadavky byl velmi náročný. Mezi technické nároky jednoznačně patří základní materiál, ze kterého má být tělo krabičky vyrobeno. Mnou zvolená krabička je celá sestavena z kvalitní hliníkové slitiny. Je tedy velmi pevná a dobře dezinfikovatelná, což souvisí s nezbytnou vlastností zdravotnických prostředků. Výhodou hliníkového materiálu je hmotnost a jednoduché opracování. Díky této vlastnosti umožňuje vyřezání předem definovaných otvorů pomocí CNC frézování. Dva otvory jsou umístěné na vrchní straně krabičky (displej a senzor), dva na bočním panelu pro externí připojení antény a zapínacího tlačítka a čtyři malé otvory jsou na spodní straně krabičky, kde slouží pro připevnění vnitřních součástek. Velká část prodávaných krabiček pro elektronické soustavy jsou buďto plastové nebo ocelové, což v ani jednom příkladu není výhodné řešení. Ze všech potenciálních výrobků jsem zvolit variantu tubusového charakteru s odnímatelnými bočními panely z hliníku opatřenými gumovou ochranou proti poškození. Výrobcem krabičky je německá firma Fischer Elektronik specializující se na elektronické součástky, konektory, chladiče a pultové skříňky. Vnější velikost krabičky dosahuje 160 x 116 x 63 mm a je přesně tvarovaná tak, aby bylo možně do ní umístit dvě desky DPS s připojenými součástkami a napájením.



Obr. 31: Model krabičky pro vestavěné zařízení

Výrobce	Fischer Elektronik
Typ krytu	S panelem
Řada krabičky	FR ME
Rozměr X (délka)	160 mm
Rozměr Y (výška)	63,5 mm
Rozměr Z (šířka)	116 mm
Materiál	Hliník + plast
Stupeň krytí	IP54
Hmotnost	370 g
Barva	Šedá / žluté rámečky
Montážní materiál	4 x šroub M3

Tab.7: Technická specifikace konstrukční krabičky

9.2 OSTATNÍ POUŽITÉ KOMPONENTY PRO SPRÁVU SYSTÉMU

Poslední kapitolu zaměřující se na hardwarové komponenty biometrického systému tvoří síťové prvky zprostředkovávající komunikaci mezi intranetem nemocniční datové infrastruktury a samotným vestavěným zařízením. Z obecného hlediska je možné pro tuto funkci použít jakékoliv koncové zařízení podporující bezdrátový přenos dat na základě standardu IEEE 802.11 a datové úložiště či NAS server s podporou databází, hardwarového a programového zabezpečení nebo zálohováním. V rámci českých nemocnic jsou v prostorách profesně orientovaných oddělení, operačních sálech a veřejných chodbách ve větší či menší míře umístěny bezdrátové access pointy teoreticky využitelné pro potřeby připojení na centrální rozvody nemocničního informačního systému. Jak už bylo vysvětleno v kapitole 8.2 věnující se blokovému schématu a návrhu biometrického systému, musí existovat alespoň lokální nebo vzdálené připojení mezi pracovními stanicemi (např. PC na příjmovém oddělení) obsahující uloženou registrační aplikaci a databázovým serverem. Bez těchto požadavků nemůže komunikace probíhat. V následujících dvou podkapitolách jsou popsány technologické a funkční charakteristiky mnou použitých a také v praxi vyzkoušených síťových zařízeních. V komerční sféře jsou tyto prvky infrastruktury důmyslnější, dražší a mnohem větší. Mezi přední světové výrobce těchto zařízení patří Cisco, TP-Link, Dell a Qnap.

9.2.1. SÍŤOVÉ DATOVÉ ÚLOŽIŠTĚ QNAP TS-251 8G

Datové úložiště TS-251 8G od Taiwanského výrobce QNAP Systems poskytuje velice výkonné a vysokokapacitní řešení pro správu, synchronizaci, vzdálený přístup a efektivní zálohování digitálních souborů. NAS je vybaven 64bitovým dvoujádrovým procesorem Intel Celeron 2,41 GHz s architekturou o velikosti 22 nm. V případě nároku na vyšší výkon dokáže systém zvýšit pracovní frekvenci procesoru až na 2,58 GHz. Nízkoenergetická operační paměť typu DDR3L disponuje 8 GB volného místa. Server je vybaven dvěma šachtami pro umístění dvou plotnových (či SSD) disků se standardizovaným SATA konektorem. Konektivita s okolními systémy je zajištěna hned několika způsoby. Primární připojení je realizováno pomocí dvou přístupných 1Gb LAN portů, dále jsou na zadním panelu serveru umístěny tři USB porty z toho jeden ve verzi 3.0. Doplňující funkcí je streamování obrazových souborů díky HDMI konektoru. Model TS-251 8G poskytuje vysokou rychlost zápisu (až 222 MB/s) a čtení (až 224 MB/s) dat na discích. Nezbytné zabezpečení systému garantuje 256bitové AES šifrování, které umožňuje zápis a čtení dat s rychlostí 68 MB/s, čímž zajišťuje dostatečný výkon pro uchování citlivých osobních údajů.

Díky operačnímu systému QTS 4.3 (založeném na platformě Linux) a virtualizační technologii QvPC funguje NAS server jako samostatný stolní počítač a lze tak spouštět aplikace určené pro operační systém Windows, Unix, Linux či Android. Je možné jej plně ovládat z jiného počítače mimo lokální síť prostřednictvím internetového prohlížeče, nebo je možné připojit klávesnici, myš, monitor a pracovat s ním jako s počítačem. Operační systém umožňuje instalaci různých aplikací (pro přehrávání multimédií, pro zálohování souborů, jejich sdílení, pro stahování souborů z internetu, pro antivirovou ochranu atd.). Veškeré softwarové prostředí a externí „help service" je lokalizován v českém jazyce. Z hlediska zálohy informací poskytuje NAS server několik variant managementu diskových polí. Základní uspořádání dat je vytvořeno pomocí metody JBOD nebo RAID0 což je nepřímý úložný systém, který neshromažďuje žádné nadbytečné soubory, jež by představovali určitý způsob zabezpečení. Další variantou je RAID1, ta je označována také jako zrcadlení (mirroring), jde o efektivní a jednoduchý způsob ochrany uložených dat, využívající principu dvojitého zapisovaní souborů na dva oddělené pevné disky. Soubory zapsané na interních discích jsou formátovány do standardu EXT4, který je typický pro linuxové systémy. [34]

Obr. 32: NAS server QNAP TS-251 8G

CPU	Intel Celeron 2,41 GHz
DRAM	8 GB DDR3L
Diskové pole	2 x 3,5" / 2,5" SATA
LAN porty	2 x Gigabit RJ-45 Eth.
Síťové rozhraní	TCP/IP, Proxy, DHCP, SMB, FTP, FTPS, TFTP, http, Telnet, SSH, SMTP, iSCSI, AFP, NFS, SMSC
Zabezpečení	256Bitové AES, SSL, CIFS
Typ zálohování	JBOD, RAID0, RAID1, Snapshots, Storage pools,
Operační systém	QTS 4.3 (Linux)
Formát souborů	Interní: EXT4, Externí: EXT3/4, NTFS, FAT32

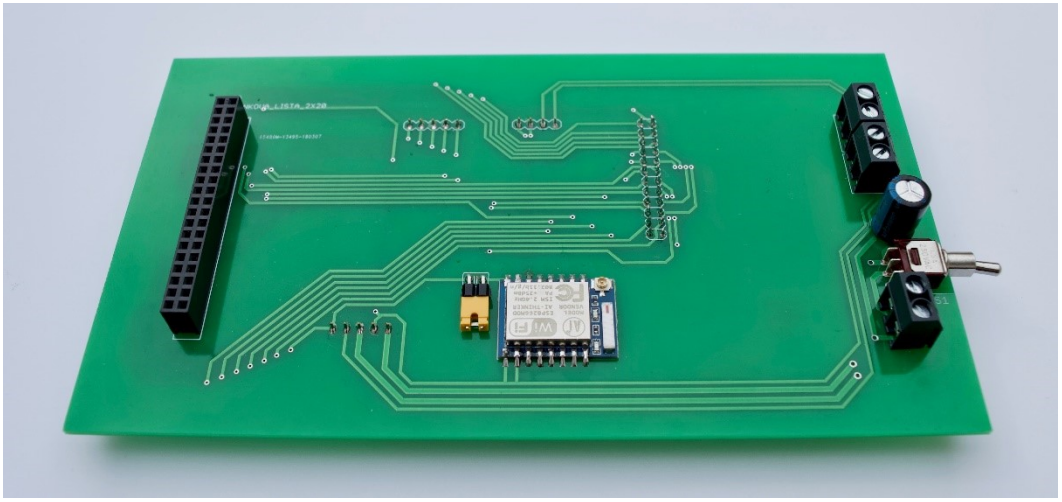
Tab. 8: Technická specifikace QNAP TS-251 8G

9.2.2. WLAN ROUTER TP-LINK AC-750 ARCHER C2

Posledním prvkem síťové komunikace je obecně jakýkoliv přístupový bod nebo WLAN router, který je dostatečně výkonný, má optimální dosah signálu, disponuje alespoň 1 Gb LAN porty a zajišťuje šifrované přenosy. Pro rozsáhlé infrastrukturní sítě se samozřejmě vyplatí instalovat profesionální AP nebo routery s průmyslovou certifikací, kterou mají např. zařízení Cisco nebo Dell. TP-Link Archer C2 je router určený především pro domácnosti a případně malé kanceláře, který nabízí bezdrátovou podporu s vyšší datovou propustností v porovnání s klasickým standardem 802.11n. Router je vybaven dvěma dvoupásmovými externími anténami s konektorem RP-SMA pracující ve frekvenčním pásmu 2,4 GHz, v němž dosahuje teoretické propustnosti 300 Mbps a v pásmu 5 GHz, kde lze poskytnout až 433 Mbps. Ve výsledku je možné síťové vysílání rozdělit, a to třeba tak, že datově méně náročný provoz (webové stránky, e-mail) bude přenášen v klasickém pásmu 2,4GHz a 5GHz pásmo bude rezervováno pouze pro přenos multimédiálních dat. Z pohledu uživatelského rozhraní jsou k dispozici čtyři gigabitové LAN porty pro připojení lokální síťových prvků a jeden gigabitový WAN port pro připojení vnější sítě, např. providera. Zařízení dále obsahuje USB port pro připojení externích disků nebo lokálně sdílenou tiskárnu. Samozřejmostí je integrovaný firewall, možnost nastavení pravidel pro přístup uživatelů a bezpečnostní podpora šifrovaného přenosu dat pomocí WPA-PSK, 64/128 WEP nebo WPA2-PSK a IPv6. [35]

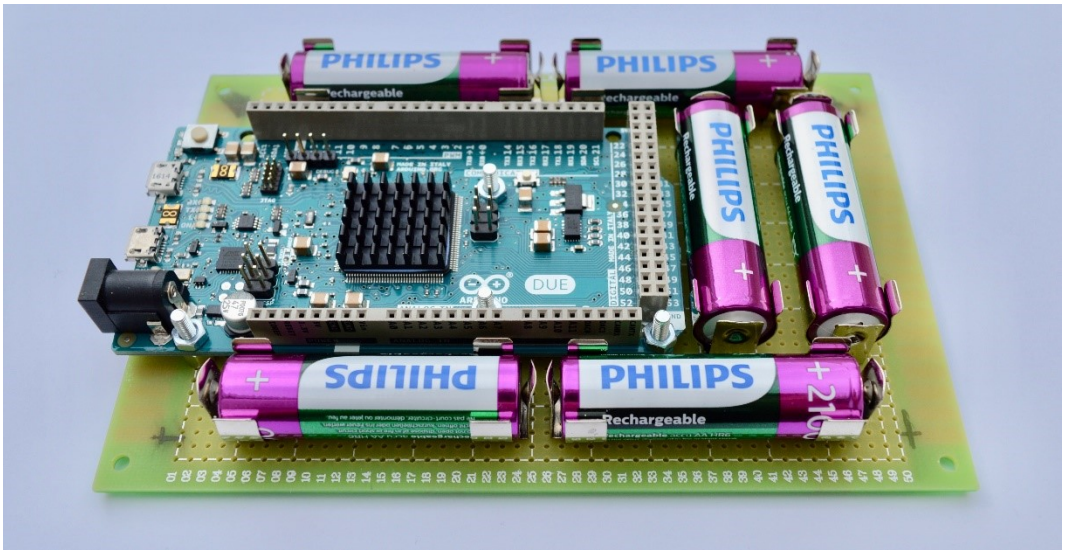
9.3 FINÁLNÍ ŘEŠENÍ A ZAPOJENÍ JEDNOTLIVÝCH ČÁSTÍ ZAŘÍZENÍ

Hotové řešení praktického zapojení všech výše uvedených komponentů je realizováno a složeno do dvou částí, které spolu navzájem spolupracují. První část tvoří mnou navržená deska plošných spojů detailně popsaná v kapitole 9.1.5, jejíž hlavním úkolem je propojit řídící jednotku s displejem, senzorem otisku prstů, Wi-Fi modulem ESP-07 a zdrojem napájení. Deska představuje jádro vestavěného zařízení a je navržena tak, aby miniaturizovala maximální velikost technického řešení celého systému, a navíc eliminovala použití drátových vodičů pro komunikační přenosy. Primární konektivita s periferiemi je vedena přes precizní kolíkové a dutinkové lišty, svorkovnice a integrované vodiče. Řídící jednotka je připojena k DPS pomocí datových a napájecích pinů. Na desku tak je přivedeno napájení z akumulátorů pro ostatní komponenty a jsou rozvedeny řídící, UART a SPI linky. Deska je také vybavena páčkovým přepínačem s aretací, sloužící jako spouštěcí tlačítko. Jde také o jediný mechanický prvek vestavěného zařízení, všechna ostatní ovládání jsou prováděna přes dotykový povrch displeje.



Obr. 33: Deska plošných spojů reprezentující hlavní část vestavěného zařízení spojující všechny ostatní komponenty jako je řídící jednotka, LCD displej, Wi-Fi modul, senzor otisků a zdroj napájení

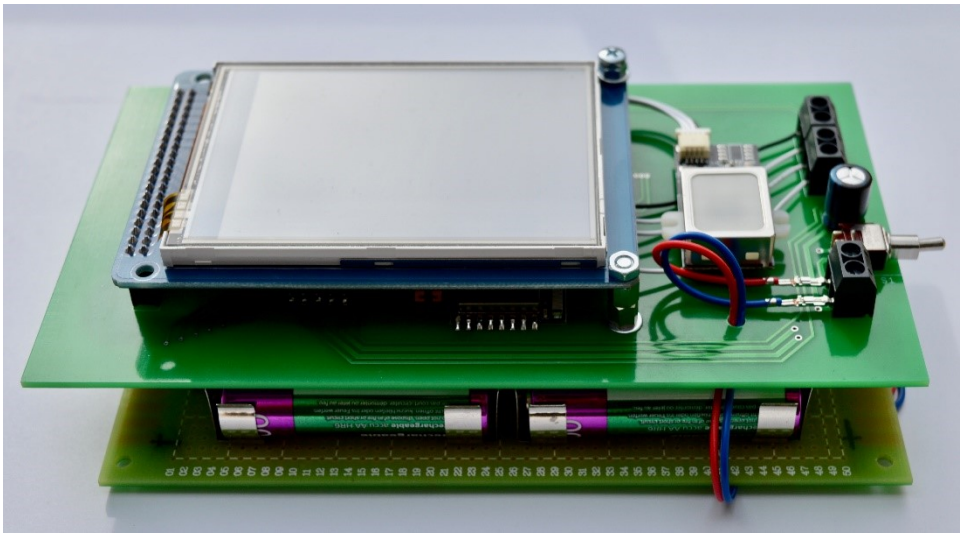
Druhou část finálního řešení představuje další DPS, které však slouží pouze pro montážní účely a nejsou na ní vytvořeny datové ani jiné plošné spoje. Svými materiálovými vlastnostmi (sklolaminát napuštění epoxidovou pryskyřicí – FR4) a rozměry jde o ideální prostředek pro upevnění řídící jednotky a zdroje napájení. Rozměry desky (10 x 15 cm) přesně pasují do konstrukční hliníkové krabičky a jejich vodících lišt. Ve fázi návrhu a výběru co možná nejlépe pasujících součástek bylo velice náročné spojit všechny prvky tak, aby velikost zařízení byla co nejmenší (vzhledem k přenosnosti), zdroj napájení měl dostatečně velkou kapacitu, ale zároveň nezaplňoval celý vnitřní prostor. Pro tyto důvody jsem umístil do prostřední části desky řídící jednotku upevněnou pomocí M3 šroubů a matic. Po obvodu jednotky a do zbývajícího prostorů jsem umístil šest akumulátoru s celkovým napětím 7,2V a kapacitou 2100 mAh. Zkoušel jsem zařízení testovat na sofistikovanějších akumulátorech typu Li-Pol, Li-Ion a jiné, nicméně svými rozměry, vhodným umístěním, přijatelnou cenou a proudovou kapacitou vyhovovali akumulátory s klasickým tvarem tužkových baterií. Díky jejich rovnoměrnému rozmístění na desce jsem mohl zvolit konstrukční krabičku s menšími rozměry což je pro tento typ zařízení žádoucí. Zdroj napájení je připojen pomocí dvou vodičů do svorkovnice umístěné na hlavní tedy první části zařízení. Obě desky jsou fyzicky spojené do jednoho celku, který je upevněn ve vnitřní části krabičky pomocí čtyř šroubů typu M3.



Obr. 34: Druhá část vestavěného zařízení obsahující řídící jednotku Arduino Due a zdroj napájení pro celý biometrický systém v podobě šesti akumulátorů s napětím 7,2V a kapacitou 2100 mAh.

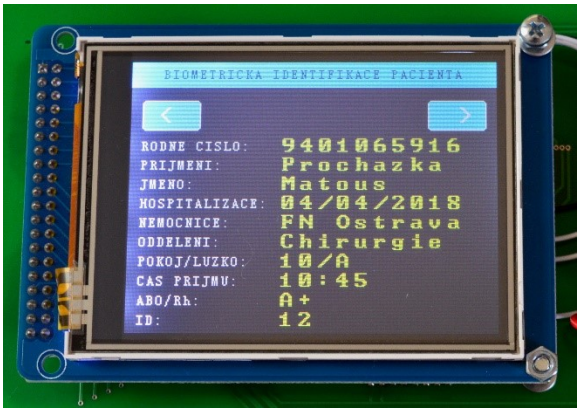
Uvedení vestavěného zařízení do provozu je uskutečněno pomocí dvoupolohového spínače na boční (pravé) straně konstrukční krabičky. Při přepnutí tlačítka do polohy „Zapnuto“ dojde k inicializaci displeje a grafického zobrazení výchozího menu. V tomto stádiu se zobrazí dvě velká dotyková tlačítka, která ovládají hlavní režimy pro identifikaci pacienta a případně offline registraci otisku prstu. V dolní části displeje je uživatel informován o stavu připojení vestavěného zařízení a především Wi-Fi modulu do lokální bezdrátové sítě nemocnice. V případě kompletního nastavení softwarové části (viz. kapitola 10.1) je za normálních podmínek zařízení připraveno na svou běžnou činnost. Tento status je indikován v podobě oznámení „Zařízení připojeno k síti“. Nyní již záleží, jaký další postup programu bude vybrán. Při zvolení prvního tlačítka je uživatel několika způsoby vyzýván k přiložení konečku prstu na snímací plochu senzoru. V prvním případě má pacient tři sekundy na to aby, přiložil prst na senzor. Tato výzva je graficky znázorněna v podobě časového odpočtu a textového oznámení. Pokud systém vyhodnotí, že šablona otisku byla identifikována s jinou totožnou šablonou, dojde ke stažení osobních údajů pacienta z databázového serveru do zařízení a následně jsou zobrazeny na displeji.

Získaná data jsou v definovaném formátu zobrazena na displeji. Jedná se o rodné číslo, příjmení a jméno pacienta, datum hospitalizace, název nemocnice (v níž je pacient umístěn), konkrétní oddělení, pokoj a lůžko, čas příjmu, krevní skupinu a ID číslo. Veškeré informace jsou jasně viditelné a písmo je z hlediska velikosti zvolené tak, aby bylo dobře čitelné. Pozadí je černé, barva označující typ informace je bílá a konkrétní text osobních dat je jasně žlutý. Další možností je zobrazení doplňujících údajů, které lze získat pomyslným přesunutím se na druhou stránku. Tento děj uživatel dosáhne tak, že zvolí tlačítko po pokračování režimu identifikace. Výsledkem je zobrazení doplňujících údajů jako je alergie na léky či potraviny, předepsané medikamenty (zabránění záměn při jejich užívání) a také informace o tom, zda má pacient implantovaný některý ze zdravotnických prostředků typu kardiostimulátor a kyčelní kloub. Z obecného pohledu je možné vytvořit několik stránek s různě důležitými informacemi, záleží pouze na tom, jaké údaje jsou pro dané oddělení podstatné. Velkou výhodou celého systému je schopnost listovat mezi jednotlivými stránkami a režimy s tím, že se uživatel může kdykoliv vrátit zpět do výchozího stavu a vykonávat opakovaně nové identifikační a registrační procesy. Zde se otevírá prostor pro eventuální vývoj, v němž by mohl být použit větší displej s vysokým rozlišením podobající se dnešním tabletům.



Obr. 35: Sestavení hardwarové části vestaveného zařízení včetně LCD displeje a senzoru otisků

Obr. 36: Výchozí stav grafického prostředí (Uživatelské menu systému – volba režimu)



*Obr. 37: Výsledek biometrické identifikace osoby (Zobrazení osobních informací v **online** režimu)*

Pokud je pomocí dotykového tlačítka zvolen druhý režim s názvem „Zápis pacienta“ je následně uživateli zobrazena jednoduchá numerická klávesnice, která slouží k vytvoření nové registrace otisku prstu a identifikačního čísla, s nímž se bude pacient po nezbytně nutnou dobu identifikovat. Jedná se o dočasné opatření, které má poskytnou alespoň částečnou identifikaci díky číselnému označení, než dojde ke kompletnímu doplnění základních osobních údajů. Tato funkce může být použita všude tam, kde je pacient hospitalizován v bezvědomí a nemá u sebe žádné osobní doklady, které by mohl personál použít při vytváření online registrace. Ve fázi offline registrace uživatel zvolí jedinečné ID číslo, které nemůže mít žádná další osoba a zahájí standardní proces pro zapsání biometrických údajů do databáze senzoru. V tomto případě se postupuje stejně jako při online registraci tedy, pacient je třikrát vyzván k přiložení konečku prstu na snímací plochu senzoru. Pokud vše proběhne korektně a systém vyhodnotí, že otisk je uložen v dostatečné kvalitě je uživatel graficky informován o úspěšném ukončení registračního procesu. Nyní je možné pacienta kdykoliv identifikovat stejně jako tomu bylo i v prvním případě, kdy uživatel zvolil režim „Kontrola pacienta“. Výsledkem identifikace je pak číslo, pod kterým byl pacient uložen. Při budoucím objasnění identity pacienta, může být vytvořena nová registrace již s kompletním zápisem všech důležitých osobních informací. Předešlá registrace se může odstranit a systém tak bude zobrazovat pouze nové informace, již v online režimu. Doplňující výhodou je opět možnost vrácení se do menu.

Obr. 38: Numerická klávesnice sloužící k offline registraci pacienta s neznámou identitou

*Obr. 39: Výsledek biometrické identifikace osoby (Zobrazení identifikačního čísla v **offline** režimu)*

Závěrečné sestavení vestavěného zařízení pro biometrickou identifikaci pacientů je zobrazeno na obrázku č. 40. Všechny hardwarové části jsou navzájem pevně spojeny a je připojen zdroj napájení. Tento celek je vložen do hliníkové konstrukční krabičky, která má pomocí CNC frézy precizně vyřezané otvory pro LCD displej, senzor otisku prstů a z boční strany také otvory na zapínací tlačítko a 2 dB Wi-Fi anténu. Anténa má zajistit kvalitnější bezdrátový přenos dat, než je k tomu určená integrovaná anténa na čipu modulu, která by jinak byla tlumena kovovou konstrukcí krabičky. Celé zařízení je navrženo tak aby se využilo veškeré volné místo v krabičce a zařízení tak bylo ve výsledku co možná nejmenší. Kryt krabičky spolu s vnitřní elektronikou tvoří jeden pevný celek, který je odolný především proti nárazům, každodennímu používání, prachu, vodě a také je dobře dezinfikovatelný, což je jeden z předpokladů při návrhu techniky a obecně přístrojů pro běžnou činnost ve zdravotnictví. Zařízení má rozměry 160 x 52 x 105 mm a jeho hmotnost včetně akumulátorů je 700 g. Cena všech částí by odpovídala přibližně 4600 Kč. Nejdražšími položkami jsou: řídící modul Arduino, senzor otisku prstů, výroba DPS, dotykový LCD displej, akumulátory, konstrukční krabička a ostatní elektronické a montážní díly. Je nutné podotknout, že zařízení v této fázi realizace není nijak certifikováno ani nenese označení CE, jde pouze o technický, avšak plně funkční prototyp, který dokáže vykonávat všechny naprogramované biometrické funkce.

Obr. 40: Hotové funkční řešení vestavěného zařízení pro biometrickou identifikaci pacientů. Na přední straně LCD dotykový displej se senzorem otisků, na boční straně Wi-Fi anténa.

10 SOFTWAROVÁ REALIZACE IDENTIFIKAČNÍHO SYSTÉMU

Následující kapitola se bude zabývat čistě softwarovou stránkou biometrického systému. Budou zde vysvětleny všechny identifikační a komunikační procesy, které probíhají mezi databází, bezdrátovou infrastrukturou nemocniční sítě, uživatelskou aplikací pro personál a samotným vestavěným zařízením. V případě komplikovaného systému jako je právě tento jsem musel vytvořit hned několik programových příkazů obsluhující naprosto rozdílné elektronické součástky. Složitost vzájemné spolupráce se zvýšila s nutností vytvořit software ve více než jednom programovacím a skriptovacím jazyce. Nejdůležitější a zároveň vývojově velmi náročný byl program pro vestavěné zařízení, řídící, identifikační a bezdrátové procesy. Druhým neméně důležitým vybavením je uživatelská aplikace určená výhradně pro pracovní počítače zdravotnického personálu. Ta byla vyvíjena v podobném programovacím jazyce, avšak v jiném prostředí. Posledními částmi tvořící pomyslný most mezi identifikačním zařízením a okolní bezdrátovou sítí jsou databázové SQL příkazy, AT software pro řízení Wi-Fi stacku, PHP scripty umožňující činnost HTTPS protokolu a mnoho dalších. Doplňující realizací bylo sestavení vlastní MySQL databáze na NAS serveru a nastavení statických tras na WLAN routeru spolu s šifrováním celého komunikačního okruhu.

10.1 KOMPLEXNÍ ALGORITMUS BIOMETRICKÉHO ZAŘÍZENÍ

Než se pustím do detailního líčení struktury programového vybavení zastavil bych se u krátkého popisu vývojového prostředí Arduino IDE (Integrated Development Environment). Jedná se o intuitivní open-source aplikaci, která je veřejně dostupná a umožňuje programovat veškeré desky od společnosti Arduino. V posledních několika letech získala na své oblibě především díky vývojovým platformám od jiných společností, zejména z prostředí IoT. Aktuální verze 1.8.5 podporuje více než dvacet oficiálních desek, přičemž další rychle přibývají. Je to zásluhou externích vývojářů, kteří programují nové knihovny pro více či méně složité systémy jako je Ethernet, Wi-Fi, LoRa, GPS, GPRS a mnoho dalších. Prostředí aplikace je rozděleno do několika sekcí. Je nutné podotknout, že Arduino IDE je velice zjednodušené a nelze jej jakkoliv srovnávat s komerčními platformami typu Visual nebo Atolic Studio. Hlavní a zároveň největší část tvoří textové okno, ve kterém jsou programovány kódy. Druhou částí je menší okno sloužící k informování programátora, zda vytvořený kód neobsahuje nějaké chyby, jakou velikost paměti SRAM a FLASH zahrnuje vlastní kód nebo informuje o stavu probíhajícího nahrávání. Poslední částí je horní tzv. editační panel umožňující provádět důležité operace s vytvořeným kódem. Při sestavování softwaru se bez tohoto panelu člověk neobejde. Obsahuje ovládací tlačítka pro kompilaci a kontrolu kódu, nahrání vlastního kódu do Arduina, dále pak tlačítka na vytvoření nového nebo otevření uloženého kódu.

Pokud je vytvořený kód kompletní a zkontrolovaný, zda neobsahuje zásadní programové chyby je možné jej pomocí tlačítka Upload nahrát do námi zvolené desky skrz předem definovaný počítačový port. Toto nastavení je nutné manuálně prověřit v nabídce Nástroje, ve které se nacházejí předvolby ke konkrétním deskám, procesorům a komunikačním portům. V oddílu pro vývojové desky je možné zvolit jednu z desítek vývojových platforem od vývojářů Arduino, Intel, Windows aj. Další oblastí jsou MCU, které lze opět nadefinovat ke konkrétní desce. Poslední nastavení se týká připojeného USB portu, který však ve většině případů není potřeba manuálně definovat. V případě mé konektivity jsem stanovil desku Arduino Due (Programming Port), mikrokontrolér na AT91SAM3X8E a port COM3. Doplňující funkcí aplikace je seriový monitor a ploter. Monitor slouží jako virtuální displej umožňující zobrazit sdělovací odezvy mikrokontroléru. Ploter naopak funguje jako osciloskop pro vykreslení analogového signálu.

Software pro vestavěné zařízení je kompletně napsán v jazyce C, respektive jazyce Wiring, což je zjednodušená forma jazyka C upravena přímo pro vývojové desky Arduino a jiné podobné platformy. Funkce a příkazy psané v syntaxi Wiring umožňují jinak příliš složitý a dlouhý kód zapsat zjednodušeně v pouze několika málo řádcích vyjadřující totožnou podstatu kódu. Tato výhoda se uplatní při nahrávání programu do flash paměti mikrokontroléru. Na rozdíl od klasického kódu psaném v jazyce C obsazuje takovýto program jen zlomek paměti. Právě díky možnosti vyvářet programy v jazyce Wiring se staly jednoduché mikrokontroléry od firmy Atmel ve spojení s deskami Arduino tolik populární. Hlavní část programu se skládá ze dvou nezbytných funkcí, a to *void setup()* v niž se nastavuje počáteční inicializace kódu a *void loop()* obsahující primární úsek kódu, u něhož chceme, aby se nekonečně opakoval.

Nyní bych přistoupil ke konkrétnímu popisu všech důležitých oblastí mého softwaru. Vzhledem ke skutečnosti, že celý kód zahrnuje více než tisíc řádků různých funkcí, deklarací a síťových příkazů, není možné zde celý script detailně vypsat a vysvětlit. Rozdělím tedy kód na jednotlivé bloky, ve kterých popíšu, co každý vykonává a jaký má vliv na ostatní části v programu. Ve výchozím bloku se zaměřím na samotnou inicializaci zařízení. Začátek kódu tvoří deklarování tři knihoven. První knihovna se věnuje definici řídících procesů optického senzoru otisku prstu, tím jsou myšleny funkce určené k biometrické operaci během zpracování otisku prstu. Díky této knihovně, která je dostupná od výrobce mohu senzor ovládat podle svých potřeb. Druhá knihovna charakterizuje konektivitu a zpracování obrazových dat na LCD displeji. Poslední knihovna umožňuje hodnotit informace z dotykové vrstvy displeje a tím i řídit doplňující funkce v kódu. Následují dvě definice hardwarových portů k připojení sériové komunikace s deskou Arduino Due. Port *Serial3* připojuje bezdrátový Wi-Fi modul a *Serial2* senzor otisků. Dalších několik proměnných definuje síťové spojení, velikost grafických obrazců, styly písma a jeho souřadnice na displeji nebo také konkrétní datové piny pro SPI komunikaci mezi řídící deskou a displejem.

```
#include "FPS_GT511C3.h"
#include <UTFT.h>
#include <URTouch.h>
#define ESP8266 Serial3
#define FPS Serial2

String SSID = "Nazev_site";
String PASSWORD = "Heslo_1234";
boolean FAIL_8266 = false;
char currentPage;
int x, y;
int id;
String w;
String delete_id;
extern uint8_t BigFont [];
extern uint8_t SmallFont [];
extern uint8_t SevenSegNumFont [];
char stCurrent [20] ="";
int stCurrentLen=0;
char stLast [20] ="";

FPS_GT511C3 fps;
UTFT myGLCD(ITDB32S,38,39,40,41);
URTouch myTouch (7,6,5,4,3);
```

Druhý blok kódu reprezentuje konfigurační příkazy potřebné ke správné funkčnosti vestavěného zařízení. Mezi tyto příkazy patří počáteční procesy programu, které spouštějí algoritmy pro uživatelské rozhraní, identifikaci pacienta a navazují komunikační přenos dat mezi všemi připojenými periferiemi. V první řadě jsou inicializovány hlavní prvky displeje, je nastaveno datové spojení, velikost a typ písma, je zahájeno čtení informací z dotykové vrstvy displeje spolu s nastavením citlivosti. Dále následují dvě funkce přerušení. První se nazývá *drawHomeScreen()* a při jejím vyvolání dojde k zobrazení grafického menu na displeji. Zde si například zdravotnický personál může vybrat, jestli bude pacient identifikován nebo registrován. Druhá funkce přerušení *loadSetup()* indikuje stav připojení zařízení k bezdrátové síti. Po této části následuje cyklus do-while v rámci něhož se vytvoří praktické spojení řídící desky s Wi-Fi modulem a senzorem otisku prstů. Na začátku se nastaví sériová komunikace mezi řídící jednotkou a periferiemi pomocí pomyslného handshakingu na rychlost 115200 a 9600 bitů za sekundu. V tuto chvíli je možně s Wi-Fi modulem a senzorem otisku prstů komunikovat a ovládat jej. Dalších několik řádků je soustředěno čistě na konfiguraci síťových parametrů jako je restartování modulu, přihlášení k vybrané

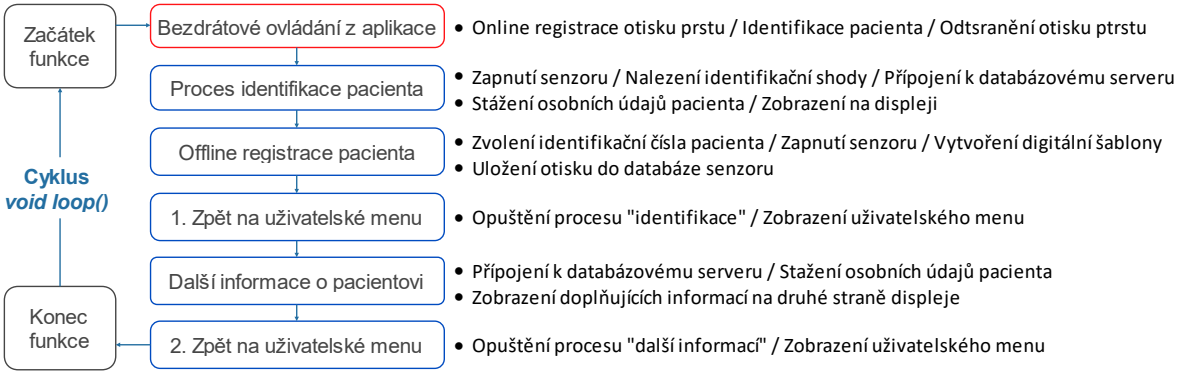
IP adrese přístupového bodu, obdržení nové IP adresy od DHCP serveru a připojení na webový server přes port 80. Poté co je řídící struktura úspěšně dokončena a bezdrátový modul je připojen k síti zbývá spustit senzor otisku prstů pomocí příkazu *fps.Open()*. Pokud všechno proběhne správně a každé zařízení je schopné komunikovat s řídící deskou, je celý inicializační proces u konce a v dalších krocích už záleží pouze na uživateli jakou bude vyžadovat funkci od systému. Jestliže zařízení není připraveno vykonávat svou standardní činnost, v tomto případě identifikovat pacienta v online režimu nebo jej registrovat do databáze pacientů, je o tomto chybném stavu uživatel informován prostřednictvím grafického oznámení na displeji. Nejčastěji se může jednat o chybu spojení s databázovým serverem nebo slabý signál.

```
void setup() {
  fps.UseSerialDebug = true;
  randomSeed(analogRead(0));
  myGLCD.InitLCD();
  myGLCD.setFont(BigFont);
  myTouch.InitTouch();
  myTouch.setPrecision(PREC_MEDIUM);
  drawHomeScreen();
  loadSetup();
  currentPage = '0';
  do{
    Serial.begin(115200);
    ESP8266.begin(115200);
    FPS.begin(9600);
    while(!Serial);
    ESP8266.println("AT+RST");
    if(ESP8266.find("OK"))
    {
      ESP8266.println("AT+CWMODE=1");
      delay(500);
      ESP8266.println("AT+CWQAP");
      delay(500);
      clearESP8266SerialBuffer();
      if(cwJoinAP())
      {
        FAIL_8266 = false;
        clearESP8266SerialBuffer();
        sendESP8266Cmdln("AT+CIFSR", 200);
        sendESP8266Cmdln("AT+CIPMUX=1", 200);
        sendESP8266Cmdln("AT+CIPSERVER=1,80", 200);
      }
      else{
      FAIL_8266 = true;
      }
    }
    else{
    FAIL_8266 = true;
    }
  }
  while(FAIL_8266);
  fps.Open();
  fps.SetLED(false);
  connectedSetup();
}
```

Třetí blok kódu tvoří zásadní část celého programu a je zaměřen na funkci, která je vykonávána v nekonečných cyklech, dokud není vyvoláno určité přerušení. Vzhledem k faktu, že tato část má několik stovek řádků, vysvětlím její princip na blokovém schématu, kde každý jednotlivý blok bude znázorňovat část charakteristické funkce. Nejdůležitější je cyklus *void loop()*, ten zahrnuje 6 hlavních podmínek *if*, které jsou neustále kontrolovány, zda platí nebo ne. Pokud není ani jedna podmínka splněna zařízení se bude chovat tak, jako by bylo v režimu spánku a čeká na rozhodnutí od uživatele jakou akci (přerušení) vyvolá. První podmínka se týká interakce mezi vestavěným zařízením a uživatelskou aplikací umístěnou na pracovní stanici zdravotnického personálu. Tato podmínka hlídá, zda uživatel vyvolal určitou aktivitu v rámci aplikace. Pokud například zdravotní sestra bude chtít registrovat nového pacienta a uložit jeho otisk prstu do databáze, musí zvolit režim snímání otisku. Tento příkaz je vyvolán pomocí stisku tlačítka a poslán přes nemocniční síť k příslušnému AP, který informace dále přepošle k cílovému zařízení kde se příkaz zpracuje a vyhodnotí. Takto je možné bezdrátově ovládat veškeré funkce vestavěného zařízení a přes HTTPS protokol vybírat mezi procesem identifikace, ukládáním nebo odstraňováním otisků prstů.

Druhá podmínka (spolu se všemi zbývajícími) se týká pouze vestavěného zařízení a uživatelské nabídky režimů zobrazené na dotykovém displeji. To znamená, že všechny následující podmínky mohou být uskutečněny pouze pokud uživatel stiskne určité tlačítko, které vyvolá specifickou reakci. Jestliže je tato první podmínka splněna a dotyková vrstva displeje zaregistruje kontakt prstu na předem definované ploše, může být zahájena biometrická identifikace pacienta. Proces identifikace byl několikrát vysvětlen v předchozích kapitolách, proto jej popíšu ve zkrácené formě. Na začátku identifikační funkce je zapnut senzor otisků prstů a jsou rozsvíceny pomocné diody. Následuje kontrola přiložení prstu na snímací část

tedy fyzický kontakt pokožky se senzorem. Poté následuje složitý algoritmus extrakce markantních bodů z papilárních linií a sestavování virtuální šablony. Ta je následně porovnávána se všemi ostatními otisky v interní databázi senzoru. Pokud je nalezena shoda, funkce odpoví unikátním číslem, které specifikuje konkrétní otisk prstu, a tedy i pacienta. Toto číslo se dále využije při kontaktu s databází a podle něj se vyhledají příslušné pacientské informace. Soubor těchto dat je zpětně odeslán přes interní síť nemocnice k bezdrátovému vysílači, ten vykoná poslední krok přenosu a poskytne informace vestavěnému zařízení. V něm se zdravotnické informace sestaví do vyhovující grafické podoby a zobrazí se na displej.

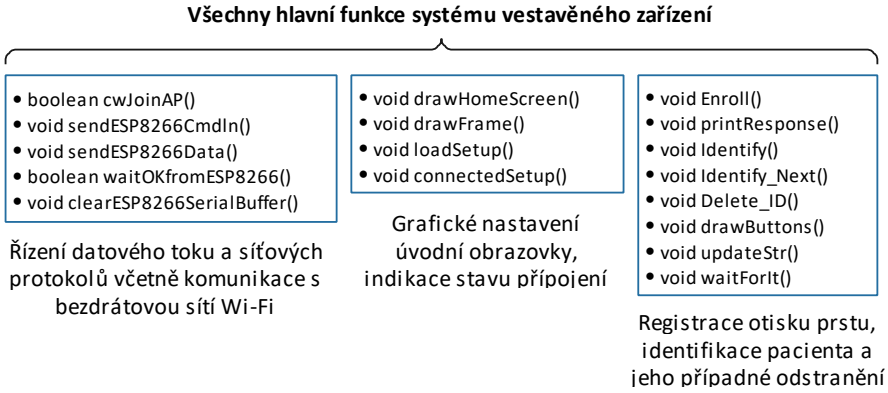


Obr. 41: Blokové schéma hlavního cyklu void loop() v operačním programu pro vestavěné zařízení

Třetí podmínka v cyklu *void loop()* ovládá úlohu umožňující registraci nově příchozího pacienta do identifikační databáze, avšak aniž by kdokoliv věděl jeho přesnou totožnost. Tento děj je typický pro urgentní příjmy, kde může být hospitalizován pacient v bezvědomí a nejsou o něm vedeny žádné zápisy. Vyvolání úlohy je opět podmíněno zvolením uživatelského režimu, a to pomocí tlačítka na dotykovém panelu displeje. Následně se zvolí nové a unikátní číslo pacienta, které bude v dalších úkonech zdravotní péče sloužit jako jednoznačný marker. Konkrétní číslo zvolí personál na numerické klávesnici přímo na displeji a potvrdí jej. Systém automaticky zkontroluje, zda vytvořené číslo nebylo použito v předchozích registracích a pokud nikoli, pokračuje stejně jako tomu bylo při online registraci. V průběhu identifikace se pacient prokazuje pod přiděleným identifikačním číslem a pokud jsou známy nové osobní informace, je žádoucí, aby byl registrován v plnohodnotném režimu se všemi doplňujícími informacemi.

Čtvrtá a šestá podmínka má v principu podobný základ, obě sjednocují stejné výsledky přerušení nicméně každá je využita v rozdílných situacích. Podmínka je vykonána, jestliže je stisknuta specifická klávesa na displeji, která v konečném důsledku zastaví stávající proces a vrátí uživatelské rozhraní do výchozího stavu, tedy do výběrového menu vestavěného zařízení. V prvním případě podmínka ukončuje proces identifikace a ve druhém režim s doplněnými informacemi o pacientovi. Z praktického hlediska jsou tyto funkce velice důležité, jelikož umožňují uživatelům kontinuální činnost systému bez nutnosti jej restartovat. Zbývající pátá podmínka představuje doplňkovou funkci biometrického systému a může personálu pomoci během bezpečnostních kontrol pacienta například před operací či podáním léčiv. Při vyžádání doplňujících dat z databáze pacientů je inicializováno nové bezdrátové připojení k nemocniční síti, do níž je odeslán HTTPS Request na databázový server, který zpětně odešle požadované informace odpovídající konkrétnímu pacientovi. Přijaté informace se stejně jako u klasické identifikace zpracují, seřadí a zobrazí v optimální formě na LCD displej. Všechny tyto podmínky jsou neustále kontrolovány, zda byly vyvolány nebo nikoliv. Celý program obsahuje dalších několik set řádků, v nichž jsou umístěny konkrétní komunikační funkce a operační procesy. Z detailního hlediska není možné přesně vysvětlit co

jaký odstavec či řádek kódu způsobuje. Pokusím se alespoň částečně vysvětlit jejich hlavní podstatu a v následujících odstavcích popsat co každá funkce obnáší. Jednotlivé úlohy jsem rozdělil do tří částí, kde každá vystihuje odlišný význam v rámci kódu. První část je zaměřena čistě na nastavení komunikačních protokolů a vytvoření spojení mezi Wi-Fi modulem ESP-07 a nejbližší dostupnou bezdrátovou sítí, která je lokálně připojena k databázovému serveru. Za počáteční připojení je zodpovědná funkce *cwJoinAP()*, která pomocí přihlašovacího SSID jména a síťového hesla vytvoří spojení s přístupovým bodem. Dalším krokem je funkce *void sendESP8266Cmdln()*, ta pomocí přesně definovaného procesu odesílá příslušné dotazy k serveru a zároveň je schopna řídit datový tok informací. Podobným komunikačním bodem je *void sendESP8266Data(),* ten však do modulu odesílá specifický typ dat v syntaxi print() místo println(). Mezi jednotlivými kroky komunikace musí probíhat časová pauza, aby nedocházelo k překrývání zpráv nebo špatnému doručení. Tuto prodlevu zajišťuje *boolean waitOKfromESP8266(),* který čeká na zprávu „OK“ od Wi-Fi modulu, že může přijímat či odesílat další data. Doplňkovou funkcí komunikační části je *void clearESP8266SerialBuffer(),* ta si průběžně do paměti (Bufferu) řídící jednotky ukládá příchozí informace od Wi-Fi modulu a umožňuje je zobrazit v sériovém monitoru. Jde o zásadní zpětnou kontrolu komunikačního procesu, při němž lze sledovat, zda příkazy a data jsou odesílány ve správné podobě. Je důležité poznamenat, že výše popsané funkce první části se týkají pouze komunikačního procesu, který probíhá mezi uživatelskou aplikací pro správu pacientských dat a vestavěným zařízením. Datové spojení mezi zařízením a NAS serverem v rámci identifikace, registrace a editace probíhá v jiném nastavení.



Obr. 42: Seznam všech důležitých funkcí obsažených v programu vestavěného zařízení

Druhou část tvoří grafická úprava uživatelského prostředí. Hlavní funkcí definující jednoznačné rozložení jednotlivých vizuálních prvků na displeji je *void drawHomeScreen().* Její součástí jsou příkazy pro nastavení barvy pozadí, tvaru a rozložení dotykových tlačítek, jejich textový popis včetně umístění, typ a velikost písma. Inicializace těchto příkazů je vyžadována vždy, když se uživatel vrací do výchozího stavu systému. Na tuto funkci navazuje další s názvem *void drawFrame().* Jedná se o grafickou úpravu tlačítek ve tvaru obdélníku, které se při stisknutím zvýrazní a vytvoří tenký rámeček signalizující činnost tlačítka. Poslední dvě funkce *void loadSetup()* a *void connectedSetup()* tvoří velice krátké příkazy, které slouží k jednoznačnému informovaní uživatele, zda vestavěné zařízení je připojeno k místní bezdrátové síti a je tak schopno vykonávat všechny identifikační a jiné činnosti nebo není. Z obecného hlediska se jedná o textové indikátory umístěné mezi začátkem konfiguračního úseku řídící jednotky (*void setup()*) a jejím ukončením. Po zapnutí přístroje se v dolní části displeje zobrazí oznámení „Připojování k síti“. Poté co jsou nastaveny všechny parametry Wi-Fi modulu, zobrazí se v zelené barvě zpráva „Zařízení je připojeno v síti“. Tím je ukončena počáteční inicializace a záleží na uživateli jaký další krok udělá.

Třetí a současně poslední část tvoří všechny ostatní funkce, které zajišťují kvalitní identifikační a registrační proces pacienta nebo také správu jeho osobních informací. Mezi hlavní funkce jednoznačně patří *void Enroll().* Jedná se o online zápis biometrických šablon otisků do paměti senzoru a je zahájen skrz uživatelskou aplikaci z externího počítače. Při vyvolání dojde k třífázovém skenování otisku, vždy z jiné pozice prstu na snímací ploše. Poté co byl otisk uložen do databáze senzoru je uživatel informován, zda celkový proces proběhl korektně a následně je systém vrácen do své výchozí pozice, kde může být zahájeno nové snímání nebo identifikace. V této fázi registrace se identifikační číslo otisku zadává ještě před snímáním, a to přímo ve vyhrazené kolonce uživatelské aplikace. Toto číslo se bezdrátově odesílá spolu s řídícím požadavkem do řídící jednotky a dále do senzoru. Další nedílnou součástí je funkce *void Identify()*.Jde o poměrně složitý úsek programu. Při jejím spuštění dojde k inicializaci senzoru a vyčkává se, než je struktura pokožky prstu zachycena na snímací ploše. V dalším kroku je zahájen algoritmus na extrakci markantních bodů a jejich porovnání se všemi dříve uloženými šablonami otisků. Výsledkem je zamítnutí identifikace nebo její přijmutí s tím, že algoritmus odpoví příslušným identifikačním číslem, které je použito ke komunikaci s databázovým serverem. Komunikace je opět vedena přes Wi-Fi modul, který se pomocí SQL příkazů dotazuje na konkrétní pacientské informace. Ty jsou mu vydány a následně přeposlány zpět do řídící jednotky, kde se v předdefinovaném formátu zobrazí na displeji.

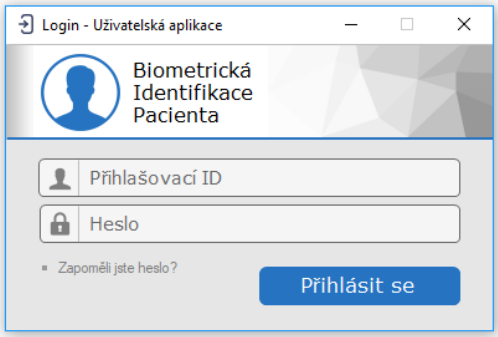
Pokud je potřeba pacienta s jeho osobními údaji a otiskem prstu z databáze odstranit je to možné vykonat pouze v uživatelské aplikaci. V ní se uvede identifikační číslo pacienta, které má být odstraněno a pomocí funkce *void Delete_ID()* se tak provede. Z bezpečnostního hlediska jsem nenastavil funkci pro vymazání všech otisků a osobních údajů najednou ačkoliv senzor tuto možnost poskytuje. Poslední kódy jako *void drawButtons()*, *void updateStr()* a *void waitForIt()* jsou použity pro offline registraci pacienta, a především na zobrazení numerické klávesnice na displeji, díky níž lze manuálně nastavit identifikační číslo přímo ve vestavěném zařízení. To pak po nezbytně nutnou dobu slouží jako jediný nástroj identity.

10.2 UŽIVATELSKÁ APLIKACE PRO SPRÁVU PACIENTSKÝCH DAT

Součástí softwarové realizace identifikačního systému je také počítačová aplikace pro pracovní stanice zdravotnického personálu, která slouží ke správě osobních informací pacienta a jeho otisku prstu. Aplikace je určena pouze pro operační systémy Windows a není třeba ji instalovat. Samotnou realizaci jsem vytvářel v jazyce C++, resp. Visual C++ v prostředí Microsoft Visual Studio. Celkové programové vybavení zahrnuje přibližně 3500 řádků a je rozděleno na tři celky. Nejkratší je hlavní funkce *Main.cpp*, která pouze definuje použité knihovny a zahajuje spuštění přihlašovacího okna aplikace. Druhou funkci tvoří hlavičková část s názvem *Login.h*, v níž je přesně stanoven grafický vzhled přihlašovací obrazovky a také dotazovací SQL příkazy potřebné ke kontrole oprávněných uživatelů, kteří jsou vedeni v oddělené tabulce MySQL databáze. Pouze tyto osoby mohou vykonávat administrativu obsahu databáze pacientů. Třetí a největší částí je hlavičkový soubor s názvem *Personal.h.* Ten zajišťuje klíčové fungování celé aplikace. Obsahuje veškeré funkce pro ovládání tlačítek, textových polí, informačních bloků, připojení k databázovému serveru a samozřejmě bezdrátové konektivity s vestavěným zařízením.

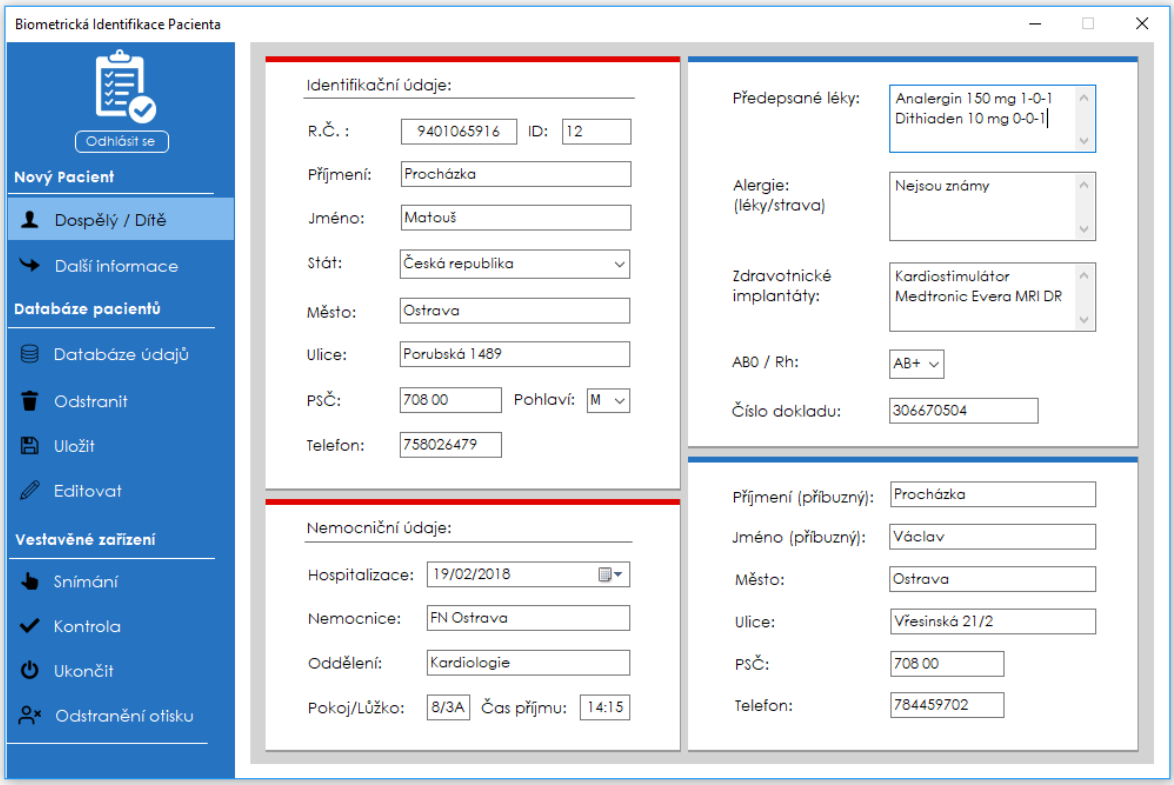
Při spuštění aplikace je v první fázi zobrazeno malé přihlašovací okno, do kterého musí personál zadat své přidělené přihlašovací jméno a heslo. Neoprávněná osoba s chybnými údaji nebude vpuštěna dále do hlavní části aplikace. Poté co se systém připojí na server a zkontroluje, zda všechny přihlašovací údaje odpovídají registrovanému uživateli, je automaticky zobrazeno editační rozhraní aplikace. Jestliže uživatel potřebuje odejít, odhlásí se a uvede aplikaci do výchozího stavu, ze kterého je možné opětovně

se přihlásit. Hlavní část aplikace je tvořena velkou informační a registrační textovou plochou rozdělenou na čtyři grafické bloky zaměřené na charakter a významnost osobních dat každého pacienta. K této ploše je připojen boční panel funkcí, který slouží k výběru specifických činností vázaných na správu osobních informací pacienta a řízení bezdrátového přenosu dat mezi aplikací a zařízením. Tento panel je rozdělen na tři tematické skupiny. První s označením „*Nový pacient*“ obsahuje dvě verze registračního formuláře, které se volí stiskem příslušného tlačítka na panelu. Uživatel se může rozhodnout jednak pro vytvoření plnohodnotného formuláře, do kterého se zapisují jak nejnutnější, tak i doplňující osobní údaje pacienta nebo eventuálně pokud je jedná o novorozence tak můžou být doplněny i jeho osobní/porodní údaje jako je datum, čas, místo narození (nemocnice), jméno a příjmení matky a otce případně další informace typu porodní váha a délka. Červeně zvýrazněné pole znázorňuje nejdůležitější informace, které musí být vždy vyplněny a zároveň musí nutně obsahovat rodné číslo nebo jiný zákonný identifikátor. Zatímco modře zvýrazněné pole charakterizuje dobrovolné nebo také méně klíčové informace, které nemusí být nutně zapsány. Poté co je registrační formulář vyplněn se uživatel přepojí do třetí skupiny „*Vestavěné zařízení*“ a zvolí tlačítko *Snímání*, tím se zahájí fyzický proces registrace otisku prstu. Ukončením záznamu otisku je pacient uložen v databázi a je možné jej kdykoliv plnohodnotně identifikovat. V rámci výše popsané skupiny je také možně realizovat bezdrátovou identifikaci nebo odstranění konkrétní šablony otisku z databáze senzoru. Poslední funkci ovládá tlačítko *Ukončit*, které je schopné přerušit aktuálně probíhající činnost na vestavěném zařízení a vrátit program do výchozího stavu, z něhož lze opět volit nový režim.

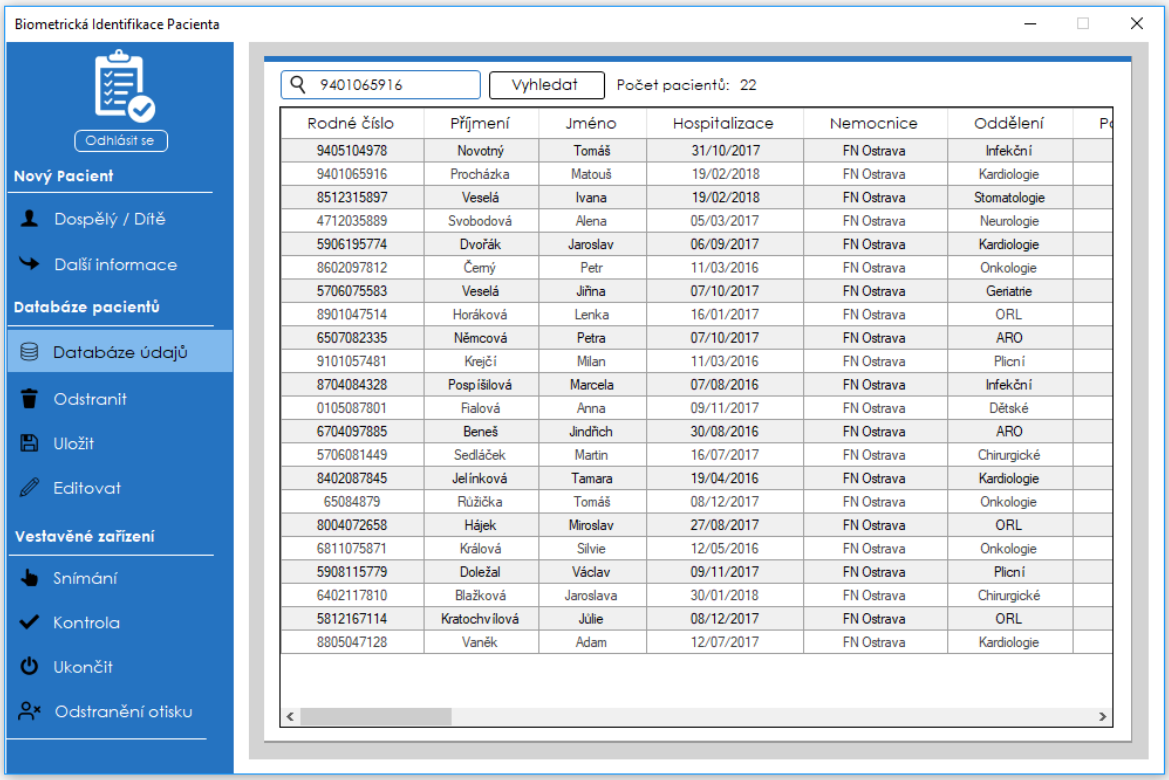


Obr. 43: Přihlašovací náhled do uživatelské aplikace umožňující zdravotnickému personálu editovat pacientské informace a bezdrátově ovládat vestavěné zařízení pro biometrickou identifikaci.

Druhá (prostřední) skupina funkcí bočního panelu je zaměřena na editační činnost. V první řadě slouží k nahlížení do celé databáze pacientů a úpravě stávajících informací pacienta. Při zvolení tlačítka *Databáze pacientů* je zobrazena tabulka se všemi uloženými pacienty, v níž je možné listovat a prohlížet si jejich údaje. K vyhledávání konkrétního pacienta slouží textové pole, díky kterému je možné filtrovat ostatní pacienty, kteří nás v danou chvíli nezajímají. Do vyhledávače lze zadat jednak celé rodné číslo, příjmení nebo také jeho část. Výsledkem je poté buďto zobrazení hledaného pacienta případně několika pacientů s podobným příjmením nebo začátkem rodného čísla. Další funkcí aplikace je částečná úprava či celková změna stávajících údajů pacienta. K tomuto účelu slouží tlačítko *Editovat* reagující pouze na rodné číslo vložené do vyhledávače. Pokud systém vyhodnotí, že v databázi existuje pacient s uvedeným rodným číslem, automaticky uživatele přesune na výchozí stránku a zobrazí vyplněný formulář se všemi dříve uloženými údaji. Následně lze v libovolné míře informace přepisovat a měnit. Zpětný zápis údajů se provede pomocí tlačítka *Uložit*. Tím se aktualizuje příslušný řádek v tabulce uložené na databázovém serveru. Jestliže již pacienta nechceme mít uloženého v databázi, lze jednoduchým způsobem všechny jeho osobní informace vymazat, a to pomocí tlačítka *Odstranit*, opět reagující na úplné rodné číslo.



Obr. 44: Hlavní náhled do editační a ovládací části uživatelské aplikace. (Červené pole označuje podstatné informace, které by měly být vždy vyplněny. Modré pole tvoří doplňující informace)



Obr. 45: Příklad náhledu do databáze všech registrovaných pacientů v rámci jedné nemocnice. V horní části tabulky se nachází vyhledávací textové pole a aktuální počet uložených pacientů.

10.3 SCRIPT UMOŽŇUJÍCÍ KOMUNIKACI S DATABÁZÍ PACIENTŮ

Jednou z důležitých softwarových součástí komunikačního spojení mezi databází a vestavěným zařízením je PHP script, který umožňuje stažení identifikačních informací pacienta ze serveru a následné konverze do speciálního formátu (String) pro přenos datovou sítí. Ve skutečnosti se Wi-Fi modul ESP07 nepřipojuje přímo k databázi pacientů ale na soubor *mysqli.php*. Ten je schopen si pomocí SQL příkazů vyžádat konkrétní data odpovídající identifikačnímu číslu pacienta. Toto unikátní číslo je stanoveno při úspěšné biometrické identifikace a odesílá se přes HTTPS příkaz právě do PHP souboru. Script je složen ze čtyř na sebe navazujících částí. Jak už je patrné celý kód je napsán ve skriptovacím jazyce PHP, který je určený pro vytváření dynamických internetových stránek a webových aplikací. Velkou výhodou PHP je podpora mnoha knihoven a síťových protokolů umožňující přístup k databázovým systémům jako je právě MySQL, kterou využívám se spojení s webovou aplikací phpMyAdmin. Z vestavěného zařízení na server se systém připojuje pomocí níže uvedeného kódu umístěného v části identifikačního procesu. Jde o GET Request, kterým je server tázán na data uložená v jeho databázi.

```
String cmd = "GET /mysqli.php?id=";
cmd += id;
cmd += "HTTP/1.1\r\nHost:192.168.0.10\r\nConection:close\r\n\r\n\r\n";
ESP8266.println("AT+CIPSEND=4," + String(cmd.length()+4));
```

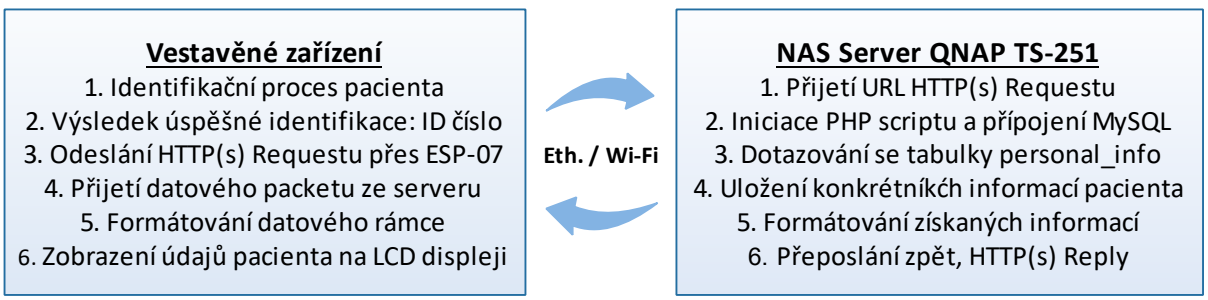
V první částí PHP scriptu jsou definovány proměnné databázového připojení, tedy jak se server jmenuje (root), na jakém portu je připojen (v tomto případě jde o port 3306 představující MySQL), jaké je heslo pro vstup do databázových tabulek a v poslední řadě, ke které tabulce má vytvářet SQL příkazy. V dalších řádcích je uskutečněno samotné připojení za použití všech výše uvedených definic. Vzhledem k tomu, že databáze obsahuje česká slova s diakritikou, bylo nutné nastavit výchozí kódování znaků na UTF-8. Druhou částí je procedura, z níž je staženo identifikační číslo pacienta, potřebné pro následující činnosti příkazů v databázi. Jestliže server obdrží konkrétní číslo, může začít SQL dotazování na tabulce *personal_info*. Jsou vyhledávány předem vybrané nejdůležitější informace, které budou zobrazeny jako praktický výsledek procesu identifikace na první stránce displeje vestavěného zařízení. Mezi tyto údaje je zařazeno rodné číslo, příjmení, jméno, hospitalizace, nemocnice, oddělení, pokoj/lůžko a čas příjmu. Výsledek nalezených dat je uložen do proměnné *result*, s níž se bude v dalších krocích pracovat.

```
<? php
$servername = "qnap-server:3306";
$username = "root";
$password = "Password1234";
$dbname = "personal";

$conn = mysqli_connect ($servername, $username, $password, $dbname);
if (! $conn)
{
        die ('Failed to connect to MySQL:‘. mysqli_connect_error ());
}
mysqli_query ($conn,"SET CHARACTER SET 'utf8'");
$id = $conn-> real_escape_string($_GET['id']);
$sql = "SELECT `Rodne cislo`, Prijmeni, Jmeno, Hospitalizace, Nemocnice, Oddeleni, `Pokoj/Luzko`, `Cas prijmu`,
`AB0/Rh` FROM personal. personal_info WHERE ID='$id'";
$result = mysqli_query ($conn, $sql);
$prevodni_tabulka = Array (
'á'=>'a',
(...)    // všechny písmena české abecedy s diakritikou
'Ž'=>'Z',
);
```

Třetí část obsahuje převodní tabulku znaků, kterou jsem použil pro odstranění české diakritiky, a to z důvodu špatné nebo žádné podpory těchto znaků na LCD displeji. Zkoušel jsem vytvořit knihovnu s vlastní sadou znaků, kterou by displej podporoval, nicméně po dlouhém testování jsem došel k závěru, že tato knihovna nebude realizovatelná, protože řadič displeje zobrazuje výlučně prvních 128 znaků z ASCII tabulky. Čtvrtá a poslední část PHP scriptu ukládá a seřazuje nalezené informace z databáze do jednoho řádku. Tato část scriptu je velmi důležitá. Z testování jsem zjistil, že Wi-Fi modul a celý systém neumí zpracovat několika řádkovou tabulku a poslat ji v původní podobě skrz síť. Proto jsem výsledky převedl do jednoho řádku začínající hvězdičkou a konče středníkem, navíc každý nalezený řádek je také oddělen středníkem. Ve výsledku je do vestavěného zařízení odeslán dlouhý řetězec informací. Na konci přenosu jsou příchozí informace detekovány díky hvězdičce a každá další soustava znaků je převedena do proměnné a zobrazena v odpovídajícím formátu na displeji. Pro převedení nalezených informací jsem použil mysqli příkaz *mysqli_fetch_array*, který převádí veškeré znaky do jednoho řádku. Na konci kódu je ukončovací příkaz *mysqli_close($conn)*, který uzavře spojení se serverem a databází pacientů.

```
while ($row = mysqli_fetch_array($result))
{
	echo "*";
	echo $row ["0"];
	echo ";";
	$prijmeni = strtr ($row ["1"], $prevodni_tabulka);
	echo $prijmeni;
	echo ";";
	$jmeno = strtr ($row ["2"], $prevodni_tabulka);
	echo $jmeno;
	echo ";";
	$hospitalizace = strtr ($row ["3"], $prevodni_tabulka);
	echo $hospitalizace;
	echo ";";
	$nemocnice = strtr ($row ["4"], $prevodni_tabulka);
	echo $nemocnice;
	echo ";";
	$oddeleni = strtr ($row ["5"], $prevodni_tabulka);
	echo $oddeleni;
	echo ";";
	$pokojluzko = strtr ($row ["6"], $prevodni_tabulka);
	echo $pokojluzko;
	echo ";";
	$prijem = strtr ($row ["7"], $prevodni_tabulka);
	echo $prijem;
	echo ";";
	$ab0 = strtr ($row ["8"], $prevodni_tabulka);
	echo $ab0;
	echo ";";
}
mysqli_close($conn);
?>
```



Obr. 46: Ukázka jednotlivých procesních kroků při komunikaci s databázovým serverem

11 PRAKTICKÉ SROVNÁNÍ S IDENTIFIKAČNÍMI METODAMI

V této kapitole se zaměřuji zejména na technické, softwarové, bezpečnostní a funkční porovnání mnou vytvořeného vestavěného zařízení s aktuálně nejčastěji používanými identifikačními metodami v nemocničních zařízeních. Ve druhé částí budu popisovat hlavní praktické výhody a nevýhody s již dříve vytvořeným zjednodušeným prototypovým zařízením, které sloužilo jako budoucí předloha pro vývoj modernějšího, sofistikovanějšího a zároveň pro pacienta bezpečnějšího zařízení. V první řadě je potřeba si uvědomit jaké techniky se v současné době používají. V České republice je v praxi nejvíce zastoupen zápěstní náramek, který musí zdravotní sestra ručně vyplňovat. Tyto náramky slouží jako základní prvek identifikace, avšak mají velkou řadu nevýhod. Jednou z nich je značně omezující prostor pro zapsání identifikačních osobních údajů pacienta. Gumový jednorázový náramek umožňuje ručně vyplnit pouze několik málo údajů jako je jméno, příjmení, název oddělení, datum narození nebo také zda pacient netrpí některými alergiemi či vadami chůze a prostorovou orientací. Obecnou nevýhodou náramků je jejich fyzická přítomnost. To znamená, že aby náramek splňoval určitou funkčnost, je nutné jej mít neustále umístěný na zápěstí. Tato skutečnost však zavádí potenciální riziko ztráty či zničení náramku a tím i znemožnění případné kontroly pacienta. Jedinou výhodou těchto náramků oproti jiným technologicky náročnějším metodám je jejich nízká pořizovací cena (v průměru 3,50 Kč/ks) a jednoduchá aplikace.

Druhou variantou jsou opět zápěstní náramky, nově však s použitím čtečky čárových kódů nebo RFID čipu umístěném v pouzdře náramku. Tato metoda spočívá v implementací identifikačního procesu připojeného do nemocničního informačního systému. V zásadě se jedná o modernizaci stávajícího řešení a rozšíření možnosti zobrazit si detailní informace o pacientovi. Své využití našla zejména ve vyspělých západních státech např. USA. Dle mého názoru se však jedná o techniku, která stále představuje určité nedostatky. V základě je systém velmi složitý a ekonomicky nehospodárný. Proto aby mohl být systém používán je nutné disponovat čtečkou čárových kódů obsahující displej pro zobrazení osobních údajů společně s tiskárnou identifikačních náramků a databází pacientů. Pokud by tyto zařízení byly umístěny na každém jednotlivém oddělení, představovaly by velkou finanční náročnost pro celou nemocnici.

Mnou vytvořené vestavěné zařízení řeší všechny výše popsané problémy, a navíc implementuje novou bezpečnostní funkci, kterou je biometrická identifikace. Díky ní se bezpečnost pacienta zdokonalí a rozšíří na optimální úroveň. Výhodou je absence jakýchkoliv fyzických identifikačních náramků, které jsou v tomto případě plně nahrazeny otiskem prstu. Pacient tak není vázán na náramek, který je možné zničit nebo ztratit. Biometrická identifikace umožňuje neustále mít k dispozici jedinečný prvek identity bez toho, aniž by se musel tisknout nebo ručně zapisovat. Spojením biometrických prvků jako je právě otisk prstu a externí databáze pacientů s osobními údaji dojde k co možná nejpřesnějšímu určení identity každého pacienta a tím i ideálnímu sestavení bezpečnostního zařízení. Výhodou mého zařízení je způsob ukládání a zacházení s citlivými daty. Všechny biometrické informace a šablony otisků jsou uloženy ve fyzické paměti senzoru otisku (interní databáze) a nikdo k nim nemá přístup, ukládají se pouze výsledné markanty otisku nikoliv celý obraz, a navíc všechny informace jsou zpětně nereprodukovatelné. Osobní údaje pacientů jsou pak umístěny na externích serverech, které jsou technicky zabezpečené a šifrované. Všechny příkazy vedené od vestavěného zařízení směrem k databází jsou odesílány pomocí šifrovaného dotazovaní HTTPS protokolu s SSL klíčem. Díky tomuto zabezpečení je možné označit celý systém, že je v souladu s budoucí evropskou směrnicí GDPR šetřící ochranu osobních údajů. Největší předností ale stále zůstává schopnost zobrazit ve velmi krátkém časovém okamžiku detailní identitu pacienta.

	Výhody	Nevýhody
Jednoduché gumové zápěstní náramky (Ručně psané informace)	Rychlé a snadné umístění, Finančně nejdostupnější, Časově nezatěžuje personál,	Omezené množství zapsaných identifikačních údajů na náramku, Možnost ztráty či zničení
Papírové náramky s čárovým kódem (nebo RFID čipem)	Detailní zobrazení osobních údajů, Uložení velkého množství informací do čárového kódu nebo RFID čipu, Rychlý proces identifikace	Nutnost používat náramek, čtečku čárových kódů a tiskárnu náramků, Finančně nákladný systém, Omezená velikost paměti čipu
Vestavěný biometrický systém (Senzor otisku prstu + Online databáze pacientů)	Biometrický prostředek identifikace, Velká kapacita uložených otisků, Detailní zobrazení osobních údajů, Bezpečné uložení všech dat, Šifrované přístupy k databázi, Dlouhodobá výdrž zařízení, Bezdrátová komunikace s databází, Přenositelnost zařízení,	Systém vyžadující stále připojení k bezdrátové nemocniční síti, Potřeba fyzického zápisu osobních informací pacienta do databáze, Akumulátorový provoz zařízení

Tab. 9: Přehled výhod a nevýhod nejčastěji používaných identifikačních metod spolu s vytvořeným vestavěným zařízením pro biometrickou identifikaci pacientů

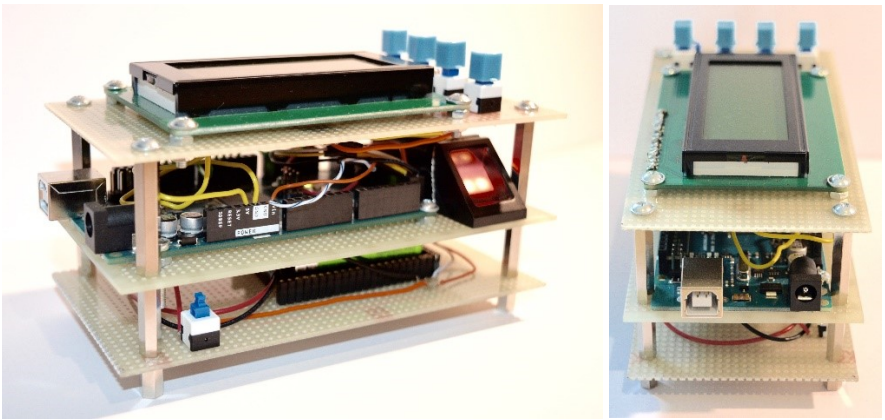
Z pohledu bezpečnosti pacienta v nemocničním zařízení, jeho identifikace, způsobu registrace a prezentace osobních informací je aktuálně nejlepším řešením mnou navržený vestavěný biometrický systém. Řeší všechny důležité bezpečnostní prvky každodenní rutinní práce zdravotnického personálu, při níž dochází k přímému kontaktu s pacientem. Splňuje všechny základní funkce identifikace pacienta, stejně jako tomu je i u jednodušších systémů, a navíc disponuje mnohonásobně rozšířenou využitelností, praktičností a moderním uživatelským prostředím. Podobnými funkcemi disponuje systém využívající čtečky čárových kódů nebo RFID čipů z osobních náramků. Taktéž umožňuje zobrazit velké množství na míru definovaných osobních informací, nicméně stále se nejedná o systém, který by co možná nejlépe eliminoval záměnu identity pacienta během klíčových léčebných postupů. Je to především zapříčiněno identifikačním náramkem, který sice je modernizován oproti předešlým generacím ale i tak může dojít ke ztrátě náramku, odcizení nebo zničení. Mnou navržený systém počítá s tím, že pacient svou identitu vždy prokazuje pomocí svých osobních a téměř stoprocentně jednoznačných biometrik. Ty nelze ztratit, zničit a ani jinak zaměnit. Velkou výhodou pro pacienta je, že jej neomezují při běžných činnostech.

Velké rozdíly nastanou při porovnání tohoto moderního způsobu identifikace a klasického ručně psaného náramku. Při používání jednoduché formy identifikace se musí personál v určitých potenciálně bezpečnostně rizikových situacích spoléhat výlučně na zápěstní náramek, který však dokáže informovat o základních informacích (v zásadě se jedná o jméno, příjmení, datum narození, RČ a oddělení) nikoliv o podrobných údajích, které by mohli zamezit případným nežádoucím situacím. Příkladem mohou být nesprávně přidělená léčiva, chybně operovaná část těla, podání krve s jinou ABO skupinou nebo záměna novorozenců těsně po porodu. Tyto a řada dalších eventuálních rizik by mohly být vyloučeny právě s pomocí používání modernějšího a bezpečnějšího systému, který všechny podstatné informace umožňuje zobrazit a neomezuje se tak pouze na velikost místa kde se údaje zapisují. Určitým omezením pro prvky jako jsou právě náramky s PDF417, QR kódem nebo s RFID čipem je velikost paměťového prostoru do něhož lze zakódovat pacientovy osobní informace. V případě jednoduchých kvazidvourozměrný kódů je maximální velikost textového nebo obrazového souboru přibližně 1,1 kB. Do modernějšího QR kódu lze uložit soubor o velikosti až 3 kB, což odpovídá textu se 4300 znaky. Posledním a zároveň nejméně častým je systém založený na RFID technologii s pasivními čipy, které slouží především jako sledovací

odpovídač při kontrole pohybu pacienta v rámci areálu zdravotnického zařízení ale také jako přenašeč jednoduchých osobních údajů. Velikost paměti čipu je pouze 32 B. Nevýhodou je, že všechny tyto kódy lze zvenčí jednoduše přečíst a nejsou tak optimálně chráněny proti zneužití. Opakem je mnou navržený systém, který je paměťově omezen pouze velikostí plotnových disků na serveru. Šance zneužití osobních údajů pacienta je zde díky biometrickým šablonám a separátně uloženým informacím minimální.

V následující části se budu věnovat praktickému srovnání s již dříve vytvořeným prototypovým zařízením a nově sestaveným biometrickým systémem pro identifikaci pacientů. V první řadě je důležité podotknout, že zjednodušený prototyp zařízení jsem vytvářel v rámci své bakalářské práce a nyní na ni navazuji s modernizovaným a více propracovaným systémem. Existuje velké množství rozdílů a nových funkcí, kterými je aktuálně sestavený biometrický systém vybaven. Jedná se především o funkce, které umožňují uživateli detailnější a bezpečnější kontrolu pacienta. Jedním z hlavních důvodů modernizace původního řešení bylo vytvoření profesionálního vestavěného zařízení, které by odpovídalo nařízení EU o ochraně osobních údajů osob tzv. GDPR a zároveň zajišťovalo pacientovu bezpečnost ve standartních i neočekávaných situacích (typicky podání léčiv, příprava na operaci nebo podání infúze).

Předchozí prototyp zařízení umožňoval registraci a identifikaci pacienta pouze v offline režimu. To znamená, že systém není žádným způsobem připojen do nemocniční sítě a pracuje čistě autonomně. Jako hlavní a zároveň jediný identifikátor sloužilo předem zvolené unikátní ID číslo, které se vždy při identifikaci zobrazovalo na displeji. Zde je hlavní rozdíl mezi novým a starým systémem, kdy v aktuální verzi systém umožňuje kromě ID čísla zobrazit řadu dalších důležitých informací o pacientovi. Zároveň způsob registrace otisku pacienta je naprosto odlišný. V původním řešení se s přístrojem komunikovalo skrz aplikaci, která zprostředkovávala pouze přímé spojení se senzorem, a tedy neumožňovala zapisovat ostatní osobní údaje potřebné k doplňující identifikaci. Nyní je veškerá datová komunikace vedena přes bezdrátovou Wi-Fi síť nemocničního zařízení a aplikace pro zdravotnický personál slouží nejen k zápisu všech klíčových informací do databáze, ale také poskytuje prohlížení a kompletní editaci pacientských dat. Z hlediska porovnání hardwarového vybavení je nutné podotknout, že obě zařízení jsou technicky velice odlišné. V původním zařízení byly použity pouze základní komponenty jako je mikrokontrolér Arduino Mega2560, optický senzor s kontaktní technologií, jednoduchý monochromatický LCD displej a zdroj napájení. Oproti aktuálně vytvořenému vestavěnému systému se jednalo o jednoúčelový nástroj pro biometrickou identifikaci na základě otisku prstu s přiděleným ID číslem. Systém podporoval tři režimy: zápis otisku a ID čísla do paměti senzoru, identifikace a odstranění otisku z paměti senzoru.



Obr. 47: Původní prototyp zařízení pro biometrickou identifikaci pacientů řešený v bakalářské práci

Výsledkem identifikace bylo zobrazení unikátního ID čísla přiděleného při registraci pacienta a hodnocení kvality neboli přesnosti s jakou byl biometrický proces proveden. Žádné doplňující informace o pacientovi systém nezpracovává a ani neregistruje. V tomto shledávám určitou bezpečnostní mezeru, díky níž může dojít k přehlédnutí ostatních důležitých údajů, které mohou zabránit případným chybám. Nový systém tyto potenciální pochybení co možná nejlépe eliminuje a při výsledu identifikace se navíc na displeji zobrazí osobní identifikační údaje a také doplňující informace pacienta. Dalším rozdílem je konstrukční řešení a celková funkčnost obou zařízení. Zde došlo opět k velkým modernizačním úpravám v oblasti uživatelského ovládání, praktického používání a systému napájení. V první řadě bylo technické řešení co nejvíce rozměrově minimalizováno tak aby finální velikost vestavěného zařízení umožňovala pohodlnou přenositelnost a nezatěžovalo tak personál v ostatních činnostech. Aktuální zařízení je nově umístěno do odolného boxu, který brání před poškozením řídící elektroniky, senzorů a zdroje napájení. V původním řešení byly tyto součástky vzájemně propojeny a umístěny na konstrukční desky oddělené distančními sloupky. Celkově bylo zařízení velice rozměrné a nevyhovovalo by praktickému provozu. Ovládání bylo realizováno pomocí čtyřech spínacích tlačítek, inicializující systémové režimy a napájení. V novém zařízení je veškeré ovládání uskutečněno skrz dotykovou vrstvu LCD displeje.

Z hlediska funkčnosti a biometrické přesnosti se oba systém téměř shodují a rozdíly ve kvalitě identifikace jsou minimální. Je to dáno především podobnými charakteristikami senzorů, které využívají téměř stejnou, tedy kontaktní optickou technologii. Oba dva snímače mají výrobcem deklarovánu chybu neoprávněného přijetí na hodnotu 0,001 %, chyba neoprávněného odmítnutí je méně pravděpodobnější u senzoru v nově zkonstruovaném zařízení (0,01 %). Výraznější rozdíl je patrný z rychlosti registrace a odstranění otisku z databáze (paměti). Modernizovaný systém umožňuje veškeré ovládání provádět na dálku a je optimalizován tak aby bezdrátový provoz způsoboval co nejmenší zpoždění. Proto jsou i tyto dva procesy rychlejší. Identifikace je naopak o něco málo pomalejší, je to dáno zejména kvůli stahování osobních informací z databáze a formátovaní textových znaků pro zobrazení na LCD displeji. Posledním rozdílem je kapacita akumulátoru a výdrž zařízení během funkčního provozu. Vzhledem ke skutečnosti, že nový systém je vybaven poměrně složitými obvody, bylo nutné jej připojit ke kvalitnějšímu zdroji napájení s vyšší kapacitou. Výsledek se pochopitelně projevil při testování výdrže, kdy byla s poměrně velkou časovou rezervou překonána původní hranice 10 minut, která by jinak byla v praxi nedostačující.

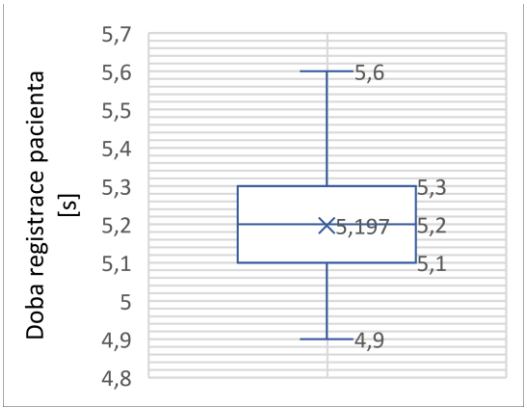
	Původní systém identifikace	**Modernizovaný systém identifikace**
Řídící deska (platforma)	Arduino Mega 2560 rev.3	Arduino Due – ARM Cortex M3
Senzor otisku prstů	Zhian Tech ZFM-206	ADH – Tech GT511-C1R
Displej (zobrazení ID pac.)	Monochrom. LCD 4x16	3,2“ LCD TFT 320 x 280 pixelů
Ovládací prvky zařízení	4 x tlačítkový spínač s aretací	Ovládání přes dotykový displej
Zdroj napájení	Akumulátor 9V 200 mAh	Akumulátor 7,2V 2100 mAh
Výdrž při používání	7 minut 20 sekund	140 minut (nepřetržitě)
Výdrž ve „sleep“ módu	10 minut	160 minut
Kapacita uložených otisků	162 snímků/otisků	20–3000 otisků (dle typu senzoru)
Rychlost registrace otisku	17,5 sekund	V průměru 5,2 sekund
Rychlost identifikace	2,2 sekundy	1,39 sekund + data (4,11 sekund)
Rychlost odstranění otisku	7,1 sekund	1,31 sekund

Tab. 10: Celkový přehled základních technických parametrů původního a aktuálního řešení vestavěného systému pro biometrickou identifikaci pacientů ve zdravotnickém zařízení

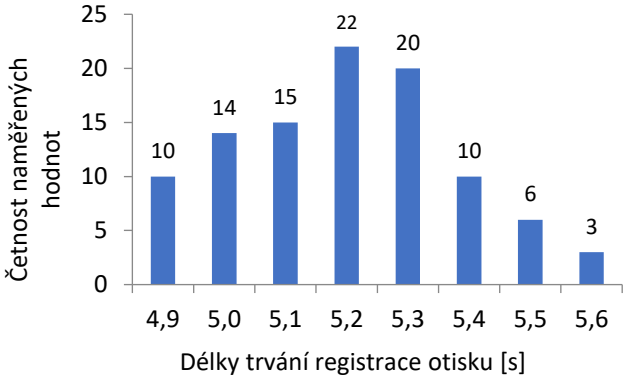
12 ANALÝZA A TESTOVÁNÍ VÝSLEDNÉHO SYSTÉMU

Závěrečné testování funkčnosti celého systému jsem rozdělil na několik kategorií, které mají co možná nejlépe zanalyzovat vytvořený produkt. V prvním případě jsem hodnotil schopnost systému jako celku registrovat otisk do interní databáze senzoru. Tím je myšleno, zda proces online a offline registrace proběhne správně a algoritmus dokáže uložit kvalitní šablonu markantních bodů pro další uplatnění jako je identifikace pacienta. Testování je zaměřeno jednak na registraci otisku v rámci uživatelské aplikace na stolním počítači a také přímo v zařízení. Druhá etapa spočívá v kontrole již uloženého pacienta, resp. jeho otisku pomocí identifikační funkce. Ve všech případech ověřuji, zda zvolený režim proběhl podle očekávání, tedy jestli konkrétní osoba byla biometricky přijata nebo odmítnuta a také jak dlouho daný proces trval. Doba průběhu jak registrace, tak identifikace je přímo závislá na dostupnosti bezdrátové sítě a síle přenosového signálu. Interní algoritmus senzoru je téměř vždy stejný, a tedy i doba tohoto dílčího kroku se mění jen minimálně. S procesem identifikace souvisí i teoretické poznatky vysvětlené v kapitole 1.4, která popisuje matematické hodnocení použitých biometrických senzorů. I tyto analytické hodnocení přesnosti používám při srovnání s údaji od výrobce. Pro testování doby a přesnosti procesů jsem změřil celkem 100 hodnot, které detailně zpracovávám a zobrazuji v tabulkách a grafech.

První část, jak už jsem naznačil se týká kvality a přesnosti registračního procesu pacienta. Ta je hodnocena kladně, jestliže je otisk prstu systémem přijat a vyhodnocen jako dostatečně kvalitní vzorek pro budoucí identifikaci. Vzhledem k faktu, že systém ve vestavěném zařízení využívá stejný algoritmus jak pro zápis otisku v online, tak i v offline režimu, jsem hodnotil přesnost a dobu zápisu pouze v prvním případě. Kladné stanovisko obdrželo to měření, které dokázalo otisk úspěšně přijmou a uložit. Celkem jsem testovaní provedl na 100 vzorcích různě velkých otisků (prstů). Důležitým hlediskem byly čisté a biologicky nezničené papilární linie. Bez dostatečně kvalitního reliéfu kůže, senzor vyhodnotí otisk jako nevhodný a odmítne jej. Samotné snímání a ukládání otisku se skládá ze tří na sebe navazujících částí, jelikož je finální šablona složena ze třech otisků tak aby výsledek byl co nejkvalitnější. Tudíž výsledný čas registrace je závislý na tom, jak rychle je pacient schopen třikrát položit prst na snímací plochu. Z celkového počtu 100 zadaných registrační procesů, bylo systémem úspěšně přijato 92 otisků a 8 jich bylo odmítnuto, resp. nesplnily předpoklady pro vhodnou extrakci markantů z nativního otisku. Výrobce v této fázi testování neuvádí, jak přesný senzor je tedy jaké procento otisků je senzor schopen uložit. Nicméně i tak jde o 92% úspěšnost, což se domnívám, že je dostatečně velké a uspokojivé číslo, které označuje senzor za velmi spolehlivý. Průměrná doba pro úspěšnou registraci otisku do databáze senzoru dosahovala 5,197 sekund (100 měření). Nejrychlejší čas byl 4,9 sekund a nejdelší zápis trval 5,6 sekund.



Graf 2: Boxplot doby registrace otisku

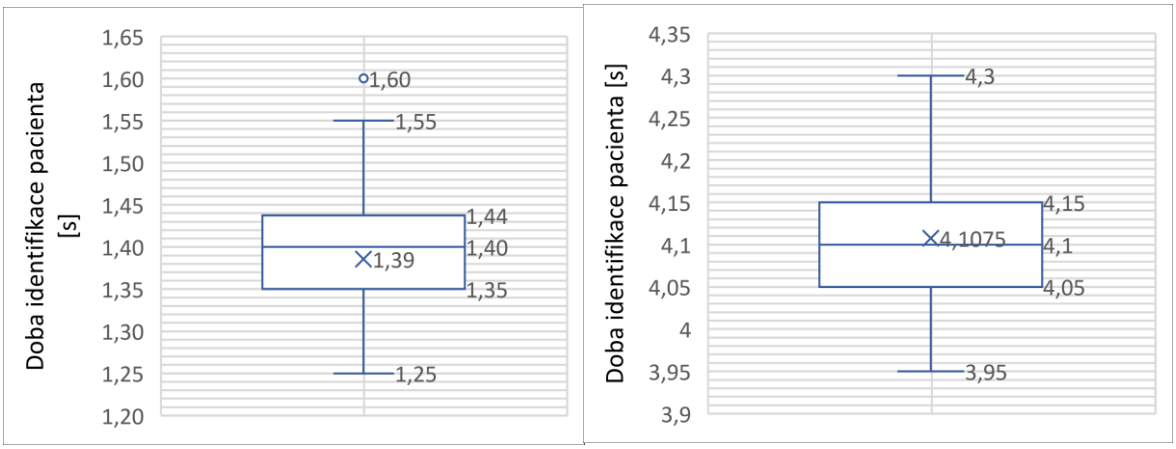


Graf 3: Histogram četnosti jednotlivých časů registrace

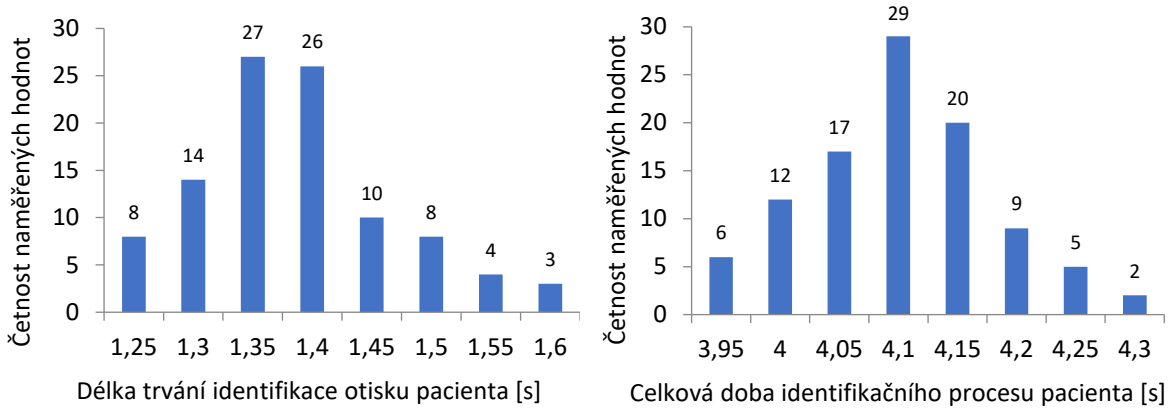
Vzhledem k tomu, že všech 100 naměřených časů bylo odlišných, zaokrouhlil jsem je na jedno desetinné místo tak, aby se s nimi kvalitněji pracovalo při statisticky analýzách. V histogramu jsou vidět nejčastější časové délky registrace, které se pohybují v rozmezí od 5,1 do 5,3 sekund. Je třeba upozornit, že měření se týká pouze fyzického zápisu otisku prstu do databáze senzoru. Mezi offline a online registrací otisku jsou velké časové rozdíly, jelikož je třeba připočítat dobu, kdy zdravotnický personál zapisuje všechny osobních informací do uživatelské aplikace. Naopak u offline registrace je nutné ve vestavěném zařízení zvolit unikátní ID číslo, pod kterým se otisk bude ukládat, a i tato činnost se velice časově proměnná.

Druhá část je výhradně zaměřena na testování identifikačního procesu pacienta. Nyní již budu vycházet z bezpečnostních parametrů udávaných výrobcem, a to sice FAR, FRR a rychlost identifikace. Pro toto testování jsem vytvořil nový seznam se 100 otisky, které jsem úspěšně uložil do interní databáze senzoru. Za prvé ověřuji teoretické předpoklady výrobce, týkající se FAR neboli neoprávněného přijetí do systému, které je deklarováno 0,001 %. Tato hodnota určuje stav, kdy je neoprávněně identifikována jedna osoba z tisíce. Já však disponuji pouze sto otisky, přesto i tento parametr jsem testoval a výsledek potvrdil teoretickou hypotézu, tedy nedošlo ani v jednom ze 100 neznámých otisků k identifikaci. Další částí je ověření chyby, kdy je odmítnuta oprávněná osoba, tedy ta, která byla dříve registrovaná a její otisk je uložen v paměti senzoru. Chyba FRR je výrobcem stanovena hodnotou 0,01 %. V tomto případě může dojít k odmítnutí jedné osoby ze sta. V rámci mnou vytvořeného souboru registrovaných otisků nastalo chybné odmítnutí pacienta ve čtyřech případech, tedy výsledná hodnota FRR se zvýšila na 0,04 %. Toto zvýšení bylo s největší pravděpodobností zapříčiněno znečištěním povrchu kožního reliéfu a také nedokonalému přiložení prstu na snímací plochu senzoru. Úspěšnost identifikace byla 96 %.

Doplňujícím testováním bylo měření rychlosti identifikace a zobrazení osobních informací na LCD displeji vestavěného zařízení. I v tomto případě je deklarována maximální doba trvání od výrobce, která by měla být menší než 1,5 sekundy, nicméně jedná se o dobu čistě identifikačního procesu v rámci senzoru. Je nutné přičíst čas, kdy je dotazován server a jsou odesílány data zpět do vestavěného zařízení. V rámci testování identifikačního času jsem dospěl k závěru, že interní funkce senzoru pro rozpoznání aktuálně snímaného otisku a dříve uložené biometrické šablony nejčastěji trvá 1,35 až 1,4 sekundy, což splňuje výrobcem stanovený limit 1,5 sekundy. Ve druhém případě jsem testoval, za jak dlouho dokáže systém pacienta identifikovat a stáhnou všechny jeho základní osobní informace ze serveru a následně je zobrazit na LCD displeji. Tato doba je závislá na několika faktorech: vzdálenosti vestavěného zařízení od AP, vzájemné umístění, reálnou šířkou pásma (Throughtput), zatížením sítě a okolním prostředím.



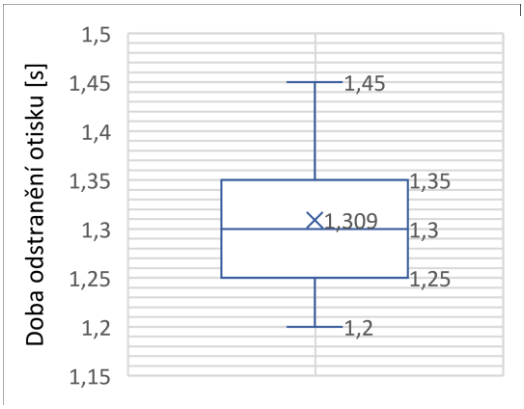
Graf 4 a 5: Boxploty dvou testovaných časů, vlevo samotný identifikační proces otisku, vpravo celkový čas identifikace otisku, stažení osobních dat z databázového serveru a zobrazení na displeji



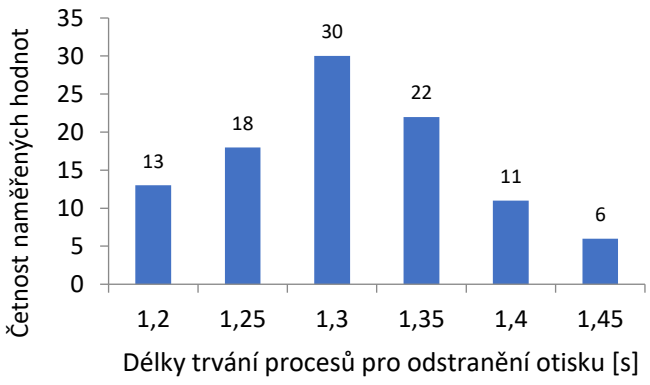
Graf 6 a 7: Histogramy dvou testovaných časů, vlevo samotný identifikační proces otisku, vpravo celkový čas identifikace otisku, stažení osobních dat z databázového serveru a zobrazení na displeji

Při minimálně zatíženém síťovém provozu a přímé vysílací dostupnosti (vzdálenost jeden metr od AP), se čas kompletního identifikačního procesu pacienta pohyboval okolo **4,11** sekund a nejčastěji v rozmezí od 4,05 do 4,15 sekund. S narůstající vzdáleností mezi vestavěným zařízením, cihlovými stěnami domu a AP se doba stažení a zobrazení osobních údajů mírně prodloužila. Na 25metrové vzdálenosti a dvěma podlažními patry byla rychlost celkové identifikace pacienta v průměru **4,35** sekund. S přibývajícím nárůstem vzdálenosti, přibližně 40 metrů, již nebyl bezdrátový modul s externí anténou schopen přijímat a vysílat datové rámce s příkazy. Nicméně i v této situaci existuje varianta tzv. offline identifikace, kdy je ve výsledku zobrazeno pouze ID číslo pacienta, avšak bez osobních údajů stažených z databáze.

Třetí část se věnuje testování přesnosti a rychlosti odstranění otisku, resp. biometrické šablony uložené ve flash paměti (databázi) senzoru GT511C1R. Odstranění je možné provézt z bezpečnostních důvodů pouze skrz uživatelskou aplikaci na počítači zapojeném do nemocniční sítě. Jde o činnost, která je vždy stoprocentní, jelikož zde dochází k přímému odstranění otisku s vázaným unikátním ID číslem. Proces odstranění může být vykonán po předem vyplněném textovém poli do něhož se uvádí konkrétní číslo otisku. Následně pomocí tlačítka „odstranění otisku“ uživatel zahájí samotné odstranění a vykonání příslušné funkce v senzoru. Komunikace se zařízením a přenos příkazů je veden prostřednictvím Wi-Fi sítě. Ze 100 příkazů pro odstranění otisku byly všechny úspěšně vymazány a při následné kontrole tedy identifikaci nebyl žádný z odstraněných otisků znovu identifikován. Průměrná rychlost odstranění otisku byla **1,31** sekund, a nejčastější naměřené časy byly v rozmezí od 1,25 do 1,35 sekund. Ve vzdálenosti 25 metrů byl čas podobně jako u identifikace prodloužen, a to v průměru o necelé dvě desetiny sekundy.



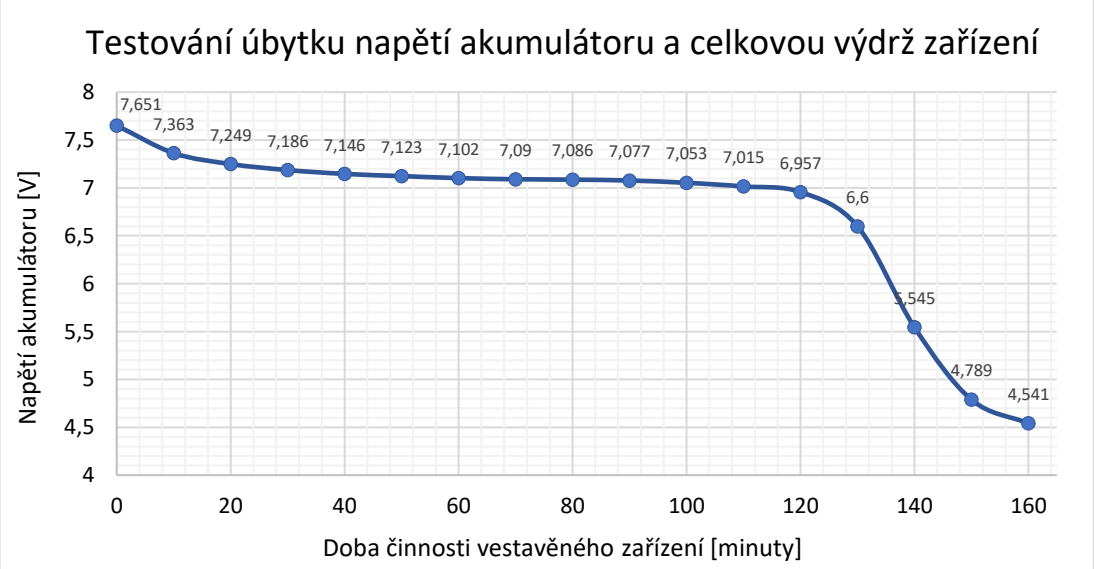
Graf 8: Boxplot doby odstranění otisku



Graf 9: Histogram jednotlivých časů odstranění otisku

Poslední testovanou charakteristikou je celková výdrž vestavěného zařízení a standardní provoz na akumulátorový zdroj napájení. Zařízení je možné napájet dvěma způsoby. Hlavním přísunem energie je akumulátorový Ni-Mh zdroj o maximálním napětí na prázdno 7,6V přičemž při zapnutí systému ihned napětí poklesne na 7,3V. Druhou variantou je fyzické připojení k počítači či jinému zařízení disponující USB portem s napětím 5V a maximálním výstupním proudem 500 mA. Tento typ připojení je očekáván při nahrávání nového firmwaru nebo také při stálé obsluze zařízení (na vytížených pracovištích), kde je nutné mít přístroj neustále k dispozici. Testování výdrže vestavěného zařízení, tedy kontrola stavu napětí akumulátoru spočívala ve dvou režimech. V prvním případě se jednalo o testování nepřetržitého provozu zařízení a měření doby, jak dlouho zařízení vydrží být zapnuté bez jakýchkoliv zvolených funkcí. Druhý režim se týkal měření doby a také průběžného napětí při kontinuálně volených identifikačních funkcí a s tím souvisejícím přikládáním různých prstů na snímač. Ve výsledku jsem se zaměřil na to, aby bylo zařízení co možná nejvíce procesně zatíženo. Ukázalo se, že zařízení při nekonečně volaných funkcích vydrží být v provozu přibližně o 20 minut méně než při klasickém používání, nicméně tento nepřetržitý stav je čistě teoretický a nikdy prakticky nemůže dojít k trvalým identifikačním či jiným funkcím.

Průměrný úbytek napětí daný za jednotu času je vypočítaný z kontinuálně vyvolávaných režimů a z napětí při provozu nezatíženého zařízení. Doba bezproblémové, tedy standardní funkce systému, kdy je zařízení v trvalém provozu a navíc každou celou minutu je zahájena 4 sekundová identifikace pacienta vychází ve výsledku na 140 minut. Během této doby napětí akumulátoru viz. Graf 10, poklesne o 2,106V na úroveň 5,545V. V této fázi již regulátor umístění na řídící jednotce pomalu přestává pracovat a celý systém se automaticky vypíná. Kompletnímu vypnutí předchází problikávání displeje a odpojení Wi-Fi modulu a senzoru otisku. V konečné části grafu ustává prudké snížení charakteristické křivky vybíjecího cyklu akumulátoru zapříčiněno odpojením odebíraného proudu. Výsledkem měření výdrže je vestavěné zařízení, které je schopno fungovat v klasickém režimu přibližně 140 až 160 minut, a to podle charakteru vykonávané činnosti. Poté je nutné zdroje napájení opět plně dobít pomocí nabíjecí stanice.



Graf 10: Testování výdrže akumulátoru v průběhu standardní činnosti vestavěného zařízení. Průměrná výdrž vestavěného zařízení dosahuje 140 až 160 minut

ZÁVĚR

Hlavním cílem této diplomové práce bylo vytvoření nové unikátní metody bezpečné identifikace pacientů případně osob nacházejících se ve zdravotnickém zařízení např. nemocnice nebo lázně. Jednou z podmínek návrhu vestavěného zařízení a řídícího systému bylo použití dobře známé technologie otisku prstu. Z této podstaty vychází celá diplomová práce, která je směřována na teoretický a praktický rozbor biometrických postupů spolu s technickým řešením dané problematiky. V teoretické části se zabývám analýzou oblasti snímání a zpracování biometrické obrazové informace se zaměřením převážně na otisk prstu. Dále se věnuji rozboru současné problematiky identifikace osob ve zdravotnických zařízeních a s tím související ochranou osobních údajů a nově také nařízením Evropské unie tzv. GDPR. Určitou část teoretické analýzy jsem směřoval nejčastěji používaným identifikačním prostředkům, kde porovnávám jejich vzájemné výhody a nevýhody, a to i s aktuálně vytvořeným zařízením. V technické části popisuji principy dnešních snímačů, způsoby nalezení a extrakce daktyloskopických markantů, historie uplatnění a zavedení biometrických technik do praxe. Podstatnou část tvoří rozbor problematiky datových úložišť, síťových prvků a databázových systémů pro uložení osobních informací každého pacienta.

V praktické části detailně objasňuji teoretický návrh a praktickou realizaci vestavěného systému pro identifikaci osob s použitím bezdrátové technologie Wi-Fi a síťového datového úložiště typu NAS. Značnou část jsem věnoval podrobnému popisu všech použitých komponentů včetně síťových zařízení a vlastnímu návrhu DPS. Výsledkem realizace praktického řešení je moderní zařízení s odpovídajícím softwarovým vybavením, které umožňuje bezpečně identifikovat pacienta při každodenních činnostech zdravotnického personálu tak, aby bylo maximálně zabráněno potenciálnímu pochybení například při dávkování medikamentů, přípravou na operaci nebo eliminaci nežádoucích jevů v rámci diagnostických metod. Doplňujícím tématem bylo charakterizování vytvořeného programu jak pro vestavěné zařízení, bezdrátový Wi-Fi modul, databázi umístěnou na fyzickém serveru tak i pro uživatelskou oblast použití. Neméně důležitou oblastí byla analýza výsledného systému, testování přesnosti a kvality biometrického procesu, míra zabezpečení citlivých osobních dat pacientů na sítích a celkovou výdrž akumulátorového zdroje energie. Poslední porovnání se týkalo pozitiv a nedostatků mezi novým zhotovením vestavěného systému a zjednodušeným prototypem přístroje vytvořeném v rámci své bakalářské práce.

Sestavené zařízení, i když je technicky a konstrukčně na vysoké úrovni, stále představuje pouze prototyp. Zde se otevírá příležitost pro možný vývoj a zdokonalení jak softwarové, tak hardwarové části zařízení do komerčního stavu. Určitým prostorem pro zlepšení zařízení je navržení jedné desky plošných spojů, která by obsahovala všechny důležité prvky systému, dále také displej s vysokým rozlišením nebo kvalitnější zdroj napájení s příslušnými nabíjecími obvody. Vývoj a začlenění tohoto systému do běžné nemocniční činnosti v sobě skrývá velký potenciál, který může zvýšit bezpečnost pacientů. Náramkové pásky jsou dnes zastaralé, nedostačující a je potřeba je obměnit za moderní způsob identifikace.

LITERATURA

[1] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. 2008. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. 1. vyd. Praha: Grada, 631 s., 32 s. obr. příl. Profesionál. ISBN 9788024723655.

[2] NÚDZIKOVÁ, Pavlína a Zdeněk SLANINA. 2014. *Elektromobilita 1* [online]. 2014. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, FEI, 2014 [cit. 2017-24-10]. ISBN 978-80-248-3531-0. Dostupné z: http://netfei.vsb.cz/downloads/autorske_texty/Elektromobilita%20I.pdf

[3] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.

[4] RATHA, N.K. a VENU GOVINDARAJU (EDS.). *Advances in biometrics sensors, systems and algorithms*. Online-Ausg. Goldaming: Springer London, 2008. ISBN 9781846289217.

[5] ADAMEC, Lukáš. *Srovnávací testy vybraných biometrických zařízení*. Fakulta informatiky, 2009. 69 s. [cit. 2017-24-10]. Bakalářská práce. Masarykova univerzita Brno.

[6] FLÍDR, Jakub. *Biometrické autentizační metody*. Fakulta elektrotechniky a komunikačních technologií, 2009. 50 s. [cit. 2017-24-10]. Bakalářská práce. VUT v Brně.

[7] ČIHÁK, Radomír. *Anatomie*. Třetí, upravené a doplněné vydání. Ilustroval Ivan HELEKAL, ilustroval Jan KACVINSKÝ, ilustroval Stanislav MACHÁČEK. Praha: Grada, 2016. ISBN 978-80-247-5636-3.

[8] BERGEROVÁ, Yvonne, BRYCHTA, Pavel a Jan J. STANEK, ed. *Estetická plastická chirurgie a korektivní dermatologie*. Praha: Grada, 2014. ISBN 978-80-247-0795-2.

[9] THORWALD, Jürgen. *Století detektivů: cesta a dobrodružství kriminalistiky*. 1. vyd. Překlad Jan Matiášek. Praha: Orbis, 1967, s. 38-39

[10] JELÍNEK, Milan. *Daktyloskopie – historie, současnost a budoucnost*. Právnická fakulta, 2014. 61 s. [cit. 2017-19-11]. Diplomová práce. Univerzita Karlova v Praze.

[11] STRAUS, Jiří. *Kriminalistická technika*. 3., rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. ISBN 978-80-7380-409-1.

[12] PROCHÁZKA, Matouš. *Vestavěný systém pro verifikaci osob na základě otisku prstu*. Fakulta elektrotechniky a informatiky, 2016. 47 s. [cit. 2017-11-12]. Bakalářská práce. Vysoká škola báňská – Technická univerzita Ostrava

[13] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi.* Fakulta bezpečnostního inženýrství, 2008. 58 s. [cit. 2017-11-12]. Studijní text. Vysoká škola báňská – Technická univerzita Ostrava

[14] Biometrics applications. *Biometrics.mainguet.org* [online]. 2014 [cit. 2017-12-18]. Dostupné z: http://biometrics.mainguet.org/appli/applications.htm

[15] LUKEŠ, Pavel. *Datová úložiště pro domácnosti a malé firmy*. Katedra matematiky, statistiky a informačních technologií, 2013. 69 s. [cit. 2018-08-02]. Bakalářská práce. Bankovní institut vysoká škola Praha

[16] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3. [cit. 2018-08-02].

[17] DEMBOWSKI, Klaus. *Mistrovství v hardware*. Brno: Computer Press, 2009. ISBN 9788025123102. [cit. 2018-08-02].

[18] SŮVA, Martin. *Záloha a archivace dat*. Katedra technologií a měření, 2012. 39 s. Bakalářská práce. [cit. 2018-8-2]. Fakulta elektrotechnická. Západočeská univerzita v Plzni.

[19] SCHREIBER, Manuel. *Absolutní bezpečí pro Vaše data*. Chip [online]. 2009, [cit. 2018-08-02] Dostupné z: http://earchiv.chip.cz/cs/earchiv/vydani/r-2009/chip-07-2009/absolutni-bezpeci.html

[20] SURYNEK, Jiří. *Problematika bezdrátových sítí.* Fakulta podnikatelská, Ústav informatiky, 2010. 83 s. Bakalářská práce. [cit. 2018-8-2]. Vysoké učení technické v Brně

[21] ZANDL, Patrick. *Bezdrátové sítě WiFi: praktický průvodce*. Brno: Computer Press, 2003. ISBN 9788072266326.

[22] CARROLL, Brandon. *Bezdrátové sítě Cisco: autorizovaný výukový průvodce*. Brno: Computer Press, 2011. Samostudium. ISBN 978-80-251-2884-8.

[23] NOVÁKOVÁ, Lada. *Stigmatizace pomocí identifikačních náramků z pohledu pacientů.* Fakulta zdravotně sociální, 2011. 95 s. Bakalářská práce. [cit. 2018-08-02]. Jihočeská univerzita v Českých Budějovicích

[24] KOPECKÁ, Petra. *Identifikace pacientů pomocí identifikačních náramků*. Fakulta zdravotně sociální, 2011. 81 s. Bakalářská práce [cit. 2018-08-02]. Jihočeská univerzita v Českých Budějovicích

[25] NULÍČEK, Michal. *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

[26] *ICEFIRE Mobile Clinic Assistant* [online]. ieimobile, 2013 [cit. 2018-02-08]. Dostupné z: http://www.ieimobile.com/index.php?option=com_content&view=article&id=157:ieimobile-introduces-icefire-104q-mobile-clinic-assistant&catid=4:news&Itemid=6

[27] OMAR, Hangaw Qader, Abdulqadir KHOSHNAW a Wrya MONNET. *Smart patient management, monitoring and tracking system using radio-frequency identification (RFID) technology*. 2016 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES) [online]. IEEE, 2016, s. 40-45 [cit. 2018-08-02]. ISBN 978-1-4673-7791-1.

[28] MARKÉTA, Hellerová. *Zavedení identifikace pacientů hospitalizovaných ve zdravotnickém zařízení.* Ministerstvo zdravotnictví. 2009. Metodická doporučení [cit. 2018-08-02] Dostupné z: http://www.mzcr.cz/dokumenty/zavedeni-identifikace-pacientu-hospitalizovanych-ve-zdravotnickem-zarizeni_3805_1841_15.html

[29] FRISCH, P., S. MIODOWNIK, P. BOOTH, P. CARRAGEE a R.N.M. DOWLING. *Patient centric identification and association*. 2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society [online]. IEEE, s. 1722-1725 [cit. 2018-08-02].

[30] Arduino Due. *Arduino.cc* [online]. 2018 [cit. 2018-03-09]. Dostupné z: https://store.arduino.cc/usa/arduino-due

[31] Fingerprint Scanner GT511C1R. *Sparkfun.com* [online]. 2018 [cit. 2018-03-09]. Dostupné z: https://learn.sparkfun.com/tutorials/fingerprint-scanner-hookup-guide?_ga=2.92869083.7312 2532.1520620794-2028374990.1502977930

[32] ESP-07 Wi-Fi module. *Mikrocontroller.net* [online]. 2018 [cit. 2018-03-09]. Dostupné z: https://www.mikrocontroller.net/attachment/338570/Ai-thinker_ESP-07_WIFI_Module-EN.pdf

[33] LCD dotykový displej TFT_320QVT. *Arduino8.webnode.cz* [online]. 2018 [cit. 2018-03-09]. Dostupné z: https://arduino8.webnode.cz/news/lekce-28-arduino-a-tft-dotykovy-displej/

[34] QNAP TS-251. *Qnap.com* [online]. 2018 [cit. 2018-03-17]. Dostupné z: https://www.qnap.com/cs-cz/product/ts-251

[35] Další elegantní směrovače 802.11ac v testu. *Digitalnidomacnost.cz* [online]. 2018 [cit. 2018-03-17]. Dostupné z: http://www.digitalnidomacnost.cz/dalsi-elegantni-smerovace-80211ac-v-testu/

CITACE POUŽITÝCH ILUSTRACÍ A OBRÁZKŮ

SEZNAM PŘÍLOH

Obsah přiloženého CD
Na přiloženém CD jsou umístěny tyto doplňující materiály:

- Diplomová práce ve formátu PDF/A
- Zdrojové kódy použitého softwaru ve formátu .cpp/.ino/.php
- Doplňující fotografie vestavěného zařízení a uživatelské aplikace pro editaci databáze