Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií

FIIT-182905-74357

Bc. Stanislav Vnenčák

BUDOVANIE ZABEZPEČENIA MOBILNÝCH ZARIADENÍ ZALOŽENÉHO NA BIOMETRICKEJ AUTENTIFIKÁCII POUŽÍVATEĽA

Diplomová práca

Vedúci práce: doc. Mgr. Daniela Chudá, PhD.

Apríl 2019

Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií

FIIT-182905-74357

Bc. Stanislav Vnenčák

BUDOVANIE ZABEZPEČENIA MOBILNÝCH ZARIADENÍ ZALOŽENÉHO NA BIOMETRICKEJ AUTENTIFIKÁCII POUŽÍVATEĽA

Diplomová práca

Študijný program: Inteligentné softvérové systémy
Študijný odbor: Softvérové inžinierstvo a Umelá inteligencia
Miesto vypracovania: Ústav informatiky, informačných systémov a softvérového inžinierstva, FIIT STU, Bratislava
Vedúci práce: doc. Mgr. Daniela Chudá, PhD.

Apríl 2019

STU FIIT
SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE
FAKULTA INFORMATIKY
A INFORMAČNÝCH TECHNOLÓGIÍ

Návrh zadania diplomovej práce

Finálna verzia do diplomovej práce [1]

Študent:

Meno, priezvisko, tituly: Stanislav Vnenčák, Bc.
Študijný program: Inteligentné softvérové systémy
Kontakt: svnencak@gmail.com

Výskumník:

Meno, priezvisko, tituly: Daniela Chudá, doc. Mgr. PhD.

Projekt:

Názov:	Budovanie zabezpečenia mobilných zariadení založeného na biometrickej autentifikácii používateľa
Názov v angličtine:	Smartphone Security based on Biometric User Authentication
Miesto vypracovania:	Ústav informatiky, informačných systémov a softvérového inžinierstva, FIIT STU, Bratislava
Oblasť problematiky:	Biometrický model používateľa

Text návrhu zadania[2]

Budovanie biometrického modelu používateľa za účelom jeho autentifikácie pri prihlasovaní do mobilného zariadenia je jednou z možností, akou dokážeme spoľahlivo zabezpečiť mobilné zariadenie proti zneužitiu. Budovanie biometrického modelu používateľa pod smartfónovou platformou je možné sledovaním jeho biometrických charakteristík pri práci so zariadením prostredníctvom dotykového displeja alebo prostredníctvom polohovacích senzorov zariadenia.

Analyzujte existujúce prístupy a metódy budovania a overovania biometrického modelu používateľa za účelom zvýšenia zabezpečenia mobilných zariadení. Navrhnite a implementujte metódu pre budovanie a overovanie modelu používateľa na základe jeho biometrických charakteristík pre účely jeho autentifikácie pri prihlasovaní do mobilného zariadenia. Zamerajte sa na možnosti využitia používateľských charakteristík správania sa na nižšej úrovni (sledovanie pohybov na dotykovom displeji, polohovanie zariadenia) a na zvyšovanie presnosti autentifikácie používateľa dynamickým prispôsobovaním jeho biometrického modelu na základe zmien v jeho správaní v priebehu času. Implementovaná metóda má slúžiť na statickú autentifikáciu používateľa pri prihlasovaní do mobilného zariadenia. Pri budovaní a overovaní modelu používateľa experimentujte s biometrickými vzorkami a algoritmami na výber vhodných biometrických charakteristík pod smartfónovou platformou. Navrhnutú metódu overte na vybranej vzorke používateľov a vyhodnoťte úspešnosť autentifikácie používateľa pri prihlasovaní do zariadenia ako aj úspešnosť identifikácie neoprávneného pokusu o prihlásenie do mobilného zariadenia.

---

[1] Vytlačiť obojstranne na jeden list papiera

[2] 150-200 slov (1200-1700 znakov), ktoré opisujú výskumný problém v kontexte súčasného stavu vrátane motivácie a smerov riešenia

Literatúra[3]

- GIOFFRIDA, C., MAJDANIK, K., CONTI, M. et al. I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics. In: DIMVA '14, Dietrich S. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. Cham: SPRINGER, 2014. ISBN 978-3-319-08508-1, s. 92-111.
- PARK, J., KIM, T., IM, E. Touch Gesture Data Based Authentication Method for Smartphone Users. In: RACS '16, Proceedings of the International Conference on Research in Adaptive and Convergent Systems. New York: ACM, 2016. ISBN 978-1-4503-4455-5, s. 136-141.

Vyššie je uvedený návrh diplomového projektu, ktorý vypracoval(a) Bc. Stanislav Vnenčák, konzultoval(a) a osvojil(a) si ho doc. Mgr. Daniela Chudá, PhD. a súhlasí, že bude takýto projekt viesť v prípade, že bude pridelený tomuto študentovi.

V Bratislave dňa 30.1.2018

Podpis študenta

Podpis výskumníka

Vyjadrenie garanta predmetov Diplomový projekt I, II, III

Návrh zadania schválený: áno / nie[4]

Dňa: 12. 2. 2018

Podpis garanta predmetov

[3] 2 vedecké zdroje, každý v samostatnej rubrike a s údajmi zodpovedajúcimi bibliografickým odkazom podľa normy STN ISO 690, ktoré sa viažu k téme zadania a preukazujú výskumnú povahu problému a jeho aktuálnosť (uveďte všetky potrebné údaje na identifikáciu zdroja, pričom uprednostnite vedecké príspevky v časopisoch a medzinárodných konferenciách)

[4] Nehodiace sa prečiarknite

Zadanie diplomovej práce

Meno študenta: **Bc. Stanislav Vnenčák**

Študijný program: Inteligentné softvérové systémy

Študijný odbor: Softvérové inžinierstvo – hlavný študijný odbor
Umelá inteligencia – vedľajší študijný odbor

Názov práce: **Budovanie zabezpečenia mobilných zariadení založeného na biometrickej autentifikácii používateľa**

Samostatnou výskumnou a vývojovou činnosťou v rámci predmetov Diplomový projekt I, II, III vypracujte diplomovú prácu na tému, vyjadrenú vyššie uvedeným názvom tak, aby ste dosiahli tieto ciele:

Všeobecný cieľ:

Vypracovaním diplomovej práce preukážte, ako ste si osvojili metódy a postupy riešenia relatívne rozsiahlych projektov, schopnosť samostatne a tvorivo riešiť zložité úlohy aj výskumného charakteru v súlade so súčasnými metódami a postupmi študovaného odboru využívanými v príslušnej oblasti a schopnosť samostatne, tvorivo a kriticky pristupovať k analýze možných riešení a k tvorbe modelov.

Špecifický cieľ:

Vytvorte riešenie zodpovedajúce návrhu textu zadania, ktorý je prílohou tohto zadania. Návrh bližšie opisuje tému vyjadrenú názvom. Tento opis je záväzný, má však rámcový charakter, aby vznikol dostatočný priestor pre Vašu tvorivosť.

Riaďte sa pokynmi Vášho vedúceho.

Pokiaľ v priebehu riešenia, opierajúc sa o hlbšie poznanie súčasného stavu v príslušnej oblasti, alebo o priebežné výsledky Vášho riešenia, alebo o iné závažné skutočnosti, dospejete spoločne s Vaším vedúcim k presvedčeniu, že niečo v texte zadania a/alebo v názve by sa malo zmeniť, navrhnite zmenu. Zmena je spravidla možná len pri dosiahnutí kontrolného bodu.

Miesto vypracovania: Ústav informatiky, informačných systémov a softvérového inžinierstva, FIIT STU v Bratislave

Vedúci práce: **doc. Mgr. Daniela Chudá, PhD.**

Termíny odovzdania:

Podľa harmonogramu štúdia platného pre semester, v ktorom máte príslušný predmet (Diplomový projekt I, II, III) absolvovať podľa Vášho študijného plánu

Predmety odovzdania:

V každom predmete dokument podľa pokynov na www.fiit.stuba.sk v časti: home > Informácie o > štúdiu > harmonogram štúdia > diplomový projekt.

V Bratislave dňa 12. 2. 2018

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
Fakulta informatiky a informačných technológií
Ilkovičova 2, 842 16 Bratislava 4
1

prof. Ing. Pavol Návrat, PhD.
riaditeľ Ústavu informatiky, informačných systémov a softvérového inžinierstva

Anotácia

Slovenská technická univerzita v Bratislave
FAKULTA INFORMATIKY A INFORMAČNÝCH TECHNOLÓGIÍ
Študijný program: Inteligentné softvérové systémy

Autor:	Bc. Stanislav Vnenčák
Diplomová práca:	Budovanie zabezpečenia mobilných zariadení založeného na biometrickej autentifikácii používateľa
Vedúci diplomovej práce:	doc. Mgr. Daniela Chudá, PhD.

Apríl 2019

Táto diplomová práca sa zaoberá problematikou budovania zabezpečenia mobilných zariadení založených na Android platforme pomocou biometrickej autentifikácie používateľov. Budovanie biometrického modelu používateľa pod smartfónovou platformou je možné sledovaním jeho biometrických charakteristík pri práci so zariadením prostredníctvom dotykového displeja alebo prostredníctvom polohovacích senzorov zariadenia. V tejto práci sú analyzované možnosti budovania a overovania biometrického modelu používateľa pre účely jeho autentifikácie a zvýšenia zabezpečenia mobilného zariadenia. Časť práce je venovaná analýze existujúcich riešení na autentifikáciu používateľov prostredníctvom sledovania ich biometrických charakteristík, možnostiam využitia informačnej fúzie v procese autentifikácie používateľov a popisu návrhu a implementácie vytváraného biometrického systému. V záverečnej časti práce je uvedené zhodnotenie výsledných hodnôt chýb FAR, FRR a EER spolu s porovnaním dosiahnutých výsledkov s prácami zaoberajúcimi sa problematikou biometrickej autentifikácie používateľov na mobilnom zariadení.

Kľúčové slová:
zabezpečenie, biometria, autentifikácia, biometrický model používateľa, spektrálna analýza, informačná fúzia

Annotation

Slovak University of Technology in Bratislava
FACULTY OF INFORMATICS AND INFORMATION TECHNOLOGIES
Degree course: Intelligent software systems

Author: Bc. Stanislav Vnenčák
Master's Thesis: Smartphone Security based on Biometric User Authentication
Supervisor: Assoc. Prof. Daniela Chudá

April 2019

This master thesis focuses on a problem of building mobile security on Android platform devices using biometric user authentication. Building a biometric user model under a smartphone platform can be done by monitoring its biometric characteristics when working with device via the touch screen or through device positioning sensors. In this thesis, we analyze the possibilities of building and verifying the biometric user model for the purpose of user authentication and building advanced mobile security. Part of the work is devoted to an analysis of existing solutions for user authentication by monitoring its biometric characteristics, advantages of information fusion in authentication process and a description of the process of designing and implementing the biometric user authentication system. In the final part of the thesis there is an evaluation of the resulting error values FAR, FRR and EER together with the comparison of similar papers addressing biometric authentication on smartphone platform.

Keywords:
security, biometry, authentication, biometrics user model, spectral analysis, information fusion

Čestné prehlásenie

Čestne prehlasujem, že som výsledky prezentované v tejto diplomovej práci vypracoval samostatne, pod odborným dohľadom vedúcej mojej diplomovej práce, pani doc. Mgr. Daniely Chudej, PhD., spolu s využitím uvedenej literatúry.

Bratislava, 30.04.2019 .....

Vlastnoručný podpis

Poďakovanie

V tejto časti by som sa chcel poďakovať vedúcej mojej diplomovej práce pani doc. Mgr. Daniele Chudej, PhD., za odbornú pomoc, praktické rady a skupinové, ako aj individuálne konzultácie, ktoré mi boli poskytnuté a pomohli mi pri vypracovávaní tejto diplomovej práce.

Osobitné poďakovanie taktiež patrí všetkým účastníkom zapojených do experimentu v súvislosti so zbieraním reálnych biometrických dát pri odomykaní zariadenia.

Obsah

Zoznam obrázkov

Zoznam tabuliek

1 Úvod

Využívanie mobilných zariadení je v súčasnosti neoddeliteľnou súčasťou života každého z nás, a tak sa bezpečnosti spojenej s používaním mobilných zariadení dostáva čoraz viac pozornosti. Ľudia sú postupom času nútení uchovávať viac citlivých údajov vo svojich mobilných zariadeniach, a sú tak vystavovaní vyššiemu riziku ich zneužitia. Práve potreba zabezpečenia mobilných zariadení proti zneužitiu vytvára miesto pre hľadanie nových druhov zabezpečenia, aby sa autentifikácia používateľa na mobilných zariadeniach dostala na úroveň, kedy ju už nie je možné jednoducho obísť.

Skúmanie biometrických charakteristík používateľov na mobilných zariadeniach je jednou z možných riešení, ako zabezpečiť vyššiu úroveň ochrany používateľov pred zneužitím ich citlivých údajov, ktoré majú uložené v mobilných zariadeniach, alebo ku ktorým sa denne dostávajú práve prostredníctvom mobilných zariadení. Biometria, alebo skúmanie psychologických či fyziologických prejavov správania sa človeka[1], ako je definovaná v Collins English Dictionary, môže napomôcť k presnejšej autentifikácii používateľov mobilných zariadení, nakoľko každý z nás je svojim správaním jedinečný a je len na nás, ako dokážeme túto vlastnosť využiť.

V časti 2 Analýza stavu problematiky sa tak zaoberáme charakteristikou klasických biometrických systémov. Rozoberáme tu jednotlivé kroky, ktoré je potrebné vykonať pre úspešnú autentifikáciu používateľa a možnosti vytvárania biometrických modelov používateľov s ohľadom na výber vhodných biometrických charakteristík. Porovnávame tu procesy verifikácie a autentifikácie v biometrických systémoch. Zaujímavou časťou tejto kapitoly sú špecifiká multibiometrických systémov, ktoré pri autentifikácii používateľov využívajú princípy informačnej fúzie na rôznych úrovniach. Taktiež sa tu zaoberáme potrebou zabezpečenia biometrických systémov a spôsobmi merania presnosti a efektívnosti týchto systémov. V tejto časti ďalej analyzujeme existujúce riešenia a prístupy k autentifikácii používateľov na základe ich biometrických charakteristík. Porovnávame výsledky jednotlivých prác a zhŕňame tu nadobudnuté poznatky získané z analýzy skúmanej problematiky biometrickej autentifikácie používateľov.

V časti 3 Ciele práce a výskumné hypotézy uvádzame ciele práce a výskumné hypotézy, ku ktorým sme dospeli počas skúmania problémovej oblasti a navrhnuté

[1] Collins English Dictionary – Complete and Unabridged, 12. vydanie 2014. Dostupné na webe dňa 19. októbra 2017, https://www.thefreedictionary.com/biometry

spôsoby ich vyhodnotenia.

Časti 4 Návrh biometrického systému a 4 Implementácia sú venované návrhu a implementácii vytváraného biometrického systému. Bližšie tu špecifikujeme požiadavky na vytváraný systém a navrhujeme architektúru systému, model biometrických charakteristík používateľa a procesy autentifikácie používateľa na základe jeho biometrického modelu. Taktiež tu zhŕňame aktuálny stav implementácie vytváraného systému.

Overenie riešenia spolu s opisom experimentov a procesmi predspracovania dát, vyhľadávania outlierov, výberu biometrických charakteristík a klasifikácie uvádzame v časti 6 Overenie riešenia. Taktiež tu uvádzame výsledky prvotných experimentov pri autentifikácii používateľov a výsledky navrhnutého biometrického systému spolu s overením hypotéz a porovnaním dosiahnutých výsledkov s podobnými prácami.

Zhodnotenie postupu a celkového výsledku tejto diplomovej práce je uvedené v záverečnej časti tejto práce v kapitole 7 Zhodnotenie.

2 Analýza stavu problematiky

Využívanie hesiel, ako formy zabezpečenia, je jedným z najpoužívanejších spôsobov, akými si väčšina používateľov zabezpečuje výhradný prístup k obsahu mobilných zariadení. Nakoľko je zadanie hesla alebo vzoru na do mobilného zariadenia pomerne rýchle a na odomknutie zariadenia stačí iba niekoľko sekúnd, ľudia tento spôsob vo veľkom využívajú bez toho, aby si uvedomovali jeho riziká. Heslá jednotlivých používateľov navyše nemusia byť unikátne, a tak si vyberajú heslá, ktoré sú ľahko zapamätateľné, a je tak možné ich jednoducho odhaliť. V prípade krátkych hesiel alebo jednoduchých odomykacích vzorov nie je problém tieto heslá viacerými spôsobmi odpozorovať alebo odhaliť aj klasickým „brute force“ spôsobom, kedy sú postupne skúšané všetky možnosti zadania hesla, až kým nie je ochrana pred neoprávneným prístupom k zariadeniu prelomená, alebo pomocou šmúh, ktoré na displeji používatelia pri odomykaní zanechávajú (tzv. angl. smudge effect). Práve kvôli slabinám zabezpečenia mobilných zariadení, ako ho poznáme dnes, vznikajú nové metódy bezpečnej autentifikácie používateľov, akými je napríklad aj sledovanie biometrických vlastností človeka ako podporná metóda overenia jeho identity pri prístupe do zariadenia.

2.1 Biometria na mobilných zariadeniach

Pod pojmom biometria rozumieme súbor štatistických a analytických vedeckých poznatkov, ktoré vedú k skúmaniu a praktickému využitiu charakteristických vlastností živých organizmov, ktoré sú merateľné a môžu slúžiť k jednoznačnej identifikácii alebo autentifikácii človeka [RAK08]. Práve u ľudí nadobúda skúmanie biometrických charakteristík väčší význam, nakoľko sledovanie biometrických charakteristík používateľov sa zdá byť spoľahlivou voľbou pri zabezpečení nielen mobilných zariadení, ktorá nijako neovplyvňuje pohodlnosť používania mobilného zariadenia, nakoľko sledovanie biometrických charakteristík ako podporných informácií pre overenie identity používateľa si nevyžaduje jeho dodatočnú pozornosť, ale tieto informácie je možné získať bez akýchkoľvek ďalších akcií popri zadávaní odomykacieho vzoru alebo hesla.

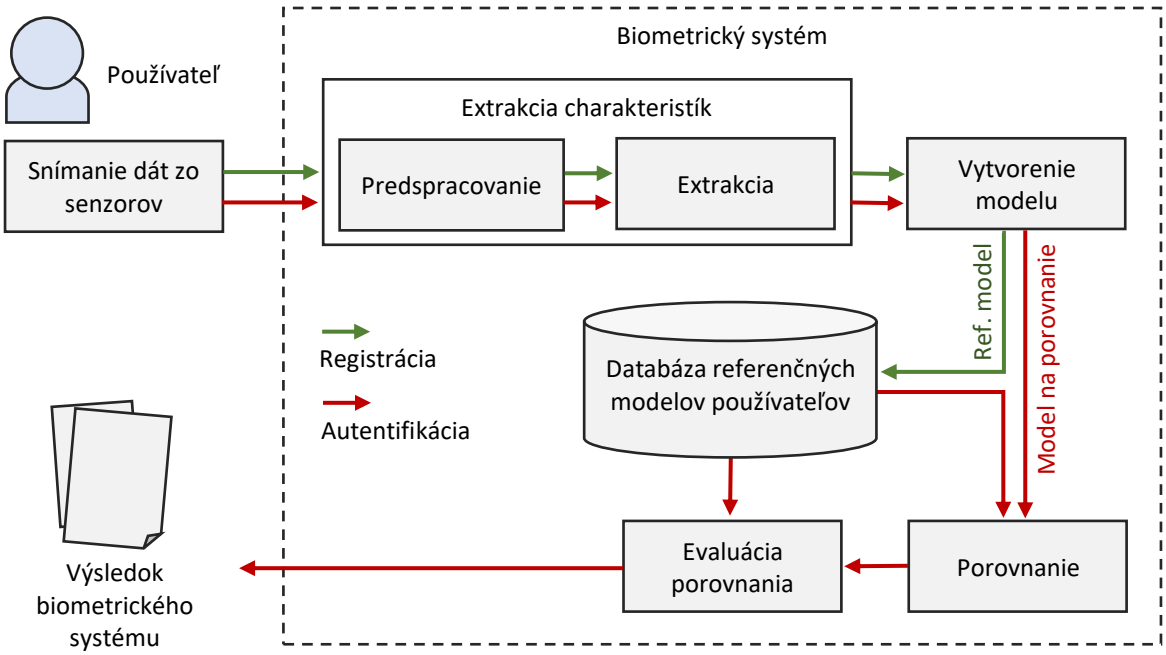
Pri overovaní identity používateľa pomocou jeho biometrických charakteristík je však potrebný odlišný prístup ako pri autentifikácii klasickými spôsobmi, akým je napríklad zadanie hesla. Pri zadávaní hesla alebo odomykacieho vzoru sa pre úspešné prihlásenie používateľa do zariadenia musí heslo alebo odomykací vzor presne zhodovať s heslom alebo vzorom, ktorý bol zadaný pri vytváraní zabezpečenia. Pri autentifikácii prostredníctvom

biometrických charakteristík je však potrebné brať do úvahy, že správanie používateľa, aj napriek tomu, že je pre každého používateľa charakteristické, sa môže z času na čas mierne meniť, a tak nemôžeme uvažovať iba o presnej zhode biometrických charakteristík pri každom prístupe do zariadenia. Je tak potrebné vykonať rozhodnutie o tom, do akej miery je možné biometrické zmeny akceptovať pri autentifikácii toho istého používateľa. Touto charakteristickou odlišnosťou biometrického zabezpečenia oproti bežným prístupom k zabezpečeniu mobilných zariadení tak vzniká priestor pre chybovosť pri autentifikácii používateľov, kedy môže byť aj ozajstnému vlastníkovi zariadenia znemožnený prístup do tohto zariadenia, alebo naopak, kedy je povolený aj neoprávnený prístup do zariadenia nesprávnym autentifikovaním používateľa, čo je hlavnou výzvou vo vytvorení kvalitného biometrického zabezpečenia.

2.1.1 Charakteristika biometrického systému

Ako sme už spomínali v úvode tejto práce, biometrické systémy môžu byť založené na behaviorálnych alebo fyziologických charakteristikách používateľov a fungujú na princípe jedinečnosti používateľov, ktorí s ním prichádzajú do styku. Tieto systémy sú častokrát využívané na rozpoznávanie používateľov a regulovanie prístupu k rôznym fyzickým zariadeniam, na zvýšenie spoľahlivosti autentifikácie osôb, reguláciu prístupu k službám alebo rozličným zdrojom informácií. V súvislosti s biometrickými systémami sa však stále objavujú otázky týkajúce sa ich spoľahlivosti. Biometrické systémy na rozpoznávanie používateľov dokážu rozpoznať používateľov iba s určitou úspešnosťou, a tak sa môže stať, že sú v niektorých prípadoch chybové. Pravdepodobnosť nastátia nesprávnej autentifikácie je síce malá, no stále nie je úplne eliminovaná. Pre zdokonaľovanie biometrických systémov je tak okrem prekonania viacerých technických problémov v súvislosti s presnosťou fyzických biometrických zariadení potrebné aj správne porozumenie miery rozdelenia biometrických znakov človeka medzi skupinu ľudí, ktorí budú biometrický systém využívať (niekedy sa môže jednať aj o celú populáciu) [JOSEPH10].

Klasický biometrický systém vo všeobecnosti pozostáva z niekoľkých častí, ktoré postupne spracovávajú dáta zaznamenané od používateľa prostredníctvom rôznych špecializovaných senzorov. Jednoduchú schému biometrického systému a rozpis jeho jednotlivých častí uvádzame na Obr. 1 Schéma klasického biometrického systému.



Obr. 1 Schéma klasického biometrického systému

V rámci fungovania biometrického systému je potrebné vykonať dva procesy. Jedným z nich je vytvorenie/zaznamenanie referenčného biometrického modelu používateľa, na základe ktorého sa bude overovať jeho identita, a druhým je samotná autentifikácia používateľa na základe jeho referenčného modelu.

Snímanie dát zo senzorov. Snímanie dát zo senzorov (niekedy sa uvádza aj ako logovanie) sa vykonáva na začiatku procesu autentifikácie používateľa meraním jeho biometrických charakteristík, ktoré môžu mať fyziologický alebo behaviorálny charakter. Vo väčšine prác, ktoré skúmali sledovanie biometrických charakteristík na mobilných zariadeniach, sa stretávame s možnosťou sledovania používateľa prostredníctvom dotykovej obrazovky alebo pomocou natívnych senzorov zariadenia, akými sú akcelerometer, gyroskop alebo magnetometer. Pri každom meraní týchto charakteristík by mali byť zachytené dáta od 1 používateľa veľmi podobné iba s minimálnou akceptovateľnou odchýlkou.

Extrakcia charakteristík. V rámci spracovania surových dát z natívnych senzorov zariadenia a dotykovej obrazovky je potrebné vykonať výber tých dát, ktoré sú vhodné pre dostatočné odlíšenie používateľov. Dáta zo senzorov a dotykovej obrazovky vo všeobecnosti obsahujú dáta, ktoré nie sú pri autentifikácii používateľa potrebné. Biometrické charakteristiky tak musia byť zo zachytených dát vyextrahované, pričom pri

ich výbere by sme mali dbať na ich dostatočnú stabilnosť a odlíšiteľnosť pre jednotlivých používateľov.

Pri extrakcii čŕt zo získaných už predspracovaných dát zo senzorov a dotykovej obrazovky zariadenia následne dochádza k transformácii dát do podoby, ktorá môže bude biometrickým systémom využitá na vytvorenie modelov používateľov. Pri mobilných zariadeniach a sledovaní odomykania zariadenia sa zväčša stretávame s výberom a dopočítaním vlastností používateľa ako napríklad rýchlosť kreslenia vzoru alebo presnosť stláčania jednotlivých kláves pri odomykaní zariadenia.

Vytvorenie modelu používateľa. Na základe dát získaných z procesu odomykania zariadenia, ktoré boli predspracované a boli z nich vyextrahované potrebné charakteristiky, dochádza k vytváraniu modelov používateľov z týchto charakteristík. Tie sú následne využívané na registráciu (pri prvotnom prihlásení používateľa do biometrického systému) na zadefinovanie referenčného modelu používateľa alebo na porovnávanie aktuálneho modelu používateľa s jeho referenčným modelom pri prihlásení. Referenčný model používateľa sa môže v priebehu času meniť, a tak je vhodné zadefinovať vhodnú stratégiu jeho aktualizácie, aby bola zabezpečená čo najvyššia presnosť biometrického systému aj po dlhšom čase jeho používania.

Porovnanie. V procese porovnávania biometrických modelov používateľov dochádza k porovnávaniu referenčných modelov používateľov s ich aktuálne získaným vstupom (napr. pri prihlásení). Samotné porovnávanie sa uskutočňuje pomocou rôznych typov klasifikátorov alebo neurónových sietí [CORPUS16, GIOFFRIDA14, LIN12, FRANK13]. Na natrénovanie klasifikátora aj neurónových sietí je však potrebné, aby bol počet referenčných modelov používateľov dostatočne veľký, aby bola aj presnosť a spoľahlivosť biometrického systému čo najvyššia.

Evaluácia porovnania. Táto časť biometrického systému je častokrát najdôležitejšia, nakoľko výstupom tejto časti je určenie výsledku autentifikácie samotného používateľa. Určenie výsledku autentifikácie sa opiera o výsledky porovnávania biometrických modelov na základe podobnosti aktuálneho modelu používateľa s referenčnými modelmi používateľov.

V procese autentifikácie by malo byť zaistené, že oprávnený používateľ dostane kladnú

odpoveď a nebude odmietnutý. K prípadom odmietnutia oprávneného používateľa však môže sporadicky dochádzať z dôvodu nejednoznačností a podobností v biometrických modeloch jednotlivých používateľov. Dochádza tak k prípadom nesprávneho akceptovania alebo nesprávneho neakceptovania používateľa (angl. False Acceptance, False Rejection) biometrickým systémom.

2.2 Biometrický model používateľa

Biometrický model používateľa pozostáva z takých fyziologických alebo behaviorálnych charakteristík používateľa, ktoré predstavujú základ pre jeho jednoznačnú autentifikáciu. Základnou vlastnosťou týchto charakteristík by mala byť ich merateľnosť, jednoznačnosť a stálosť (v priebehu času by sa nemali meniť alebo by malo dochádzať iba k minimálnym zmenám).

Tvorbe biometrických modelov používateľov sa venuje pomerne vysoká pozornosť, nakoľko výber vhodných charakteristík, ktoré budú využité na dostatočné odlíšenie používateľov, môže mať vysoký vplyv na spoľahlivosť biometrického systému. O potrebe skúmania možnosti vytvárania biometrických modelov používateľov a vplyvu na úspešnosť pri autentifikácii používateľov sa dozvedáme z práce [ALARIKI16].

Biometrické modely používateľov sú využívané v procese klasifikácie, preto aj forma uchovávania jednotlivých charakteristík musí byť v podobe, v akej ju sú schopné jednotlivé klasifikátory spracovať. V podobných prácach sa stretávame s mnohými typmi sledovaných charakteristík v závislosti od spôsobu sledovania používateľa. Niektoré zo sledovaných charakteristík, ktoré sa týkajú biometrie na mobilných zariadeniach s využitím dotykového displeja a mobilných polohovacích zariadení, uvádzame v nasledujúcej tabuľke Tab. 1 Príklady sledovaných charakteristík.

Tab. 1 Príklady sledovaných charakteristík

Spôsob zaznamenávania	**Sledovaná charakteristika**
Dotyková obrazovka	*Dĺžka dotyku*
	Trvanie dotyku
	Veľkosť dotyku (min, max)
	Súradnice X, Y pre začiatok a koniec pohybu
	Súradnice X, Y pre celý pohyb

	Rýchlosť (min, max, priemer)
	Veľkosť prsta (hlavná/vedľajšia os, min, max, priemer)
	Tlak dotyku (min, max, priemer)
Akcelerometer	*Akcelerácia v smere osi X, Y, Z (min, max, priemer, štandardná odchýlka)*
Gyroskop	*Naklonenie v smere osi X, Y, Z (min, max, priemer, štandardná odchýlka)*

2.2.1 Výber biometrických charakteristík

Pri tvorbe biometrického modelu používateľa je potrebný výber tých charakteristík používateľov, ktoré sú v značnej miere pre používateľov odlišné, a dokážu tak napomôcť pri ich autentifikácii (angl. Feature Selection). Ako sa uvádza v práci [UNNIKRISHAN14], hlavným cieľov výberu biometrických charakteristík je transformácia vstupných dát do skupín tak, aby boli všetky dáta patriace do jednej skupiny podobné a dáta patriace do rôznych skupín čo najviac odlišné. Takto dokážeme získať robustné charakteristiky, ktoré sú pri transformáciách, akými sú napríklad ich zoslabenie alebo násobenie, nemenné, a ktoré najlepšie vystihujú sledovanú biometrickú charakteristiku.

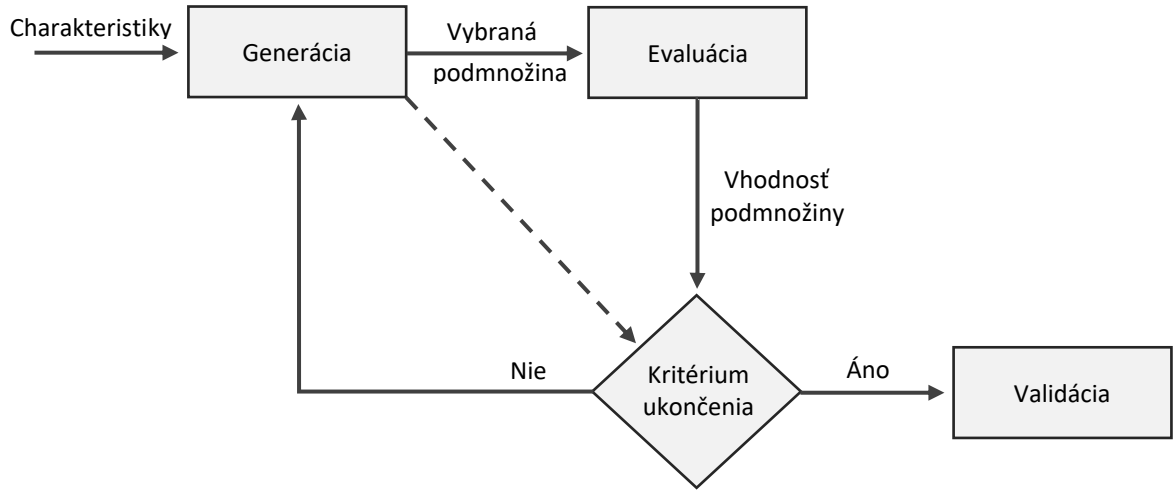
Okrem výberu biometrických charakteristík z dát získaných od používateľov je však potrebný aj vhodný výber tých charakteristík, ktoré budú použité pri procese klasifikácie. Odstránením dát, ktoré nenesú významnú a pre používateľov dostatočne odlíšiteľnú charakteristiku, alebo dát, ktoré sú zašumené (angl. Noisy Data), sa môže presnosť ale aj rýchlosť klasifikácie, a teda aj biometrického systému, zvýšiť.

Klasické metódy na výber vhodných biometrických charakteristík využívajú evaluáciu, na základe ktorej z celej dostupnej množiny sledovaných biometrických charakteristík vyberú tú kombináciu charakteristík, pomocou ktorej je úspešnosť klasifikácie najvyššia. Táto metóda je však výpočtovo náročná aj pre menšie datasety s priemerných počtom sledovaných charakteristík. Medzi efektívnejšie metódy však patria prístupy, ktoré pri vyhľadávaní optimálnej kombinácie biometrických charakteristík využívajú rôzne heuristiky alebo metódy náhodného vyhľadávania. Metódami výberu vhodných charakteristík sa venuje viacero prác, ktoré popisujú spôsoby a metódy využívané v procese výberu charakteristík.

Podľa [MANORANJAN03] a [KIRA92], proces výberu charakteristík, ktorým sa budeme riadiť aj my pri výbere vhodných biometrických charakteristík, ktoré použijeme pri tvorbe biometrického modelu používateľa a následnej klasifikácii, pozostáva zo štyroch

základných krokov (Obr. 2 Proces výberu vhodných charakteristík):

1) *generácia podmnožín charakteristík* – stratégia vyhľadávania na generovanie podmnožiny charakteristík pre evaluáciu (možnosť pridávania, odoberania alebo náhodného výberu charakteristík do vybranej podmnožiny);
2) *evaluácia* – overenie vhodnosti vygenerovanej podmnožiny charakteristík na základe vyhodnocovacej funkcie (lepšia podmnožina charakteristík nahrádza horšiu, výsledok tohto kroku sa môže líšiť od výberu vyhodnocovacej funkcie);
3) *kritérium ukončenia* – bez tohto kritéria by proces výberu vhodných charakteristík mohol trvať veľmi dlho alebo donekonečna. Toto kritérium môže byť definované počtom vybraných charakteristík, maximálnym počtom vyhľadávacích iterácií a podobne;
4) *validácia* – tento krok nemusí byť súčasťou procesu výberu vhodných charakteristík, no v niektorých prípadoch je vhodné ho do tohto procesu zahrnúť z dôvodu otestovania a porovnania výsledkov s predchádzajúcimi podmnožinami vybraných charakteristík na predpripravených alebo reálnych dátach.



Obr. 2 Proces výberu vhodných charakteristík (vytvorené podľa [MANORANJAN03])

Proces výberu vhodných charakteristík biometrického modelu je veľmi dôležitý pre úspešnosť ale aj rýchlosť samotného biometrického systému. Ako sa uvádza v práci [UNNIKRISHAN14] a [PARK16], pri výbere vhodnej podmnožiny charakteristík (ak existuje viacero vhodných riešení), ale taktiež pre zabránenie pretrénovania modelu pri klasifikácii, je možné využiť princíp Occamovej žiletky (angl. Occam's razor principle), na základe ktorého je vhodné vybrať zo všetkých vyhovujúcich podmnožín charakteristík

podmnožinu charakteristík definujúcu najjednoduchší model používateľa, pomocou ktorého stále dosahujeme požadované výsledky [GAMBERGER97]. Pomocou tohto princípu sú vytvárané modely s najnižším možným počtom sledovaných charakteristík pri najvyššej možnej presnosti klasifikácie nových inštancií.

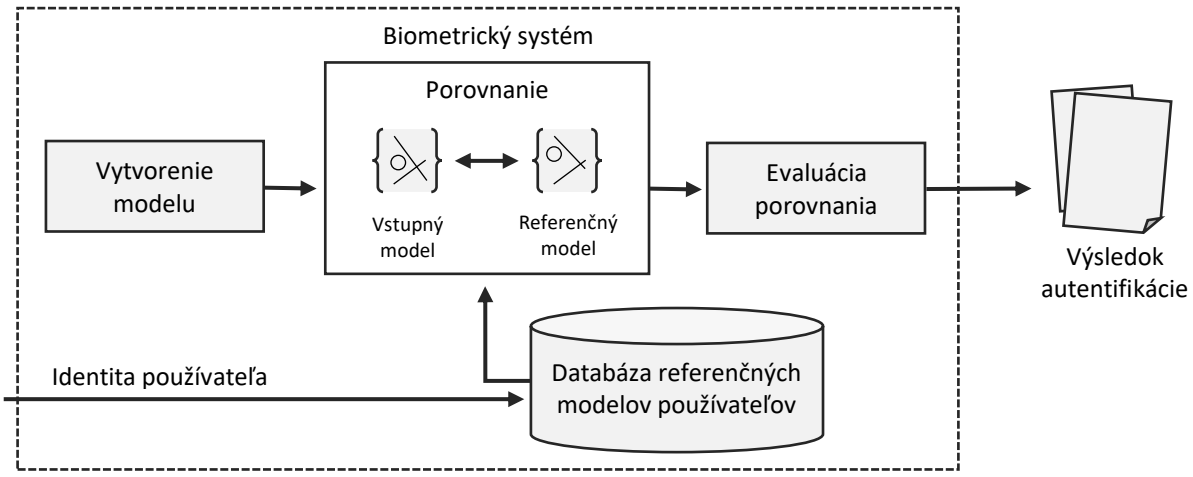
Samotnú evaluáciu je možné vykonávať pomocou rôznych typov klasifikátorov. Medzi najznámejšie klasifikátory (také, ktoré sa v skúmaných prácach uvádzaných v časti 2.7 Podobné práce) vyskytovali najčastejšie), patrí klasifikátor náhodného lesa (angl. Random Forest Classificator), naivný Bayesov klasifikátor (angl. Naive Bayes Classificator) a klasifikátory podporných vektorov (angl. SVM Classifier). Na klasifikáciu sa však často využívajú aj neurónové siete, tie však najmä kvôli vysokej náročnosti natrénovania majú len obmedzené použitie.

2.3 Proces autentifikácie používateľa

V závislosti od účelu a kontextu využitia biometrického systému môže byť biometrický systém používaný na identifikáciu alebo verifikáciu používateľov. Tieto procesy sa mierne líšia, a je preto potrebné sa rozhodnúť, ktorý z nich je vhodný na riešenie konkrétneho problému.

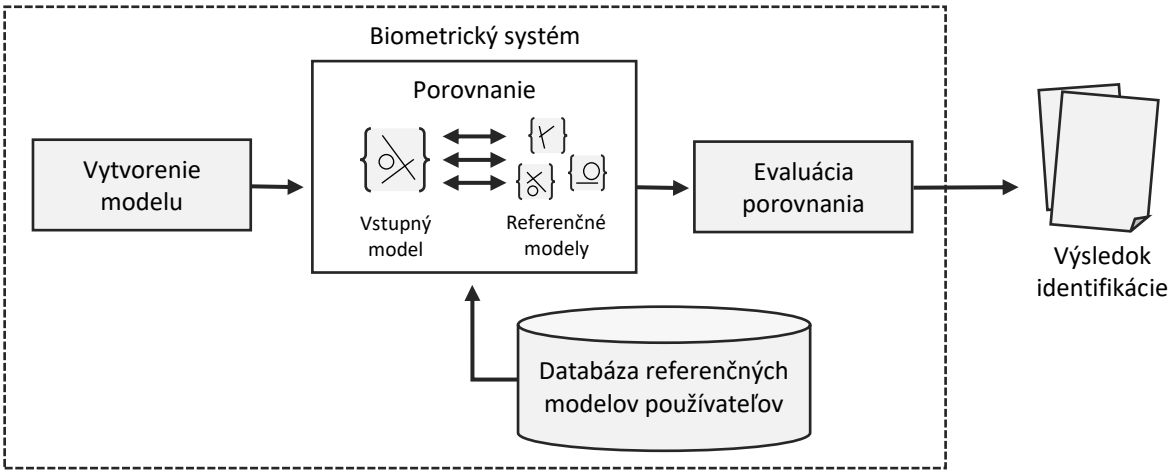
V prácach zaoberajúcich sa biometrickou autentifikáciou používateľov sa stretávame aj s kombináciou oboch prístupov, kedy je identifikácia využitá na výber jedného z referenčných modelov, s ktorým bude porovnávaný aktuálny model používateľa, nakoľko ich môže mať viac z dôvodu vyššej variabilnosti zadávania vstupu (výber ľavej alebo pravej ruky, poloha zariadenia pri používaní). Následne na základe vybraného referenčného modelu dochádza k verifikácii používateľa.

Verifikácia. Verifikácia v biometrickom systéme pozostáva z overenia, či sa aktuálny biometrický model používateľa (zadaný napr. pri prihlásení) zhoduje s referenčným biometrickým modelom používateľa vytvoreným pri registrácii. V procese verifikácie (Obr. 3 Verifikácia používateľa) je známe, s ktorým referenčným modelom sa má aktuálny model používateľa porovnať, nakoľko identita používateľa je vopred známa zadaním jeho mena alebo iného identifikačného znaku. Na základe porovnania jeden voči jednému (angl. One-to-One Comparison) sa následne rozhodne, či bude používateľ akceptovaný.



Obr. 3 Verifikácia používateľa

Identifikácia. Identifikácia používateľa je na rozdiel od verifikácie náročnejší proces, nakoľko v tomto prípade dochádza k porovnaniu biometrických modelov typu jeden voči viacerým (angl. One-to-Many Comparison). K identifikácii používateľa dochádza na základe porovnávania referenčných modelov používateľov a hľadania zhody medzi aktuálnym modelom a referenčným modelom používateľa vytvoreným pri registrácii (Obr. 4 Identifikácia používateľa).



Obr. 4 Identifikácia používateľa

Využitie identifikácie používateľov pomocou biometrických systémov je vhodné v prípadoch, kedy chceme zabrániť používaniu viacerých identít jednou osobou (známe tiež ako negatívne rozpoznanie používateľa, angl. Negative Recognition), kedy nie je možné vykonať skutočné zistenie identity používateľa iným spôsobom ako prostredníctvom sledovania jeho biometrických charakteristík.

2.4 Multibiometrické systémy

Väčšina biometrických systémov pracuje na základe vyhodnotenia biometrických charakteristík používateľa získaných z jedného zdroja, akým je napríklad snímač odtlačkov prstov, rohovky alebo dotykový displej zariadenia. Využitím informačnej fúzie však dokážeme jednotlivé zdroje, ktoré poskytujú rôzne biometrické údaje o používateľoch, spojiť, a dosiahnuť tak zvýšenie presnosti biometrických systémov - vtedy hovoríme o multibiometrických systémoch [ROSS07].

2.4.1 Fúzna biometria

Ako sa uvádza v práci [ROSS07], multibiometrické systémy kombinujú informácie získané z rôznych biometrických senzorov, získané rôznymi algoritmami, z rôznych vzoriek, v rôznych jednotkách alebo z rôznych čŕt používateľa. Okrem dosiahnutia vyššej výkonnosti týchto systémov je tak pomocou kombinácie viacerých charakteristík používateľa možné dosiahnuť aj vyššie pokrytie rôznorodosti biometrických charakteristík populácie, a biometrický systém tak môže byť využívaný vyšším počtom používateľov s pomerne vysokou úspešnosťou.

Hlavnými výhodami využívania multibiometrických systémov pri autentifikovaní používateľov podľa [ROSS07] sú:

- *riešenie neuniverzality dát*, čo pridáva multibiometrickým systémom na flexibilnosti (pri neschopnosti zachytenia jednej z vlastností používateľa môže byť preukázaná identita používateľa na základe inej vlastnosti);
- *riešenie problému škálovateľnosti dát*, nakoľko pri obrovskom množstve dát dochádza k obťažnému filtrovaniu a indexovaniu veľkých databáz používateľov (pri multimodálnych systémoch môže byť výsledok jedného porovnávania použitý ako index na výber vhodných kandidátov do ďalšieho porovnávania, čím sa zníži celkový počet potrebných porovnávaní);
- *dynamickosť autentifikácie* pomocou rôznych kombinácií dostupných biometrických charakteristík v prípade, že sa nedarí dostatočne presne overiť identitu používateľa inými metódami;
- *redukcia šumu*, nakoľko tým, že biometrické vlastnosti používateľov sú získavané z viacerých zdrojov, v prípade zašumených dát z jedného zdroja môžu byť na rozpoznanie používateľa využité dáta z iných zdrojov. Niektoré systémy dokonca pri autentifikácii používateľov pri fúzii zohľadňujú aj kvalitu jednotlivých zachytených

biometrických čŕt na základe ich zašumenia (schopnosť rozpoznania zašumenia dát je kľúčová);

- *robustnosť* v prípade nedostupnosti niektorého z biometrických zdrojov v prípade zlyhania hardvéru, softvéru alebo neoprávneného zásahu používateľa do procesu autentifikácie.

Ako sme už spomínali vyššie, multibiometrické systémy sú závislé na prítomnosti viacerých zdrojov biometrických informácií o používateľoch. Na základe typu zdrojov týchto informácií sa multibiometrické systémy zadeľujú do týchto kategórií [ROSS06]:

1) multi-senzorové – založené na zachytávaní jednej biometrickej charakteristiky používateľa viacerými senzormi (z dôvodu presnosti zachytených dát);
2) multi-algoritmové – založené na viacerých algoritmoch výberu používateľských charakteristík alebo porovnávacích algoritmoch nad jednými biometrickými dátami. Tieto systémy kombinujú výsledky z viacerých algoritmov, a tak aj výpočtová zložitosť týchto systémov narastá;
3) multi-inštančné – tieto systémy kombinujú viaceré inštancie jednej charakteristiky používateľa v rôznych situáciách (ľavé a pravé oko, ruka, jednotlivé prsty);
4) multi-modálne – takéto systémy kombinujú viaceré biometrické vlastnosti pri autentifikácii používateľa. Zvyčajne sa jedná o kombináciu takých charakteristík, ktoré spolu nesúvisia alebo súvisia len minimálne. Zvyšovaním počtu sledovaných charakteristík sa tak dá dosiahnuť rapídne zlepšenie biometrického systému, no v rámci optimalizácie netreba zabúdať na zvyšovanie náročnosti takejto autentifikácie z dôvodu zvyšovania dimenzionality porovnávaných dát (angl. Curse of Dimensionality).
5) hybridné – kombinujú niektoré z vyššie spomínaných typov multibiometrických systémov.

Správne pochopenie možností fúzie biometrických informácií používateľov s využitím informačnej fúzie v multibiometrických systémoch je kľúčové pre hľadanie vhodných kombinácií zdrojov informácií biometrických charakteristík používateľov a pre spájanie týchto informácií pre vytvorenie špecifických charakteristík, ktoré môžu byť použité pri budovaní biometrických modelov používateľov.

Pri autentifikácii a výbere vhodných biometrických charakteristík používateľov je možné vyberať tieto charakteristiky aj pomocou viacerých techník v závislosti od stupňa a zložitosti samotnej charakteristiky. V práci [STALLINGS05] sú rozoberané možnosti

fúzie na úrovni senzorov (angl. Sensor level), charakteristík používateľa (angl. Feature level), skóre (angl. Score level), rozhodnutia (angl. Decision level) a ohodnotenia (angl. Rank level). V tejto práci využili na zvýšenie presnosti biometrického systému techniku fúzie charakteristík používateľa, pri ktorej na identifikovanie používateľa využili kombináciu rôznych charakteristík získaných z viacerých biometrických zdrojov – multimodálnu fúziu. Na vylepšenie výsledkov autentifikácie pridali každému levelu fúzie modality (alebo váhy), a to na základe výkonnosti samotného levelu.

Ako je možné vidieť v prácach [SANDERSON02, ARONOWITZ14], fúziu je možné vykonať pred alebo po procese klasifikácie (angl. Pre-classification, Post-classification Fusion). V prípade pre-klasifikačnej fúzie dochádza k fúzii samotných dát z biometrických senzorov, charakteristík používateľa alebo iných dát používaných pri klasifikáciu používateľa pred vykonaním klasifikácie, pri po-klasifikačnej fúzii dochádza k fúzii výsledkov jednotlivých klasifikátorov [ARONOWITZ14].

2.5 Bezpečnostné opatrenia v biometrických systémoch

V súvislosti s biometrickými systémami je kladený vysoký dôraz aj na dodržiavanie základných bezpečnostných opatrení, ktoré sa týkajú zabezpečenia osobných údajov používateľov pred zneužitím.

Ako sme už spomínali v časti 2.1.1 Charakteristika biometrického systému, biometrické systémy sa využívajú prevažne na zvýšenie zabezpečenia rôznych systémov (medzi nimi aj mobilných zariadení). Na druhej strane však netreba zabúdať na to, že aj pri budovaní biometrických systémov treba zohľadňovať otázky týkajúce sa zabezpečenia týchto systémov. Na túto problematiku poukazuje aj kniha [VIELHAUER06], v ktorej autor zdôrazňuje potrebu zabezpečenia používateľských dát, ktoré sú zbierané za účelom vytvárania referenčných modelov používateľova a používané pri porovnávaní počas vykonávania autentifikačného procesu používateľa.

Na zabezpečené uchovávanie biometrických údajov o používateľoch je možné tieto dáta šifrovať, aby aj v prípade, že niekto dokáže pristúpiť k týmto dátam, budú ochránené voči zneužitiu. V súčasnosti je možné využiť niekoľko dostupných kryptografických metód a hashovacích funkcií, ktoré je možné zohľadniť pri budovaní zabezpečenia nami navrhovaného biometrického systému na mobilných zariadeniach.

2.6 Meranie presnosti biometrických systémov

Biometrické systémy pracujú s vysokým množstvom biometrických modelov používateľov, ktoré využívajú pri autentifikácii používateľov. K správnemu a spoľahlivému fungovaniu takýchto systémov je potrebná dostatočná miera odlíšiteľnosti jednotlivých používateľov. Zaznamenávanie biometrických charakteristík používateľov biometrických systémov by však malo byť opakovateľné pre každého používateľa, čo znamená, že zachytené biometrické charakteristiky by mali byť pri každej autentifikácii podobné. Nakoľko však tieto systémy pracujú nedeterministicky (pretože zaznamenané biometrické charakteristiky používateľov nezávisia len od identity daných používateľov ale aj od prostredia, zmien v správaní či v spôsobe používania zariadenia), presnosť týchto systémov nie je možné formálne vyjadriť [VIELHAUER06]. Evaluácia presnosti fungovania takýchto systémov môže byť vykonaná prostredníctvom testovaní na reálnych dátach a štatistickej analýze úspešnosti autentifikácie používateľov týchto systémov.

Nakoľko testovacie prostredie nemusí vždy zodpovedať prevádzke systému v reálnom prostredí, aj spoľahlivosť biometrických systémov môže byť pri nasadení rozdielna. V prácach, ktoré sa zaoberajú vývojom biometrických systémov, sa však najčastejšie stretávame s ohodnotením presnosti týchto systémov pomocou šiestich typov metrík, ktoré uvádzame v Tab. 2 Metriky pre vyhodnotenie úspešnosti biometrických systémov. Opis jednotlivých typov metrík uvádzame podľa [VIELHAUER06].

Tab. 2 Metriky pre vyhodnotenie úspešnosti biometrických systémov

Metrika	**Vysvetlenie**
FMR	*Angl. skr. False Match Rate* Pomer medzi počtom nezhodných zhôd, ktoré systém vyhodnotil správne a celkovým počtom vykonaných vyhodnocovaní.
FNMR	*Angl. skr. False Non-Match Rate* Pomer medzi počtom zhodných zhôd, ktoré systém nevyhodnotil správne a celkovým počtom vykonaných vyhodnocovaní.
EER	*Angl. skr. Equal-Error-Rate* Určuje bod, v ktorom sa pravdepodobnosť nesprávne akceptovaných a nesprávne neakceptovaných vyhodnotení systému vyrovná.
BER	*Angl. skr. Binning Error Rate* Pomer nesprávne nezhodných zhôd spôsobený chybami pri rozdeľovaní databázy referenčným modelov používateľov (pri systémoch, u ktorých je potrebné rozdelenie databázy používateľov z dôvodu vysokého počtu

	používateľov).
PC	*Angl. skr. Penetration Coefficient* Priemerná percentuálna veľkosť databázy, ktorú je potrebné prehľadať pri každom autentifikačnom procese (pri systémoch, u ktorých je potrebné rozdelenie databázy používateľov a potrebná podpora rozdeľovania modelov používateľov do viacerých partícií tejto databázy)
TT	*Angl. skr. Transaction Time* Čas potrebný na vykonanie jednej autentifikačnej požiadavky (vypočítaný ako súčet časov prístupu k používateľským dátam a vykonania autentifikácie).

V mnohých prácach sa stretávame s určením pravdepodobností chybného odmietnutia (angl. skr. FAR - False Acceptance Rate) alebo chybného akceptovania (angl. skr. FRR - False Rejection Rate) používateľa. Miera FAR určuje pravdepodobnosť, že biometrický systém nesprávne autentifikuje používateľa a umožní mu neautorizovaný prístup do zariadenia, FRR predstavuje pravdepodobnosť, že autorizovanému používateľovi bude zamietnutý prístup do zariadenia, a EER určuje bod, v ktorom sa pravdepodobnosť nesprávne akceptovaných a nesprávne neakceptovaných prístupov do zariadení vyrovná. Čím je hodnota EER nižšia, tým je možné biometrický systém považovať za presnejší [SCHLENKER13].

V rámci optimalizácie a zvyšovania úspešnosti (presnosti) nami navrhovaného biometrického systému sa sústredíme na znižovanie hodnoty EER. Hoci miera EER priamo neurčuje vhodnosť nastavenia biometrického systému na parametre s najnižšou hodnotou EER, táto miera môže byť použitá ako prvotné ohodnotenie presnosti biometrického systému [VIELHAUER06].

2.7 Podobné práce

Ako sme už načrtli v predchádzajúcich častiach tejto práce, autentifikáciu používateľa je možné vykonávať rôznymi spôsobmi. V tejto časti sa tak venujeme skúmaniu iných prác, ktoré vykonávali autentifikáciu používateľov pomocou rôznych prístupov a pre rôzny účel.

Existujú techniky, kedy je autentifikácia používateľa vykonávaná staticky, čo znamená, že správanie používateľa je sledované iba počas špecifických a zvyčajne krátkych udalostí, akými je napríklad zadávanie hesla pri prihlasovaní do zariadenia [SANDHYA16]. Tento prístup k zabezpečeniu zariadenia je určite účinnejší ako prihlasovanie prostredníctvom hesla bez ďalších podporných zabezpečovacích mechanizmov, no

neposkytuje zabezpečenie zariadenia počas doby jeho používania po úspešnom prihlásení sa do zariadenia. Pre zabezpečenie zariadenia aj počas doby jeho používania existujú ďalej dynamické prístupy sledovania biometrických charakteristík používateľa, ktoré monitorujú správanie používateľa pri dlhodobom používaní tohto zariadenia [SANDHYA16].

Problematikou identifikácie používateľa na základe jeho biometrických charakteristík sa už v minulosti zaoberalo viacero prác. V prvých fázach sledovania biometrie človeka pre jeho lepšiu autentifikáciu sa vykonávalo sledovanie jeho biometrických charakteristík prostredníctvom dynamiky písania na klávesnici počítača. Pri týchto experimentoch boli sledované doby stláčania jednotlivých kláves klávesnice alebo doby medzi stlačeniami jednotlivých párov kláves. Výsledky týchto sledovaní boli potom použité pri tvorbe modelu používateľov, na základe ktorých následne dochádzalo k ich autentifikácii [BERGADANO02, MESZAROS07, SCHLENKER13]. V niektorých prácach okrem dynamiky stláčania kláves skúmali aj ďalšie charakteristiky, akými sú napríklad postupnosti stlačení viacerých kláves za sebou (n-grafy). Pridaním ďalších charakteristík sa postupne podarilo dosahovať lepšie výsledky pri autentifikácii používateľov.

Pri moderných mobilných zariadeniach, kedy má dotyková obrazovka zariadenia za úlohu sprostredkovanie podstatnej časti interakcie medzi používateľom a zariadením, je možností sledovania biometrických charakteristík používateľov omnoho viac. V niektorých prácach sa tak zaoberali možnosťami rozšírenia modelu používateľov smartfónových zariadení o charakteristiky, akými sú napríklad pozície stlačení jednotlivých kláves na digitálnej klávesnici (dotykovej obrazovke), či zaznamenávanie tlaku pri stláčaní jednotlivých kláves pri písaní na obrazovku zariadenia [NGUYEN17, RAO14].

V niektorých prácach sa spomína využitie odomykacieho vzoru ako jednoduchšieho spôsobu odomykania zariadenia, nakoľko je u ľudí lepšie vyvinutý zmysel pre zapamätanie si tvarov ako postupnosti čísel [BIDDLE12] (znakových/číselných hesiel). Výsledky niektorých prác poukazujú na to, že používanie grafických hesiel má pre používateľa viacero výhod, akými sú napríklad ich krátka doba nastavenia alebo prihlásenia sa do zariadenia ich nakreslením, nižší počet chybne zadaných pokusov alebo potreba nižšieho sústredenia sa používateľa oproti zadávaniu klasických znakových hesiel pre odomknutie zariadenia [ABARI08].

V práci [FRANK13] sa stretávame s odlišným prístupom k autentifikácii používateľa, nakoľko sa v tejto práci snažili identifikovať možnosti dynamického verifikovania identity používateľa. V tejto práci sa zaoberali tvorbou modelu používateľa na základe posunu prsta po obrazovke zhora-nadol a zľava-doprava (najčastejšie pohyby po

obrazovke), pričom z charakteristík vykonávaných pohybov vytvárali model používateľa. Výsledky tejto práce poukazujú na to, že táto metóda nie je úplne vhodná pre kontinuálne verifikovanie používateľov, no na základe výsledkov usúdili, že túto metódu by bolo lepšie uplatniť pri statickom overovaní identity používateľa pri prihlasovaní do zariadenia.

Využitie gyroskopu pri rozšírení biometrického modelu používateľa sa zdá byť tiež jedným zo spôsobov, ktorými sa dá zvýšiť úspešnosť autentifikácie používateľov. Využitím dát z polohovacích senzorov pri identifikácii používateľa sa zaoberali v prácach [CORPUS16, PARK16] a [GIOFFRIDA14]. V práci [LIN12] sa zaoberali tvorbou modelu používateľa na základe rôznych gest, ako napríklad posunu prsta po obrazovke zhora-nadol a zľava-doprava, podobne ako v práci [FRANK13], no na rozdiel od spomínanej práce využívali pri tvorbe modelu používateľa aj dáta z polohovacích senzorov mobilného zariadenia. V tejto práci vychádzali z hypotézy, že každý používateľ drží zariadenie počas zadávania hesla (používania zariadenia) jedinečným spôsobom, a tak sledovanie tejto charakteristiky môže taktiež napomôcť pri zdokonalení modelu používateľa a následne k jeho presnejšej autentifikácii.

V práci [ALARIKI16] sa dozvedáme, že výber sledovaných biometrických charakteristík používateľov pri budovaní ich biometrických modelov môže byť taktiež výrazným problémom a môže mať priamy vplyv na úspešnosť autentifikácie používateľa. V uvádzanej práci sa tak zaoberali extrakciou rôznych kombinácií biometrických charakteristík používateľa a vytváraním modelu používateľov, na základe ktorých sa následne použitím diskriminačného klasifikátora snažili nájsť kombináciu charakteristík, ktorá by urobila identifikáciu používateľa čo najpresnejšou (angl. Feature Selection). Vhodným výberom charakteristík používateľa sa im podarilo prekonať iné existujúce prístupy, a to využitím popredného výberu skupiny charakteristík správania používateľa algoritmom Náhodného lesa (angl. Random Forest Algorithm).

Ako posledné uvádzame výsledky dosiahnuté v prácach [ARONOWITZ14] a [BURIRO16]. Tieto práce sú zaujímavé tým, že pri autentifikácii používateľov využívajú princípy informačnej fúzie. V práci [ARONOWITZ14] na informačnú fúziu využili biometrické charakteristiky tváre, odtlačku prsta a hlasu používateľov, preto je úspešnosť tohto systému veľmi vysoká. V tejto práci je však zaujímavé predstavenie spôsobu spájania používateľských charakteristík na úrovni skóre jednotlivých klasifikácií podľa druhu sledovanej charakteristiky. Práca [BURIRO16] sa venuje fúznej biometrii na mobilných zariadeniach s využitím dát z dotykovej obrazovky zariadenia, polohovacích senzorov (akcelerometer a gyroskop) pri zdvíhaní zariadenia (v prípade prichádzajúceho hovoru)

a z mikrofónu zariadenia (priebeh hovoru, rozpoznávanie hlasu). V práci je zhodnotený vplyv informačnej fúzie pri spojení dotykov, pohybov a hlasu ale aj iba dotykov a pohybov na výsledok autentifikácie (pre nás je výsledok s hlasom nezaujímavý, nakoľko sa mu nevenujeme). Výsledky tejto práce tak rovnako ako v prípade [ARONOWITZ14] poukazujú na viaceré výhody využitia informačnej fúzie v procese autentifikácie používateľov biometrického systému (hlavne rýchlosť a presnosť) oproti klasickým prístupom k autentifikácii používateľa (v práci sú priamo uvedené porovnateľné výsledky).

Pre sumarizáciu skúmaných existujúcich prístupov sme získané pozorovania zhrnuli v Tab. 3 Sumarizácia existujúcich prístupov a Tab. 4 Dosahované výsledky analyzovaných prác. V Tab. 3 Sumarizácia existujúcich prístupov uvádzame typy zariadení, metódy získavania biometrických vzoriek a spôsob testovania biometrických systémov spolu s typom autentifikácie. V Tab. 4 Dosahované výsledky analyzovaných prác uvádzame výsledky dosahované pri využití jednotlivých prístupov spolu s informáciami o spôsobe vykonania experimentu (počet ľudí v experimente), počte sledovaných charakteristík, ktoré boli použité na budovanie modelu používateľov, a výsledkami jednotlivých prác (miery FAR, FRR a EER – ak boli uvedené).

Tab. 3 Sumarizácia existujúcich prístupov

Zn.	**Zariadenie**	**Metóda**	**Testovanie**	**Typ autentifikácie**
1	Klávesnica	doba stlačení kláves doba medzi stlačeniami kláves	písaný text	statická
2		postupnosti stlačení kláves (n-gramy)	písaný text	statická
3	Dotyková obrazovka	pozície stlačení kláves	písaný text	statická
4		tlak stláčania kláves	písaný text	statická
5		dynamika kreslenia	kreslenie vzoru	statická
6		dynamika posunu prsta po obrazovke	posuny zľava-doprava a zhora-nadol	dynamická
7	Akcelerometer a gyroskop	nakláňanie zariadenia	písaný text	statická
8	Akcelerometer, gyroskop a dotyková obrazovka	dynamika posunu prsta po obrazovke nakláňanie zariadenia	posuny zľava-doprava a zhora-nadol	statická

Tab. 4 Dosahované výsledky analyzovaných prác

Práca	**Typ**[2]	**Zapojených ľudí do experimentu**	**Počet sledovaných charakteristík**	**FAR**	**FRR**	**EER**
[BERGADANO02]	1, 2	44	-	0,04	-	-
[MESZAROS07]	1	25	-	-	-	0,100
[SCHLENKER13]	1	-	-	-	-	-
[NGUYEN17]	3, 4, 6	10	-	-	-	0,070
[RAO14]	3, 4, 8	4	-	0,03	0,03	0,010
[FRANK13]	6	41	30	-	-	0,040
[CORPUS16]	1, 2, 8	30	-	0,07	0,4	-
[PARK16]	1, 2	94	48	-	-	0,007
[GIOFFRIDA14]	1, 2, 3, 7	10	-	-	-	0,008
[LIN12]	7	20	53	-	0,28	0,069
[ALARIKI16]	3, 4	13	84	0,01	0,08	0,083
[BURIRO16]	3, 4, 8	26	-	0,11	0,04	0,076

Z analýzy skúmaných prác vyplýva, že na úspešnosť jednotlivých spôsobov autentifikácie má vplyv viacero faktorov. Jednotlivé metódy sa okrem rozdielneho počtu skúmaných charakteristík odlišovali v zariadeniach, ktoré boli pre sledovanie biometrických charakteristík používateľov využívané. Každá z prác taktiež sledovala odlišné biometrické charakteristiky používateľa (doby stlačenia kláves, posun prsta po obrazovke, nakláňanie zariadenia) a aj samotná množina testovacích vzoriek tak v každej práci pozostávala z iného typu a počtu biometrických charakteristík.

Najnižšiu hodnotu FAR (angl. False Acceptance Rate) mali práce, u ktorých bola vykonávaná statická autentifikácia a porovnávanie biometrických vzoriek bolo vykonávané na vysokom počte testovaných vzoriek (počet vzoriek však nezodpovedal počtu ľudí zapojených do experimentu). Z analýzy prác však bolo zrejmé, že čím bol počet ľudí zapojených do experimentu vyšší, hodnota FAR sa zvyšovala (presnosť biometrického systému klesala).

Zaujímavé však bolo pozorovanie, že v prácach, v ktorých využívali na

[2] Typ práce je určený podľa Zn. v Tab. 3 Sumarizácia existujúcich prístupov

autentifikáciu používateľov aj natívne senzory mobilných zariadení (akcelerometer alebo gyroskop), bola hodnota EER nižšia ako v prácach, kde dáta z týchto senzorov nevyužívali.

Jednotlivé práce sa taktiež líšili v typoch použitých metód, ktoré boli využité pri výbere vhodných charakteristík používateľov a tiež v typoch klasifikátorov (najúspešnejšie klasifikátory angl. Naive Bayes, Random Forest, Sequential Minimal Optimization, Neural Net), ktoré používali pri finálnej autentifikácii používateľov.

2.8 Zhrnutie analýzy aktuálneho stavu problematiky

Cieľom tejto časti diplomovej práce bolo vytvorenie prehľadu o skúmanej problematike autentifikácie používateľov na mobilných zariadeniach. V časti 2.1 Biometria na mobilných zariadeniach sme predstavili charakteristické vlastnosti biometrických systémov a základné vlastnosti, ktoré by mal spĺňať biometrický model používateľa. V časti 2.3 Proces autentifikácie používateľa sme zhrnuli základné kroky procesu autentifikácie používateľov, priblížili sme výhody a nevýhody multibiometrických systémov, načrtli sme otázky týkajúce sa zabezpečenia týchto systémov a zhrnuli sme metriky pre určovanie presnosti systémov na autentifikáciu používateľov.

V poslednej časti analýzy sme skúmali existujúce riešenia v oblasti biometrickej autentifikácie používateľov, ktoré sa odlišovali v prístupe, spôsobe a úspešnosti vytvorených autentifikačných systémov.

Na základe analýzy existujúcich riešení je zrejmé, že autentifikáciu používateľov s využitím biometrie na mobilných zariadeniach je možné vykonávať rôznymi spôsobmi. V prípade biometrických fyziologických charakteristík, akými sú napríklad odtlačky prstov, snímky tváre alebo rohovky, je variabilnosť jednotlivých prístupov k zariadeniu pomocou týchto charakteristík pomerne malá a tieto systémy pracujú s vysokou úspešnosťou. V prípade využívania behaviorálnych charakteristík používateľa pri autentifikácii je však problém s vysokou variabilitou získaných dát od jedného používateľa pri každom opakovanom prístupe, nakoľko behaviorálne charakteristiky používateľov nie sú ovplyvnené len časom, ale aj stavom samotného používateľa. V prípade, že je používateľ unavený, má mastné, spotené ruky alebo je pod stresom, spôsob jeho správania a práce so zariadením je podstatne odlišný ako v prípade normálneho stavu. Zachytené behaviorálne biometrické charakteristiky sa tak často menia aj v priebehu dňa.

Z analýzy skúmaných prác je zrejmé, že zachytené biometrické charakteristiky používateľov sa častokrát odvíjajú aj od spôsobu práce so zariadením alebo od typu

používaného zariadenia. V prípade, že používateľ stojí, sedí, leží alebo kráča, presnosť a spoľahlivosť biometrického systému výrazne klesá. V prípade rozdielnosti zariadení (typ dotykovej klávesnice, veľkosť displeja, veľkosť rozlíšenia) tiež dochádzalo k znižovaniu presnosti týchto systémov, takže aj túto skutočnosť je potrebné zohľadňovať pri návrhu autentifikačných systémov.

Na základe poznatkov získaných v tejto časti diplomovej práce sme ďalej pokračovali pri návrhu, implementácii a overení nami navrhnutého riešenia na autentifikáciu používateľov na mobilných zariadeniach s využitím ich behaviorálnych biometrických charakteristík.

3 Ciele práce a výskumné hypotézy

Na základe analýzy skúmaného problému sme zistili, že okrem hľadania spôsobu porovnávania biometrických modelov používateľov je dôležitý aj samotný spôsob vytvárania biometrického modelu používateľa. Na základe tohto zistenia sme sa rozhodli zamerať na problematiku výberu vhodných charakteristík, ktoré by bolo vhodné využiť pri budovaní modelov používateľov. Pri výbere vhodných biometrických charakteristík sa pokúsime zohľadniť všetky možnosti sledovania biometrických charakteristík za pomoci dotykového displeja a polohovacích senzorov mobilného zariadenia (smartfónu) pri prihlasovaní používateľa do tohto zariadenia. Zameriame sa teda na výber vhodných čŕt pre zdokonalenie statickej autentifikácie používateľa pre zabezpečenie prístupu k zariadeniu, čím vytvoríme dvojstupňové zabezpečenie zariadenia pozostávajúce zo zadania odomykacieho vzoru a overenia biometrického modelu používateľa.

Medzi ciele skúmania a tvorby biometrického systému pod smartfónovou platformou teda zaraďujeme:

1) vytvorenie metódy na zbieranie a predspracovanie biometrických dát od používateľa pomocou dát z dotykového displeja a polohovacích senzorov zariadenia;
2) vytvorenie spoľahlivej metódy na budovanie biometrického modelu používateľa;
3) vytvorenie metódy na autentifikáciu používateľa na základe jeho biometrických charakteristík;
4) overenie možnosti využitia informačnej fúzie pre účely zvýšenia úspešnosti autentifikácie.

3.1 Výskumné hypotézy

V rámci skúmania problematiky zabezpečenia mobilných zariadení pomocou biometrickej autentifikácie používateľov sme dospeli k niekoľkých hypotézam, ktorým sa ďalej venujeme v tejto diplomovej práci.

Hypotéza 1. Pri skúmaní riešeného problému sme dospeli k predpokladu, že výber menšej množiny charakteristík, ktoré sa u používateľov odlišujú v najväčšej miere, má nepriamy vplyv na hodnotu chyby EER, ktorá určuje kvalitu navrhnutého biometrického systému.

Túto hypotézu budeme overovať experimentami, v ktorých určíme množiny sledovaných charakteristík vytvorené na základe výsledkov ohodnotenia

najsignifikantnejších charakteristík s rôznou veľkosťou. Následne, pomocou týchto množín vykonáme navrhnutý proces autentifikácie používateľov a v prípade, že nájdeme menšie množiny charakteristík, ktoré vykazujú vyššiu úspešnosť ako množiny s vyšším počtom charakteristík (obsahujúce menšiu množinu), túto hypotézu budeme považovať za platnú.

Hypotéza 2. Našu ďalšiu hypotézu zakladáme na možnosti využitia informačnej fúzie na úrovni porovnávacieho skóre. Predpokladáme, že využitím prístupu informačnej fúzie na úrovni porovnávacieho skóre (al. angl. ensemble), v ktorom je finálny výsledok autentifikácie dosiahnutý vhodným spojením výsledkov klasifikácie viacerých klasifikátorov (2-úrovňový), dokážeme zvýšiť presnosť biometrického systému a znížiť náročnosť výberu signifikantných charakteristík rozdelením na menšie podmnožiny.

Pre overenie tejto hypotézy natrénujeme sadu klasifikátorov pre vzorovo závislé a vzorovo nezávislé charakteristiky a pomocou metódy „ensemble“ vytvoríme 2-úrovňový klasifikátor, ktorý bude autentifikovať používateľov v 2 krokoch (viacnásobná „Single-Class“ klasifikácia a ohodnotenie používateľa „áno/nie“). V prípade, že sa presnosť biometrického systému zvýši pre menšie množiny charakteristík (hodnota EER sa zníži), túto hypotézu budeme považovať za platnú.

Hypotéza 3. V rámci možností budovania biometrického modelu používateľa sme dospeli k ďalšej hypotéze, v ktorej predpokladáme, že postupné prispôsobovanie modelu používateľa počas používania biometrického systému môže zvýšiť presnosť autentifikácie používateľa, nakoľko sa aj samotná technika používateľa viacnásobným zadávaním odomykacieho vzoru na zariadení postupne zdokonaľuje a správanie používateľa sa časom mení.

Túto hypotézu overíme dlhodobým sledovaním používateľských charakteristík tak, že používateľ bude zadávať 1 typ odomykacieho vzoru 1 spôsobom po dobu niekoľkých dní, aby sa ho dokonale naučil. Natrénovanie klasifikátora na autentifikáciu používateľa vykonáme vždy nanovo odstránením najstarších a pridaním najnovších biometrických dát. V prípade, že sa presnosť biometrického systému bude postupom času bez zmeny sledovaných charakteristík prirodzene zlepšovať, túto hypotézu budeme považovať za platnú.

4 Návrh biometrického systému

Táto časť diplomovej práce obsahuje opis riešenia jednotlivých etáp práce na návrhu biometrického systému pre Android platformu. Uvádzame tu ciele projektu, špecifikáciu požiadaviek vytváraného systému na autentifikáciu používateľa, návrh a spôsob implementácie vytváraného biometrického systému.

4.1 Ciele projektu

V tejto časti špecifikujeme hlavné ciele tvorby systému na autentifikáciu používateľa pomocou jeho biometrických charakteristík. Medzi hlavné ciele vytvorenia systému na podporu zabezpečenia mobilných zariadení zaraďujeme:

- vytvorenie metódy na zbieranie biometrických údajov od používateľov,
- vytvorenie metódy na budovanie biometrických modelov používateľov,
- vytvorenie metódy na výber dominantných charakteristík pre porovnávanie biometrických modelov,
- vytvorenie metódy na porovnávanie biometrických modelov za účelom autentifikácie používateľov,
- zvýšenie zabezpečenie mobilných zariadení využitím informačnej fúzie pri prihlasovaní používateľa do mobilnej aplikácie.

4.2 Špecifikácia požiadaviek

Táto časť obsahuje požiadavky na vytváraný biometrický systém. Tieto požiadavky vznikali postupne v procese analýzy existujúcich riešení, na základe ktorých sme stanovili základné predpoklady pre správne a efektívne fungovanie biometrického systému.

Vytváraný biometrický systém pre mobilné zariadenia bude umožňovať zachytávanie a následné spracovávanie biometrických charakteristík od používateľov za účelom tvorby ich biometrických modelov. Na zachytávanie biometrických charakteristík bude využívať dáta z dotykového displeja a mobilných polohovacích senzorov, ktoré podporuje Android platforma pri zadávaní štandardného odomykacieho vzoru. K tvorbe a overovaniu modelov používateľov bude dochádzať priamo na centrálnom serveri, pričom prístup do aplikácie bude vyžadovať prístup k databáze používateľských modelov dostupných online

Pre používanie biometrického systému bude potrebné, aby sa používateľ najskôr zaregistroval. Registrácia prebehne zaregistrovaním dostatočne veľkého počtu referenčných

biometrických modelov pre každý kontext odomykania, ktoré budú následne využívané pri identifikácii kontextu odomykania a autentifikácii používateľa (aby bola presnosť biometrického systému čo najvyššia, systém bude schopný identifikovať, akým štýlom bol odomykací vzor používateľom zadaný - ľavá alebo pravá ruka, typ prsta, zariadenie uchopené v rukách alebo položené na stole).

4.2.1 Funkcionálne požiadavky

V tejto časti sme zhrnuli všetky identifikované funkcionálne požiadavky na vytváraný biometrický systém.

- **Zaznamenávanie biometrických dát používateľa pomocou natívnych senzorov a dotykovej obrazovky zariadenia.** Vytváraný biometrický systém dokáže spracovať dáta zachytené pomocou natívnych senzorov a dotykovej obrazovky na smartfónovej platforme. Biometrické dáta budú získavané zo senzorov s najvyššou možnou frekvenciou.
- **Vytváranie modelu používateľa zo zaznamenaných dát.** Na základe získaných dát bude systém vytvárať modely používateľov. Zo surových dát dopočíta ďalšie charakteristiky, ktoré sú potrebné pre vytvorenie modelu používateľa.
- **Identifikácia spôsobu prihlásenia používateľa do aplikácie**. Systém bude schopný pomocou vybraného klasifikátora rozoznať, akým spôsobom bol zadaný odomykací vzor (poloha zariadenia, ruka, prst).
- **Autentifikácia používateľa pri prihlásení do aplikácie.** Systém bude schopný verifikovať identitu používateľa na základe jeho referenčného modelu. Referenčný model používateľa bude pozostávať z niekoľkých biometrických modelov podľa toho, akým spôsobom boli zadané (poloha zariadenia, ruka, prst). Pre zvýšenie presnosti autentifikácie bude systém využívať metódu informačnej fúznej biometrických charakteristík používateľa a výsledku klasifikácie.
- **Aktualizácia modelu používateľa pri viacnásobnom prihlasovaní do aplikácie.** Biometrický systém bude priebežne na základe naposledy zaznamenaných biometrických dát aktualizovať biometrický model používateľa.
- **Šifrovanie používateľských dát pre ochranu proti zneužitiu.** Pre ochranu používateľských dát proti zneužitiu budú biometrické dáta používateľov šifrované.

4.2.2 Nefunkcionálne požiadavky

Efektívnosť. Klientska časť vytváraného systému nebude vyžadovať vysoké hardvérové špecifikácie, ale bude spustiteľná aj na starších Android zariadeniach so systémom Android od verzie API 15 a novším. Autentifikácia používateľov bude prebiehať online v reálnom čase.

Bezpečnosť. Biometrický systém bude dáta o používateľoch šifrovať a následne odosielať na vzdialený server pre autentifikáciu, čím bude tieto dáta chrániť proti zneužitiu. Používateľské dáta budú šifrované aj priamo na strane servera pri ukladaní do databázy.

Použiteľnosť. Systém bude možné ľahko používať, bude mať intuitívne nastavenia a jednoduchú správu používateľských kont.

Dostupnosť. Biometrický systém bude možné používať iba pri spojení so vzdialeným serverom slúžiacim na online autentifikáciu používateľa porovnávaním jeho biometrických modelov. Všetky modely, ktoré vzniknú v tomto prípade, budú uchovávané priamo na strane servera.

Spoľahlivosť. Vytváraný systém bude pracovať s dostatočne veľkou presnosťou, pričom bude prevažovať počet správnych autentifikácií používateľov nad nesprávnymi (hodnota chyby EER nie vyššia ako 0.1).

4.3 Návrh riešenia autentifikácie používateľa

V tejto časti diplomovej práce sa bližšie venujeme softvérovému návrhu vytváraného biometrického systému. Identifikujeme a navrhujeme tu procesy súvisiace s autentifikáciou používateľov na mobilných zariadeniach.

4.3.1 Procesy autentifikácie používateľa

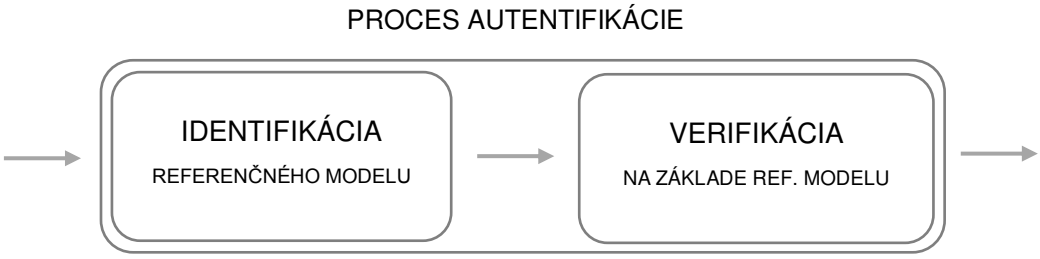
Samotná autentifikácia používateľa pomocou biometrického systému bude pozostávať z nasledujúcich krokov:

1) Získanie prvotných biometrických údajov od vlastníka zariadenia pre vytvorenie jeho referenčného modelu;
2) Natrénovanie klasifikátora pre identifikáciu spôsobu zadania odomykacieho vzoru používateľom (angl. Multi-Class Classification);
3) Natrénovanie „Single-Class“ klasifikátora pre verifikáciu používateľa na základe jeho referenčného modelu (angl. Single-Class Classification) - vlastník áno/nie;
4) Autentifikácia používateľa pri prístupe do zariadenia (Obr. 5 Proces autentifikácie

používateľa na základe referenčného modelu)

a) Výber referenčného modelu pre verifikáciu používateľa (na základe identifikácie spôsobu odomknutia zariadenia);
b) Verifikácie aktuálneho modelu používateľa s vybraným referenčným modelom;

5) Pri rozpoznaní autorizovaného prístupu uloženie získanej vzorky k vzorkám používateľa pre aktualizáciu modelu používateľa na základe získaných biometrických dát pri odomykaní (postupné prispôsobovanie modelu používateľa).



Obr. 5 Proces autentifikácie používateľa na základe referenčného modelu

Pre zabezpečenie navrhnutej funkcionality je tak potrebné realizovať niekoľko základných procesov pri vytváraní a overovaní biometrického modelu používateľa (popis jednotlivých procesov uvádzame nižšie; diagramy k uvedeným procesom uvádzame v prílohe Príloha B: Procesy biometrického systému).

P1 Natrénovanie klasifikátora kontextu odomknutia. V procese autentifikácie používateľov predpokladáme, že dokážeme úspešne identifikovať kontext používateľa pri zadávaní odomykacieho vzoru (poloha, ruka, prst). Klasifikátor kontextu odomykania bude natrénovaný na základe dát od všetkých používateľov, pričom tento klasifikátor bude používaný pre určovanie kontextu u všetkých používateľov spoločne.

Po predspracovaní a vyhľadaní anomálií vo všetkých vzorkách odomykania získaných od používateľov systému (vzorka dát, v ktorej sú zastúpené všetky kontexty podporované systémom) vyhľadá takú množinu charakteristík, pre ktorú je presnosť klasifikácie pre vybranú množinu vzoriek odomykania najvyššia (určenie spôsobu odomykania je najúspešnejšie).

Pomocou tejto množiny následne natrénuje klasifikátor, ktorý bude používaný pri určovaní kontextu používateľov. Tento klasifikátor je potrebné počas existencie systému pri definovaní nového kontextu odomknutia aktualizovať, aby bolo možné tento kontext identifikovať.

P2 Získanie vzorovo nezávislých čŕt pre budovanie vzorovo nezávislého modelu používateľa. Pre získanie optimálneho počtu charakteristík, ktoré sa medzi používateľmi odlišujú v najväčšej miere, sa vykoná na základe dostupných vzoriek od rozličných používateľov (bez ohľadu na odomykací vzor) výber dominantných charakteristík pre každý z kontextov odomykania, ktoré v systéme existujú. Typ vybraných charakteristík nebude závislý na tvare odomykacieho vzoru, nakoľko predpokladáme, že existujú charakteristiky, ktoré nie sú vzorovo závislé (angl. Pattern Independant, skr. PI).

Vznikne tak množina charakteristík, ktorá sa následne použije pri natrénovaní modelu používateľa ako jedného z 2 modelov použitých pri autentifikácii používateľa s využitím informačnej fúzie na úrovni porovnávacieho skóre (vzorovo nezávislý model).

P3 Získanie vzorovo závislých čŕt pre budovanie vzorovo závislého modelu používateľa. Pre získanie optimálneho počtu charakteristík, ktoré sa medzi používateľmi odlišujú v najväčšej miere, sa vykoná na základe dostupných vzoriek od konkrétneho používateľa a vzoriek od rozličných používateľov (s ohľadom na odomykací vzor) výber dominantných charakteristík pre každý z kontextov odomykania, ktoré v systéme existujú. Typ vybraných charakteristík bude závislý na tvare odomykacieho vzoru, nakoľko predpokladáme, že existujú charakteristiky, ktoré sú vzorovo závislé (angl. Pattern Dependant, skr. PI) a ich odlíšenie od vzorovo nezávislých dát môže zvýšiť úspešnosť autentifikácie.

Vznikne tak množina charakteristík, ktorá sa následne použije pri natrénovaní modelu používateľa ako jedného z 2 modelov použitých pri autentifikácii používateľa s využitím informačnej fúzie na úrovni porovnávacieho skóre (vzorovo závislý model). Vybraná množina charakteristík sa použije pri vytváraní modelu používateľa (nastavenie odomykacieho vzoru).

Obmedzením tohto procesu, a teda rozdelenia charakteristík na vzorovo závislé a nezávislé, je predpoklad existencie dostatočného množstva vzoriek od ostatných používateľov pre vybraný odomykací vzor pre výber charakteristík odlišujúcich jednotlivých používateľov v najväčšej možnej miere.

P4 Nastavenie odomykacieho vzoru používateľom. Proces nastavenia odomykacieho vzoru používateľom prebieha na mobilnom zariadení aj na systémovom serveri, ktorý zabezpečuje autentifikáciu používateľov.

Pre vytvorenie modelu používateľa je nutné, aby si používateľ zvolil kontext,

v ktorom chce daný vzor používať. Následne je potrebné, aby pre daný kontext vykonal dostatočne veľké množstvo odomknutí pre vybraný vzor (logovanie dát), z ktorých sa následne v rámci prvotného predspracovania vypočítajú základné charakteristiky.

Ďalej tento proces pokračuje na strane servera, na ktorého strane dôjde k dodatočnému predspracovaniu dát a určeniu ďalších charakteristík, ktoré sú výpočtovo náročnejšie (aby mohla autentifikácia bežať aj na slabších zariadeniach a zároveň bolo optimalizované využitie dostupných zdrojov servera).

Pre dané vstupy sa následne natrénujú 2 modely používateľa (tieto modely budú použité v procese informačnej fúzie na úrovni porovnávacieho skóre):

- vzorovo-nezávislý (PI) model (ako množina charakteristík pri trénovaní sa použije množina vzorovo nezávislých charakteristík získaná v procese *P2 Získanie vzorovo nezávislých čŕt pre budovanie vzorovo nezávislého modelu používateľa*);
- vzorovo-závislý (PD) model (pre natrénovanie modelu sa určí množina charakteristík, ktoré sú vzorovo závislé - pomocou procesu *P3 Získanie vzorovo závislých čŕt pre budovanie vzorovo závislého modelu používateľa*).

Oba modely sa uchovajú v systéme a budú použité pri následnom pokuse o prihlásenie používateľa do zariadenia pri identifikovaní kontextu, pre ktorý boli vytvorené.

P5 Autentifikácia používateľa pri prihlásení. Pre prihlásenie používateľa do systému je po zadaní odomykacieho vzoru overené, či je zadaný odomykací vzor správny. V prípade, že je zadaný vzor správny, na strane klienta sa predvypočítajú základné (výpočtovo nenáročné) charakteristiky a biometrická vzorka sa odošle na server pre autentifikáciu.

Na strane servera dôjde najprv k určeniu kontextu odomykania (pomocou klasifikátora vytvoreného v procese *P1 Trénovanie klasifikátora kontextu odomknutia*). Na základe identifikovaného kontextu odomknutia sa následne vykoná autentifikácia používateľa pomocou vzorovo nezávislého a vzorovo závislého odomykacieho vzoru, ktorej výsledok je spojený v procese informačnej fúzie na úrovni porovnávacieho skóre.

Výsledok autentifikácie sa následne vráti klientovi, ktorý sa rozhodne, ako sa s výsledkom autentifikácie vysporiada.

4.3.2 Uchovávanie biometrických vzoriek

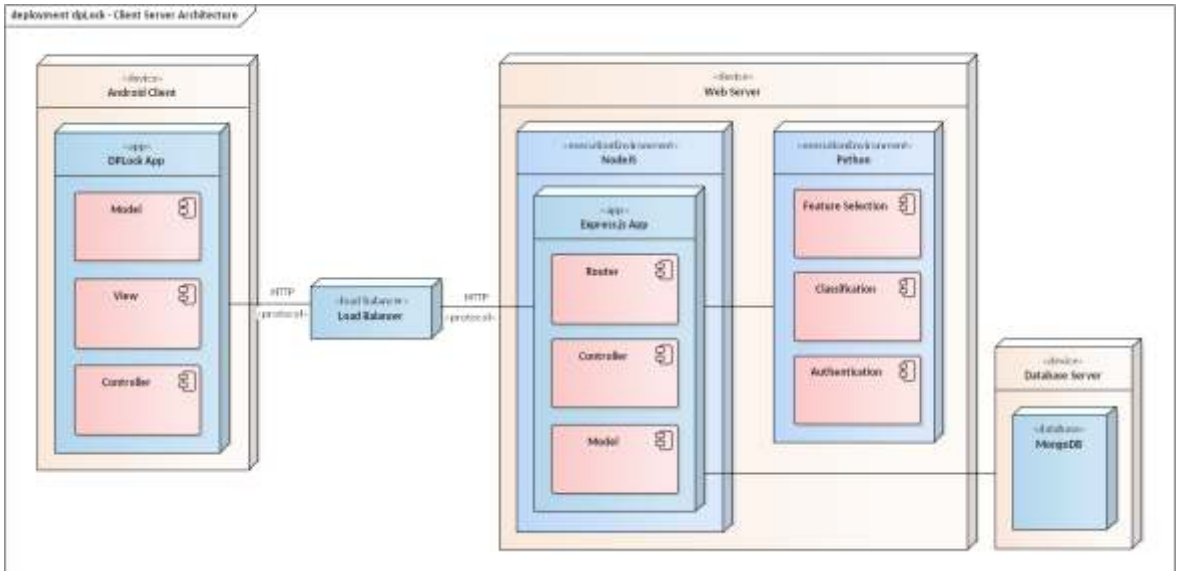
Pre uchovávanie a prenos biometrických vzoriek používateľov sme navrhli štruktúru uchovávania všetkých zaznamenaných dát spolu s predvypočítanými základnými

metrikami, informáciami o používateľovi a kontexte odomykania. Tento dátový model uvádzame v priloženej technickej dokumentácii (Príloha C: Dátový model).

Pre každú vzorku zadania odomykacieho vzoru si tak uchovávame aj priamo udalosti (angl. events) zo špecializovaných senzorov zariadenia (gyroskop, akcelerometer) a dotykovej obrazovky zariadenia, aby v prípade pridania novej charakteristiky do množiny možných používateľských charakteristík mohla byť táto charakteristika dopočítaná. Toto je tiež možné využiť pri zmene algoritmu a prepočte už známych biometrických charakteristík.

4.3.3 Architektúra systému

Pre splnenie požiadavky pre online autentifikáciu používateľov na základe ich biometrických modelov sme sa rozhodli navrhnúť Klient-Server architektúru, ktorá by zabezpečovala pri použití sady niekoľkých funkcií vytvorenie časti tenkého klienta, pomocou ktorej by bola autentifikácia sprostredkovaná (Obr. 6 Rozmiestnenie softvérového systému (diagram rozmiestnenia)).



Obr. 6 Rozmiestnenie softvérového systému (diagram rozmiestnenia)

Klientska časť (Android aplikácia) tak pri autentifikácii môže využívať výpočtový výkon vzdialeného servera prostredníctvom REST API volaní. Pomocou týchto volaní bude možné po získaní referenčných dát od používateľa zašifrovať a odoslať tieto dáta z klientskej časti aplikácie na server pre ďalšie predspracovanie a vytvorenie biometrického modelu používateľa, ktorý sa uloží v centrálnej databáze vytváraného systému pre následné použitie pri autentifikácii.

Následne, pri každom pokuse o prihlásenie sa používateľa do aplikácie sa zachytené

biometrické charakteristiky opäť odošlú na server, kde sa vykoná overenie identity používateľa. Počet webových serverov potrebných pre autentifikáciu bude možné dodatočne škálovať s možnosťou paralelného behu viacerých (odlišných) aplikácií využívajúcich navrhnutý systém na autentifikáciu používateľa.

4.4 Charakteristiky biometrického modelu používateľa

Pri výbere charakteristík, ktoré použijeme pri budovaní používateľských biometrických modelov používateľov, sme vychádzali z referenčnej príručky k Android zariadeniam dostupnej online[3]. Vzhľadom na typ údajov, ktoré nám poskytuje platforma Android, a typy senzorov jednotlivých Android zariadení, pre každú vzorku zadania vzoru uchovávame dáta uvedené v Tab. 5 Zaznamenávané dáta odomykacích udalostí a ich opis.

Tab. 5 Zaznamenávané dáta odomykacích udalostí a ich opis

Typ	**Označenie**		**Opis**
Kontextové dáta o používateľovi, odomykacom vzore a kontexte odomykania	timestamp		*časová známka odomknutia*
	user		*referencia používateľa*
	unlockContext		*kontext odomknutia*
		posture	*poloha človeka (chôdza, stoj, sed)*
		hand	*ruka (ľavá, pravá)*
		finger	*prst (prsty ruky)*
		testId	*ID experimentu (pre zoskupenie odomykacích vzorov zadaných ihneď za sebou)*
	sequelNum		*poradie odomykacieho vzoru v rámci experimentu*
	correctPattern		*správny odomykací vzor*
	enteredPattern		*zadaný odomykací vzor*
	patternSize		*veľkosť správneho odomykacieho vzoru (3x3 = 9, 4x4 = 12)*
Surové dáta zo senzorov	patternEvents		*udalosti zachytené dotykovým displejom (viažu sa na konkrétne body odomykacieho vzoru)*

[3] Dostupné na webe dňa 12. októbra 2017, https://developer.android.com/reference

	touchEvents		*udalosti zachytené dotykovým displejom*
	accelerationEvents		*udalosti zachytené akcelerometrom*
	rotationEvents		*udalosti zachytené gyroskopom*
Dopočítané metriky na zariadení	metrics		*dopočítané základné metriky*
		touchTime	*doba odomykania (prvý až posledný dotyk so zariadením)*
		touch	*metriky k udalostiam dotyku*
		acceleration	*metriky k udalostiam akcelerácie*
		rotation	*metriky k udalostiam rotácie*

Na základe dát uvedených v Tab. 5 Zaznamenávané dáta odomykacích udalostí a ich opis sú pre jednotlivých používateľov dopočítavané ďalšie charakteristiky, ktoré sú použité v procese budovania používateľského modelu. Medzi tieto charakteristiky sme zaradili:

- aktuálna rýchlosť pohybu na dotykovom displeji pre každú zachytenú udalosť;
- priemerná, minimálna a maximálna rýchlosť kreslenia vzoru;
- priemerná, minimálna a maximálna rýchlosť medzi bodmi vzoru;
- doba zadávania odomykacieho vzoru (od prvého po posledný dotyk);
- dĺžka krivky zadaného vzoru;
- charakteristika kriviek pri kreslení vzoru (ostré vs. oblé zákruty, vyjadrené cez minimálny polomer krivky);
- charakteristiky pre naklonenie zariadenia pre každú zachytenú udalosť (min, max, priemer);
- charakteristiky naklonenia zariadenia v závislosti od jednotlivých bodov mriežky (na každom bode odomykacieho vzoru iné naklonenie);
- charakteristiky pre zrýchlenie zariadenia pre každú zachytenú udalosť (min, max, priemer);
- zmena zrýchlenia zariadenia medzi jednotlivými bodmi mriežky (polohovanie zariadenia pri posune prsta/ruky);
- veľkosť dotyku (u niektorých zariadení, závisí od HW podpory zariadenia);
- tlak dotyku (u niektorých zariadení, závisí od HW podpory zariadenia – aktuálne nepodporované);
- horizontálna a vertikálna charakteristika dotyku (šírka a výška prsta);
- charakteristiky celkového zadávania odomykacieho vzoru určené na základe dát

z gyroskopu a akcelerometra zariadenia (získané spektrálnou analýzou dát akcelerácie a rotácie);

- charakteristika prvotného dotyku so zariadením určená na základe dát z gyroskopu a akcelerometra zariadenia (získaná spektrálnou analýzou dát akcelerácie a rotácie, viac v časti 4.5 Charakteristika prvotného dotyku so zariadením).

Podrobný zoznam uvádzaných charakteristík spolu s ich opisom sa nachádza v Tab. 10 Dorátané biometrické charakteristiky a ich opis v Príloha E: Dorátané biometrické charakteristiky. Charakteristiky s označením 68-91 sú využívané ako charakteristiky prvotného dotyku používateľa so zariadením. Spôsob získania týchto charakteristík opisujeme bližšie v časti 4.5 Charakteristika prvotného dotyku so zariadením.

Nie všetky charakteristiky však musia byť významné pri overovaní identity používateľa, a tak pri návrhu metódy pre výber dominantných charakteristík, ktoré sú najvýznamnejšie a najviac ovplyvňujú presnosť biometrického systému, využijeme algoritmy na výber vhodných charakteristík uvádzané v časti 2.2 Biometrický model používateľa.

Biometrický model používateľa však musí okrem biometrických charakteristík používateľa obsahovať aj informácie o používateľovi, na základe ktorých ho bude možné jednoznačne identifikovať. Medzi tieto identifikačné údaje sme sa rozhodli zaradiť základné údaje o používateľovi uvedené v Tab. 6 Identifikačné údaje požívateľov (viac o dátových entitách využívaných v navrhovanom biometrickom systéme v prílohe Príloha C: Dátový model).

Tab. 6 Identifikačné údaje požívateľov

Označenie	**Opis**
name	*meno a priezvisko používateľa (alebo alias)*
email	*prihlasovací email (potrebné na komunikáciu so vzdialeným serverom, na ktorom budú uchovávané jeho biometrické modely)*
gender	*pohlavie*
dominantHand	*dominantná ruka*
password	*prihlasovacie heslo*
dateOfBirth	*dátum narodenia*
registerDate	*dátum registrácie*

Charakteristiky uvádzané v tejto časti práce predstavujú aktuálne množinu charakteristík, ktoré sa nám podarilo získať analýzou dostupných dát, a ktoré dokážeme sledovať pomocou dotykovej obrazovky a polohových senzorov zariadenia. Tieto charakteristiky je však možné do budúcna rozširovať, aby množina charakteristík pre proces výberu vhodných charakteristík bola čo najväčšia.

Celkovo sa nám podarilo navrhnúť 91 skupín rôznych charakteristík, pričom pre niektoré skupiny sa daná skupina môže ďalej rozširovať podľa druhu danej skupiny (dáta z dotykovej obrazovky je napr. možné rozdeliť podľa smeru osi na x-ové a y-ové dáta). Tieto skupiny sa však môžu ďalej rozširovať aj na základe vybraného odomykacieho vzoru, nakoľko niektoré skupiny charakteristík sú určené na základe dvojíc alebo trojíc jednotlivých odomykacích bodov.

Na základe druhu vybranej skupiny pri členenení podľa závislosti od vybraného odomykacieho vzoru teda môžeme všetky biometrické charakteristiky rozdeliť do 2 skupín:

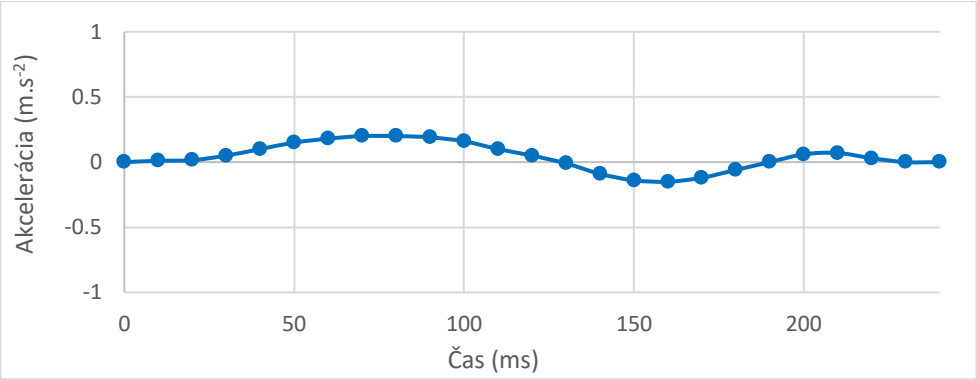
- **vzorovo-nezávislé charakteristiky** (angl. skr. PI): tieto charakteristiky sú spoločné pre všetky odomykacie vzory a je možné ich využiť aj pri medzivzorovej autentifikácii;
- **vzorovo-závislé charakteristiky** (angl. skr. PD): tieto charakteristiky sa viažu na konkrétny odomykací vzor (medzi týmito charakteristikami však môžu existovať aj charakteristiky, ktoré je možné zdieľať medzi rozličnými vzormi).

4.5 Charakteristika prvotného dotyku so zariadením

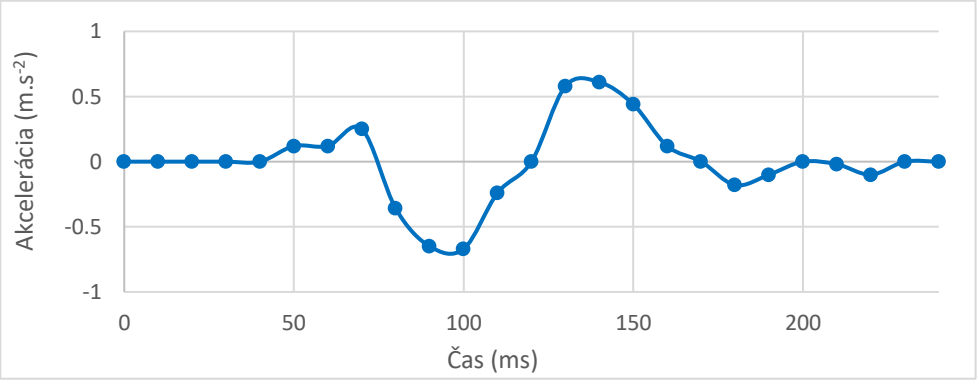
V rámci budovania biometrického modelu používateľa sme navrhli vytvorenie takých skupín používateľských charakteristík, ktoré popisujú prvotný kontakt používateľa so zariadením (dotykovou obrazovkou zariadenia pri zadávaní odomykacieho vzoru). Predpokladáme, že s využitím dát z akcelerometra a gyroskopu dokážeme vytvoriť model prvotného dotyku používateľa so zariadením, ktorý by mal byť pre každého používateľa jedinečný, a v procese fúzie tak dokáže finálnu úspešnosť nami navrhnutého biometrického systému zvýšiť.

Ako príklad uvádzame závislosť akcelerácie zariadenia od času kontaktu so zariadením (Obr. 7 Príklad spôsobu slabého ťuknutia na dotykovú obrazovku zariadenia, Obr. 8 Príklad spôsobu silného ťuknutia na dotykovú obrazovku zariadenia), na ktorom je možné vidieť rozdielnosť vlastnosti dotyku s obrazovkou zariadenia pri slabom (na obrázku vľavo) a silnom (na obrázku vpravo) ťuknutí na displej zariadenia. Tieto dva dotyky sa líšia

napríklad v maximálnych a minimálnych hodnotách zrýchlenia alebo vo frekvencii samotnej krivky akcelerácie (v prípade porovnania s kmitavým pohybom). Tieto charakteristiky by mali odzrkadľovať nielen spôsob práce používateľa so zariadením ale aj spôsob správania sa používateľa k zariadeniu (tvrdé vs. jemné dotyky, tuhá ruka a podobne).



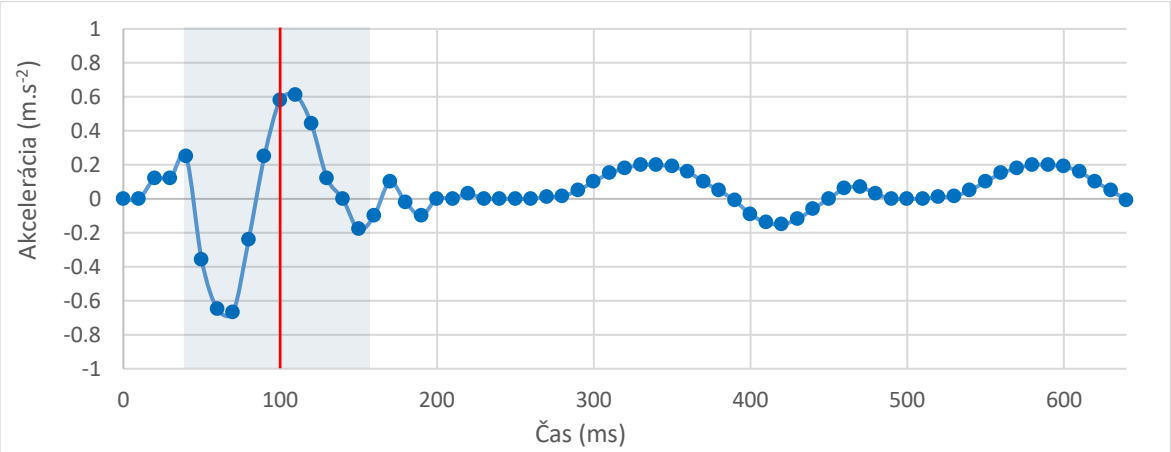
Obr. 7 Príklad spôsobu slabého ťuknutia na dotykovú obrazovku zariadenia



Obr. 8 Príklad spôsobu silného ťuknutia na dotykovú obrazovku zariadenia

Podobné charakteristiky je možné vytvoriť aj za pomoci dát z gyroskopu (naklonenie zariadenia).

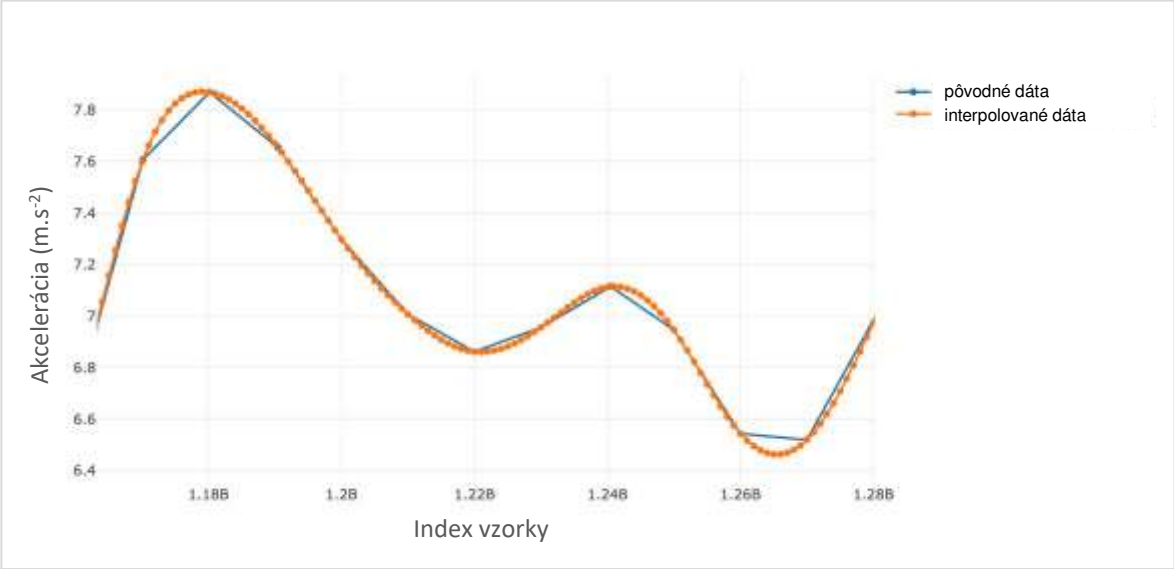
Dôležitým krokom v procese vytvárania modelov prvotných dotykov používateľov je však samotná identifikácia a určenie hraníc, ktoré vymedzujú prvotný dotyk so zariadením (vyznačené tmavšou plochou na Obr. 9 Snímanie akcelerácie zariadenia pri odomykaní zariadenia), nakoľko zadávanie odomykacieho vzoru môže prebiehať ľubovoľne dlhý moment. Pre výber tých dát z akcelerometra a gyroskopu sme sa preto rozhodli zohľadniť dotykové udalosti (angl. touch events) odomknutia tak, že budeme zohľadňovať udalosti (rotácie a akcelerácie) v okolí ±0,25 s od prvého dotyku používateľa so zariadením.



Obr. 9 Snímanie akcelerácie zariadenia pri odomykaní zariadenia

Pri získaní charakteristík z prvotného dotyku so zariadením sme vychádzali z práce [WILK16], ktorej cieľom bolo vyvinutie metódy na zistenie neurologických chorôb založenej na analýze výstupných signálov z akcelerometra umiestneného na ukazováku pravej ruky. V tejto práci analyzovali trasenie rúk používateľov pomocou spektrálnej analýzy týchto dát.

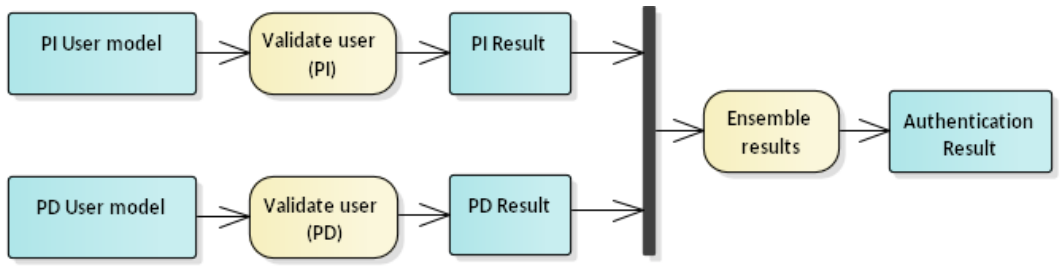
Pre vykonanie spektrálnej analýzy je však potrebné vykonať interpoláciu dát z akcelerometra a gyroskopu, nakoľko pre spektrálnu analýzu je potrebná konštantná vzorkovacia frekvencia naprieč celými dátami.



4.6 Informačná fúzia

Proces autentifikácie sme sa rozhodli za účelom zvýšenia úspešnosti výsledku navrhnutého biometrického systému obohatiť o informačnú fúziu na úrovni porovnávacieho skóre (spomínané v časti 2.4.1 Fúzna biometria).

Fúzia na úrovni porovnávacieho skóre. V rámci fúzie na úrovni porovnávacieho skóre plánujeme kombinovať výsledky klasifikácií pre jednotlivé typy zachytávaných biometrických charakteristík (vzorovo závislé charakteristiky (PI User model) a nezávislé charakteristiky (PD User model)). Na základe vykonaných klasifikácií pre každý typ sledovaných charakteristiky natrénujeme znovu klasifikátor, ktorý skombinuje výsledky predchádzajúcich klasifikátorov (vzorovo závislého a nezávislého). Tento prístup poznáme tiež pod pojmom súhra (angl. ensemble).



Obr. 10 Spojenie výsledkov klasifikátorov pre vzorovo závislé a nezávislé charakteristiky (informačná fúzia na úrovni porovnávacieho skóre)

Nakoľko pri trénovaní klasifikátora pre autentifikáciu používateľa budeme využívať „One-Class“ klasifikátor, aj spájajúci klasifikátor musí byť tohto typu, aby bolo možné finálny model používateľa pozostávajúci z týchto 3 klasifikátorov natrénovať výlučne pomocou dát od používateľa (bez potreby útočníckych dát).

5 Implementácia

Nakoľko si povaha tejto diplomovej práce vyžaduje implementáciu navrhovaného riešenia biometrického systému na autentifikáciu používateľov pod smartfónovou platformou, v tejto časti uvádzame implementačné detaily nami navrhnutého riešenia.

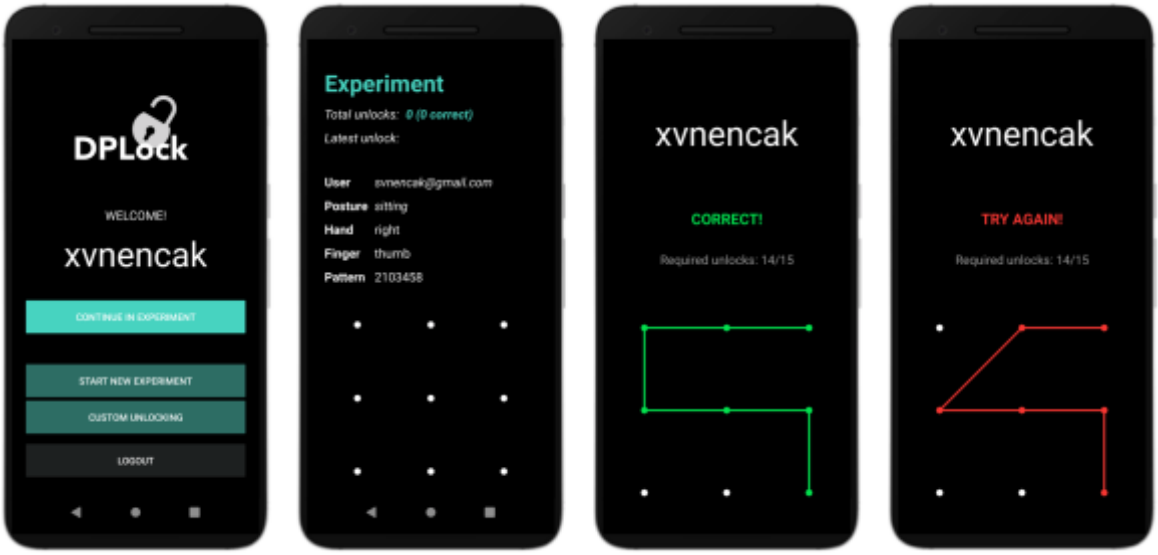
5.1 Použité technológie a vývojové prostredie

Na implementáciu navrhovaného systému bolo potrebné vytvorenie klientskej a serverovej časti aplikácie.

5.2 Klientska Android aplikácia

Klientska Android aplikácia slúži na zaznamenávanie biometrických vzoriek používateľov. Aktuálna verzia aplikácie bola navrhnutá tak, aby bolo pomocou nej možné zbierať dáta potrebné pri vykonávaní experimentov pre určenie optimálneho procesu autentifikácie používateľov.

Mobilnú aplikáciu sme sa primárne rozhodli implementovať v jazyku Kotlin, ktorý podporuje vzájomnú kompatibilitu s jazykom Java. Hlavnými výhodami tohto jazyka je podpora lambda výrazov, jednoduché ošetrovanie nulových výnimiek (angl. Null Exceptions), podpora dátových tried a mnoho ďalšieho, čo uľahčuje a zefektívňuje písanie Android aplikácií. Tento jazyk je možné používať vo viacerých vývojových nástrojoch, my sme sa rozhodli pre Android Studio, ktoré je zaužívaným prostredím pri vývoji Android aplikácií.



Obr. 11 Hlavná obrazovka Android klienta dpLock (zľava), zobrazenie experimentu a obrazovka zadávania vzoru používateľom (správny a nesprávny vzor)

Odomykací vzor. Pre zadávanie odomykacieho vzoru sme použili knižnicu PatternLockView[4] voľne stiahnuteľnú z verejného git repozitára. Táto knižnica sa nachádza aj v jCenter repozitári, čo je základný Maven repozitár bežne používaný programom Android Studio.

Ako príklad zaznamenaných dát uvádzame grafové dáta pre dotyk, akceleráciu a naklonenie zariadenia v prílohe Príloha A: Príklad zaznamenanej biometrickej vzorky (časové známky pre zachytené udalosti sú pre všetky tri typy udalostí v nanosekundách od začiatku zaznamenávania odomknutia).

5.3 Serverová časť biometrického systému

Serverovú časť biometrického systému sme sa rozhodli vyvíjať v jazyku JavaScript spoločne s aplikačným rámcom NodeJS, ktorý je vhodný na budovanie serverových častí aplikácií s podporou sieťových funkcií. Na ukladanie biometrických vzoriek a modelov používateľov sme sa rozhodli využiť nerelačnú databázu MongoDB (spolu s aplikačným rámcom Mongoose), ktorá dokáže spoločne s NodeJS serverom bežať na zdieľanom Unix serveri (pre nerelačnú databázu MongoDB sme sa rozhodli z dôvodu dobrej podpory vysokého množstva ukladaných dát a jednoduchej podpory shardovania databáz pre rýchlejší prístup k dátam).

[4] Dostupné na webe dňa 7. decembra 2017, https://github.com/aritraroy/PatternLockView

Autentifikácia používateľov. Samotný výber biometrických charakteristík, trénovanie používateľských modelov a autentifikáciu používateľov (tak ako uvádzame v časti 4.3Návrh riešenia autentifikácie používateľa) prebieha v prostredí jazyka Python. Pre tieto účely sme vytvorili sadu Python modulov, ktoré je možné používať v jednotlivých krokoch navrhnutých procesov (obsah digitálnej časti práce).

Na prvotné experimenty a predspracovanie biometrických údajov pre účely vhodnosti navrhnutých procesov sme využili možnosti jazyka Python a dostupných knižníc v prostredí PyCharm a Jupyter Notebook (jednotlivé skripty použité pri simulácii procesov autentifikácie sú súčasťou digitálnej časti práce).

5.4 Zhrnutie aktuálneho stavu implementácie

Nami implementovaný systém na autentifikáciu používateľov prostredníctvom ich biometrických charakteristík pozostáva z dvoch častí tak, ako sme ho špecifikovali v návrhu nášho riešenia. V rámci klientskej (mobilnej časti) aplikácie sú získavané biometrické dáta od používateľov, ktorých ukážku je možné vidieť v prílohe Príloha A: Príklad zaznamenanej biometrickej vzorky. Tieto biometrické vzorky sú posielané na vzdialený server prostredníctvom REST API volaní. Biometrické dáta môže do systému zadávať (prostredníctvom zadávania odomykacieho vzoru) iba zaregistrovaný používateľ, aby každá biometrická vzorka mala jednoznačne určeného vlastníka.

Na serverovej strane aplikácie dochádza k ukladaniu biometrických vzoriek používateľov do centrálnej databázy v MongoDB. Kompletný popis API, ktoré je možné vykonávať nad spusteným serverom je uvedený v prílohe Príloha D: Rozpis serverových API. Pomocou tohto servera je možné pristupovať k získaným používateľským dátam, no prístup k dátam je možné tiež vykonať priamo pomocou databázového MongoDB klienta (napr. MongoDB Compass).

Súčasťou serverovej časti implementácie sú aj nami vytvorené Python moduly, ktoré sú využívané v procesoch autentifikácie používateľov (predspracovanie dát, odstránenie chybových záznamov (angl. outlierov), prvotný výber najdôležitejších charakteristík a klasifikáciu).

Aktuálny stav implementácie umožňuje efektívne zbieranie biometrických dát o používateľoch, ktoré je možné využiť pri experimentovaní a budovaní biometrického systému.

6 Overenie riešenia

6.1 Experimenty

V tejto časti sa nachádza opis experimentov spolu so zhodnotením výsledkov získaných pri autentifikácii používateľov. Sú to porovnané výsledky jednotlivých algoritmov určených na vyhľadávanie anomálií v dátach (angl. outliers), výber vhodných charakteristík pre budovanie modelov a klasifikáciu používateľov. Taktiež sa tu nachádza opis experimentov zameraných na overenie hypotéz uvedených v časti 3.1 Výskumné hypotézy tejto práce.

6.2 Opis experimentov

Pre získanie biometrických údajov sme uskutočnili 2 sady experimentov, v rámci ktorých sme získali dáta od 52 rôznych používateľov. V rámci experimentov sme sa zamerali na získanie dát pre 4 rôzne odomykacie vzory a 2 rôzne spôsoby odomykania (podrobný opis priebehu experimentov sa nachádza v Príloha E: Experiment 1 a Príloha F: Experiment 2).

Prvý z experimentov (ďalej len EXP1) bol uskutočnený v riadenom prostredí, pričom cieľom tohto experimentu bolo získanie dát pre overenie možnosti zisťovania kontextu odomykania. Účastníci experimentu (28 účastníkov) mali za úlohu odomykať mobilné zariadenia pomocou 2 rôznych vzorov a pre 2 rôzne kontexty.

Druhý experiment (ďalej len EXP2) sme vykonali v širšom časovom intervale a v neriadenom prostredí, aby sme od používateľov získali dáta, aké by sme mohli očakávať v reálnom prostredí. V tomto experimente sa zapojilo 33 používateľov a celkový počet biometrických vzoriek presahoval hodnotu 12 000 (približne 380 vzoriek od každého používateľa).

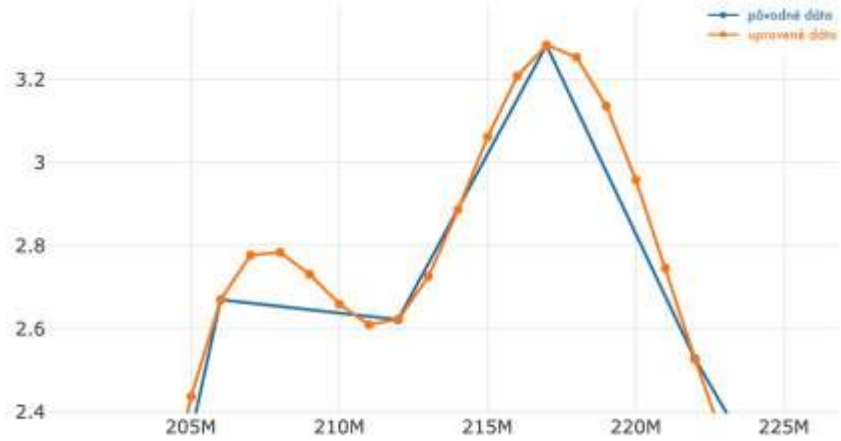
6.3 Predspracovanie dát

Dáta získané v počas experimentu (so základnými biometrickými charakteristikami) sme ďalším predspracovaním rozšírili o charakteristiky opísané v časti 4.4 Charakteristiky biometrického modelu používateľa (podrobné charakteristiky nájdete uvedené v Tab. 10 Dorátané biometrické charakteristiky a ich opis).

Spektrálna analýza dát z akcelerometra a gyroskopu. Pre určenie špecifických množín charakteristík prvotného dotyku so zariadením pri odomykaní sme implementovali algoritmus určujúci skupinu charakteristík s označením 68-91 v Tab. 10 Dorátané

biometrické charakteristiky a ich opis v Príloha E: Dorátané biometrické charakteristiky na základe spektrálnej analýzy dát z gyroskopu a akcelerometra.

Pre vykonanie spektrálnej analýzy týchto dát bolo potrebné tieto dáta interpolovať, aby sme získali konštantnú vzorkovaciu frekvenciu (interpoláciu dát sme vykonali kubickou interpoláciou). Príklad výsledku pozmenených dát akcelerometra uvádzame na Obr. 12 Interpolácia dát z akcelerometra (konštantná vzorkovacia frekvencia).



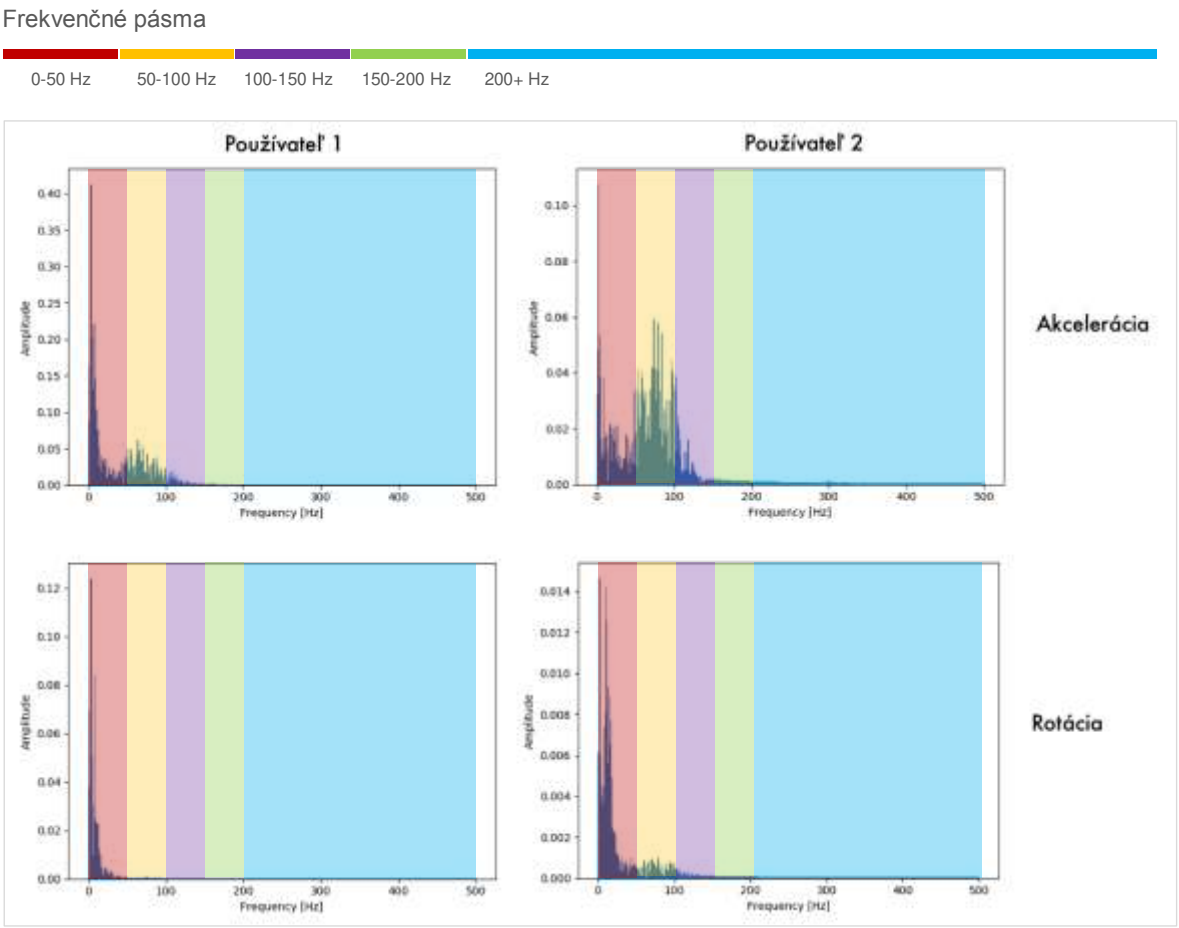
Obr. 12 Interpolácia dát z akcelerometra (konštantná vzorkovacia frekvencia)

Po upravení dát tak, aby sme nad nimi mohli vykonať rýchlu Fourierovu transformáciu (angl. skr. FFT) pre spektrálnu analýzu sme z výsledku spektrálnej analýzy odvodili viaceré charakteristiky, ktoré využijeme pri budovaní biometrického modelu používateľa.

Aj na základe náhodného porovnania dát 2 rôznych používateľov môžeme usúdiť, že spektrá dát z akcelerometra a gyroskopu sa pre jednotlivé udalosti odomykania značne odlišujú (Obr. 13 Výsledok spektrálnej analýzy pre 2 používateľov pre rôzne frekvenčné pásma). Samotný výsledok spektrálnej analýzy však nie je možné použiť pri klasifikácii používateľa, nakoľko predstavuje výkonnostné rozdelenie jednotlivých frekvencií v dátach. Aby bolo možné frekvenčné spektrá porovnať medzi jednotlivými používateľmi, bolo potrebné tieto spektrá ďalej spracovať. Výsledné charakteristiky sa nachádzajú v Tab. 10 Dorátané biometrické charakteristiky a ich opis na pozícii 44-91 (spektrálna analýza dát z akcelerometra a gyroskopu pre celkové dáta a dáta z prvotného dotyku so zariadením pri zadávaní vzoru).

Špecifickými charakteristikami získanými z frekvenčných spektier (mimo maximálnych a priemerných výkonov frekvencií celého spektra) sú charakteristiky získané rozdelením frekvenčného spektra do frekvenčných pásem (angl. frequency bands), čím sme oddelili jednotlivé frekvencie na veľmi vysoké (200+ Hz), vysoké (150-200 Hz), stredné

(100-150 Hz), nízke (50-100Hz) a veľmi nízke (0-50Hz). Z pozorovaní nad získanými dátami usudzujeme, že používatelia trpia pri odomykaní zariadenia rôznou intenzitou špecifických frekvencií (slabé a intenzívne trasenie alebo silné a tlmené trasenie ruky). Pre takto vzniknuté spektrálne pásma sme následne určili (rovnako ako pre celé frekvenčné spektrum) celkový, maximálny a priemerný výkon príslušných frekvencií.



Obr. 13 Výsledok spektrálnej analýzy pre 2 používateľov pre rôzne frekvenčné pásma

6.4 Vyhľadávanie outlierov

Pre odstránenie nekonzistencií v dátach sme sa rozhodli vykonať vyhľadanie a následné odstránenie outlierov zo získaných dát.

EXP1. Nakoľko na naučenie plynulého zadávania odomykacieho vzoru nemal používateľ žiadne pokusy, rozhodli sme sa zo všetkých dát odstrániť prvé 3 pokusy pre každú sekvenciu zadávania odomykacieho vzoru.

EXP2. Pre tento experiment sme sa taktiež rozhodli odstrániť z dát prvých 5 odomknutí pre každú sériu odomykaní (zadanie vzoru pri prvých pokusoch malo vysokú mieru chybovosti – nenaučený vzor).

Pri vyhľadávaní outlierov vo zvyšných dátach sme následne postupne pre každého používateľa rozdelili biometrické dáta do skupín podľa zadaných odomykacích vzorov a kontextu pri odomykaní. Pre každú z týchto skupín sme vykonali vyhľadanie outlierov na základe určenia medzikvartilovej rozptýlky (angl. skr. IQR, známa tiež ako H-Spread) a z-skóre (angl. z-score) danej skupiny na základe skupiny základných charakteristík, čím sme z dát odstránili anomálie (vyhľadanie anomálií v rámci sekvencie zadávaných vzorov).

Aby bol pre každého používateľa výsledný počet biometrických vzoriek podobný, vykonali sme SMOTETomek vyváženie jednotlivých tried používateľov[5], ktoré kombinuje „upsampling“ minoritných a „downsampling“ majoritných tried (vytváraním syntetických vzoriek namiesto ich duplikácie hľadaním najbližších vzoriek použitím KNN algoritmu), nakoľko pre nevyvážené triedy by mohlo dôjsť k nesprávnemu trénovaniu a výberu vhodných množín charakteristík (väčšina algoritmov strojového učenia pracuje najlepšie pre vyvážené triedy z dôvodu maximalizácie presnosti (angl. accuracy) a minimalizácie chyby (angl. error)).

6.5 Výber biometrických charakteristík

Nakoľko je množina charakteristík tvoriaca biometrický model používateľa pomerne veľká, vykonali sme sadu experimentov, v rámci ktorých sme vyhľadávali tie charakteristiky, ktoré majú najvyšší vplyv na úspešnosť klasifikácie. Predpokladáme, že odstránením málo signifikantných charakteristík dokážeme zvýšiť nielen presnosť ale aj rýchlosť vytváraného biometrického systému.

Nami navrhnutý proces autentifikácie používateľov sa skladá z dvoch častí, a to z identifikácie spôsobu odomknutia (poloha, ruka a prst) a z verifikácie získanej biometrickej vzorky voči špecifickému modelu používateľa (získaného v procese identifikácie)(opísané v časti 4.3 Návrh riešenia autentifikácie používateľa).

V rámci vyhľadávania optimálneho počtu charakteristík sme pre oba problémy najprv vykonali vyhľadanie korelovaných charakteristík pomocou 2 rôznych prístupov:

- určením matice korelácie a vymazaním charakteristík s koreláciou vyššou ako stanovený prah (±0.8);
- určovaním hodnoty VIF (angl. skr. Variance Inflation Factor) pre postupne sa zmenšujúce podmnožiny charakteristík (vymazanie charakteristík, ktorých prah korelácie je vyšší ako maximálna povolená hodnota).

[5] https://imbalanced-learn.readthedocs.io/en/stable/combine.html

Výhodou vyhľadávania korelovaných charakteristík pomocou VIF metódy oproti vyhľadávaniu pomocou korelačnej matice je to, že VIF metóda nepredpokladá koreláciu medzi dvojicami jednotlivých charakteristík, ale vyhľadáva korelované charakteristiky pre rôzne podmnožiny charakteristík. Týmto spôsobom tak dokážeme vyhľadať aj multikorelácie medzi jednotlivými charakteristikami.

Nakoľko predpokladáme, že veľkosť množiny sledovaných charakteristík môže mať nepriamy vplyv na úspešnosť biometrického systému (3.1 Výskumné hypotézy), v procese výberu vhodných charakteristík sme vykonali minimalizácie počtov sledovaných charakteristík pre oba experimenty.

Minimalizácia množiny charakteristík. V procese výberu vhodných charakteristík sme sa preto zamerali na nájdenie tých charakteristík, ktoré majú najväčší vplyv na určenie spôsobu odomknutia (v našom prípade prsta) a na klasifikáciu používateľov podľa získaných biometrických dát.

Pre nájdenie signifikantných charakteristík pre rozlíšenie prsta a rovnako aj samotného používateľa sme zvlášť pre každý kontext a každého používateľa určili dôležitosť jednotlivých charakteristík pri klasifikácii pomocou algoritmov *k-best* a *extra-tree*. Pomocou získaného ohodnotenia sme následne minimalizovali množinu charakteristík tak, že sme postupne vykonali trénovanie klasifikátorov postupne pre rôzne podmnožiny (vznikali odoberaním najmenej relevantných charakteristík spätnou elimináciou), a určovali presnosť danej podmnožiny pri klasifikácii. Podmnožinu charakteristík, ktorá dosahovala najvyššiu úspešnosť sme považovali za najlepšiu minimálnu množinu charakteristík, ktorú je možné použiť pri klasifikácii kontextu zadávania vzoru používateľom.

Výsledné podmnožiny najrelevantnejších charakteristík pre jednotlivé použité algoritmy sa nachádzajú v digitálnej časti práce (dokumentácia k Jupyter Notebook).

6.6 Klasifikácia

6.6.1 Detekcia spôsobu odomknutia

Pri klasifikáciu kontextu zadania vzoru (prsta) sme použili podmnožiny charakteristík, ktoré sme získali v procese výberu relevantných charakteristík v predchádzajúcom kroku.

Klasifikáciu kontextu odomknutia sme vykonali pomocou viacerých klasifikátorov, a to *Gaussovho Naive Bayes klasifikátora, klasifikátora rozhodovacích stromov (angl. Decision Tree Classifier),* a *lineárnou diskriminačnou analýzou.*

Najvyššiu úspešnosť klasifikácie mali klasifikátory využívajúce množinu signifikantných charakteristík určených algoritmom *k-best* a *extra-tree,* pričom presnosť (angl. accuracy) klasifikácie prsta dosahovala priemernú hodnotu 88%.

6.6.2 Autentifikácia používateľov

Pre zhodnotenie úspešnosti autentifikácie používateľov bolo potrebné vykonať natrénovanie „Single-Class“ klasifikátora. Na tento účel sme natrénovali špeciálny SVM (angl. Support Vector Machine) klasifikátor, ktorý dokáže určiť relatívnu pozíciu zaradenia novej vzorky do „normálnej“ (al. angl. inline) skupiny vzoriek.

Natrénovanie klasifikátora sme uskutočnili krížovou validáciou pre každého používateľa zvlášť, pričom časť používateľských dát bola použitá na trénovanie a iná časť na testovanie. Okrem používateľských dát boli do testovania modelu každého používateľa zaradené aj vzorky iných používateľov, čím sme simulovali pokusy o autentifikáciu neautorizovaného používateľa.

EXP1. Pri vyhodnotení dát z experimentu EXP1, pre ktorý sme mali k dispozícii aj dáta s rôznym kontextom zadávania vzoru, sme pri autentifikácii zohľadnili aj spôsob zadanie odomykacieho vzoru (kontextu odomykania) a vykonali sme experimenty so známym spôsobom odomknutia (identifikácia prsta) aj bez neho.

Výsledky autentifikácie používateľov ukazujú mierne zlepšenie úspešnosti biometrického systému v prípade, že k verifikácii modelu dôjde až na základe identifikácie špecifického modelu (prsta) používateľa. Najvyššiu úspešnosť však všeobecne vykazoval klasifikátor SVM s typom jadra *sigmoid* a *poly* (obe rovnako), a použitými signifikantnými charakteristikami určenými v procese výberu charakteristík algoritmom *k*-best.

V prípade komplikovanejšieho odomykacieho vzoru a úspešnej detekcii prsta pri určení referenčného modelu používateľa tento klasifikátor pracoval s presnosťou *EER 0.19458* pri odstránení outlierov pomocou metódy z-skóre.

V prípade jednoduchšieho odomykacieho vzoru a úspešnej detekcii prsta pri určení referenčného modelu používateľa tento klasifikátor pracoval s presnosťou *EER 0.14673* pri odstránení outlierov pomocou metódy IQR.

Podrobné výsledky klasifikácie pre jednotlivé experimenty a použité algoritmy uvádzame v prílohe Príloha L: Výsledky autentifikácie a v digitálnej časti práce (rozdelené podľa Príloha K: Scenáre pri klasifikácii používateľov – EXP1).

EXP2. Pre vyhodnotenie úspešnosti biometrického systému nad dátami získanými v dlhodobom experimente EXP2, kde sme mali podstatne vyšší počet referenčných vzoriek zadávania vzoru pre každého používateľa, sme taktiež vykonali krížovú validáciu pre určenie úspešnosti rôznych prístupov k predspracovaniu, vyhľadaniu signifikantných charakteristík a klasifikácii používateľov pomocou klasifikátora SVM s typmi jadra *sigmoid* a *poly*.

Najvyššiu úspešnosť klasifikácie dosahovali metódy, u ktorých bolo použité klasifikačné jadro typu *sigmoid* a bolo prevedené odstránenie korelovaných dát na základe matice korelácie a vymazaní charakteristík s koreláciou vyššou ako stanovený prah 0.8 (angl. threshold).

V prípade porovnania úspešnosti klasifikácie pomocou minimalizovaných a neminimalizovaných množín charakteristík oba prístupy dosahovali porovnateľné výsledky. Avšak na základe princípu Occamovej žiletky (angl. Occam's razor principle), ktorý preferuje u modelov s podobnou úspešnosťou vybrať model s nižším počtom charakteristík, pokladáme navrhnutú metódu minimalizácie počtu sledovaných charakteristík za výhodnú (zníženie náročnosti klasifikácie používateľa).

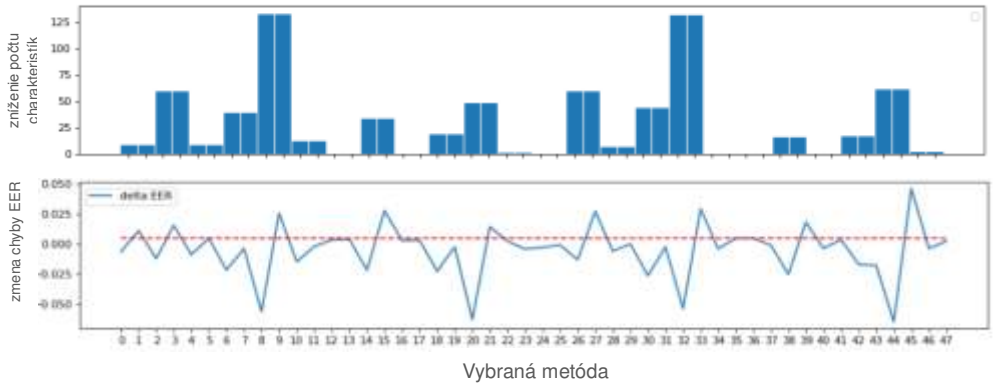
Najnižsia hodnota EER, ktorú sa nám podarilo pre jednotlivé prístupy dosiahnuť, dosahovala hodnotu 0.053240.

6.7 Overenie hypotéz

V rámci skúmania problematiky zabezpečenia mobilných zariadení pomocou biometrickej autentifikácie používateľov sme dospeli k niekoľkých hypotézam uvádzaným v časti 3.1 Výskumné hypotézy.

Hypotéza 1. Overenie platnosti tejto hypotézy sa nám podarilo dosiahnuť v procese minimalizácie množín sledovaných charakteristík. Na základe získanej hodnoty EER pre minimalizované a neminimalizované množiny charakteristík je zrejmé, že čím bola množina sledovaných charakteristík menšia, tým aj priemerná hodnota chyby skúmaných metód bola nižšia (jednotlivé metódy a využité prístupy v daných metódach sú uvedené v Tab. 13 Výsledky autentifikácie používateľa využitím viacerých metód v procese návrhu systému). Zmeny hodnôt chýb EER pri rôznom znížení počtu sledovaných charakteristík pre jednotlivé metódy uvádzame na Obr. 14 Zmena hodnoty EER pre minimalizované množiny charakteristík, kde zníženie počtu sledovaných charakteristík predstavuje počet odobratých charakteristík v procese eliminácie nesignifikantných charakteristík a zmena hodnoty chyby

EER predstavuje zmenu hodnoty chyby EER po odobratí týchto charakteristík z procesu trénovania.



Obr. 14 Zmena hodnoty EER pre minimalizované množiny charakteristík

Z uvedeného grafu je možné vidieť, ako sa vysoký počet odobratých charakteristík pozitívne prejavil aj na výslednej hodnote chyby EER (znížila sa). Toto vylepšenie sa podarilo dosiahnuť určením dôležitosti jednotlivých charakteristík pomocou algoritmu rozhodovacích stromov (angl. Decision Tree Classifier) a následnej eliminácii charakteristík pomocou určovania presnosti klasifikácie týmto klasifikátorov (Tab. 7 Výsledok minimalizácie počtu sledovaných na hodnotu chyby EER). Priemerné zníženie EER pre všetky typy metód dosahuje hodnotu 0.0048, FAR 0.0005 a FRR 0.0023. K zlepšeniu teda došlo pre všetky hodnoty chýb.

Tab. 7 Výsledok minimalizácie počtu sledovaných na hodnotu chyby EER

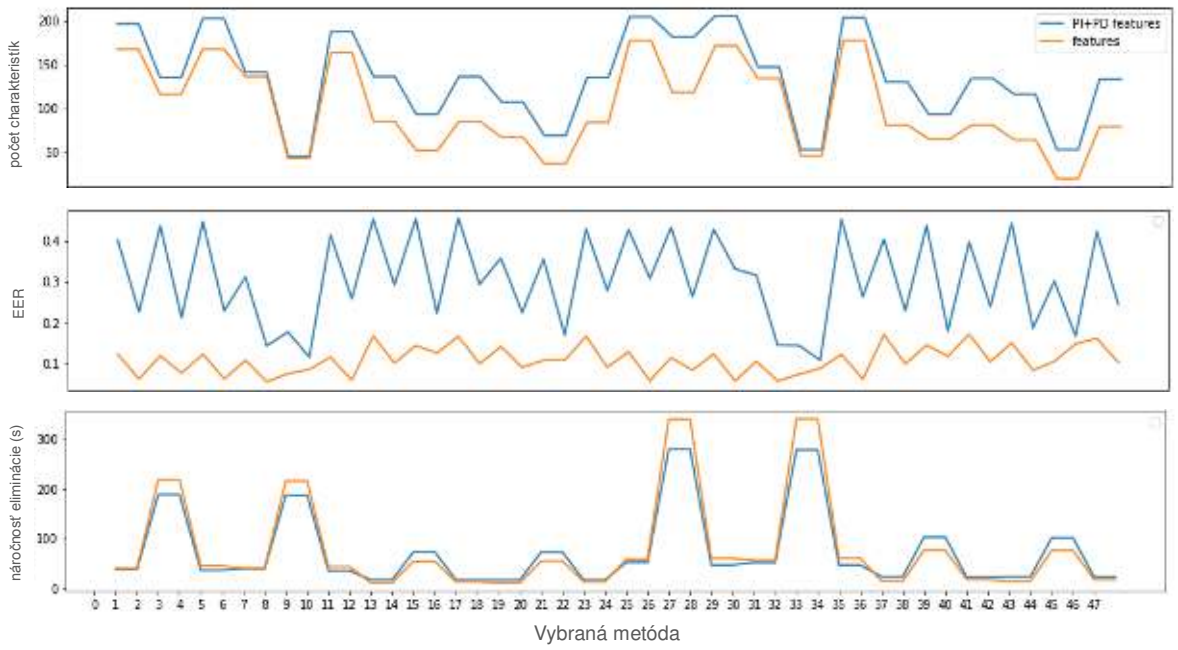
Eliminácia outlierov	Ohodnotenie relevantnosti charakteristík	Minimalizácia počtu charakteristík	Pôvodný počet charakteristík	Minimalizovaný počet charakteristík
IQR	*extra-tree*	*decision-tree*	176	43
			86	37
Z-Skóre			178	46
			82	20

Toto predstavuje výhodu nielen v presnosti navrhnutého biometrického systému, ale aj v efektívnosti samotnej autentifikácie, nakoľko menšia množina sledovaných charakteristík znamená automaticky nižšie nároky na spracovanie každého pokusu o autentifikáciu používateľa spojené s predspracovaním a samotnou klasifikáciou získanej

biometrickej vzorky.

Navrhnutá metóda pre výber signifikantných charakteristík biometrického modelu používateľa bola úspešná a pre menšie množiny charakteristík pracoval navrhnutý biometrický systém s vyššou úspešnosťou (nižšou hodnotou chyby EER). Túto hypotézu teda pokladáme za platnú.

Hypotéza 2. Pre overenie tejto hypotézy sme natrénovali pre každého používateľa 3 klasifikátory podľa navrhnutej metódy informačnej fúzie na úrovni porovnávacieho skóre pre rozdelenie charakteristík na vzorovo závislé a nezávislé (4.6 Informačná fúzia). Pri porovnaní s prístupom, kedy sa charakteristiky v procese výberu dominantných charakteristík nedelili na vzorovo závislé a nezávislé (Obr. 15 Porovnanie parametrov klasifikačných metód pre rozlišovanie a nerozlišovanie vzorovo závislých a nezávislých charakteristík), je počet sledovaných charakteristík pri tomto prístupe vyšší, a teda aj náročnosť autentifikácie je vyššia. Zaujímavé je však pozorovanie, že pri rozdelení charakteristík na vzorovo závislé a nezávislé sa pri následnom výbere najsignifikantnejších charakteristík aj napriek väčšej množine využitých charakteristík pri klasifikácii znížila celková časová náročnosť výberu minimálnej množiny charakteristík použitej pri trénovaní (predpokladáme, že toto je spôsobené menším celkovým počtom kombinácií v rámci menších množín charakteristík ako je celkový počet kombinácií charakteristík vo väčšej množine).

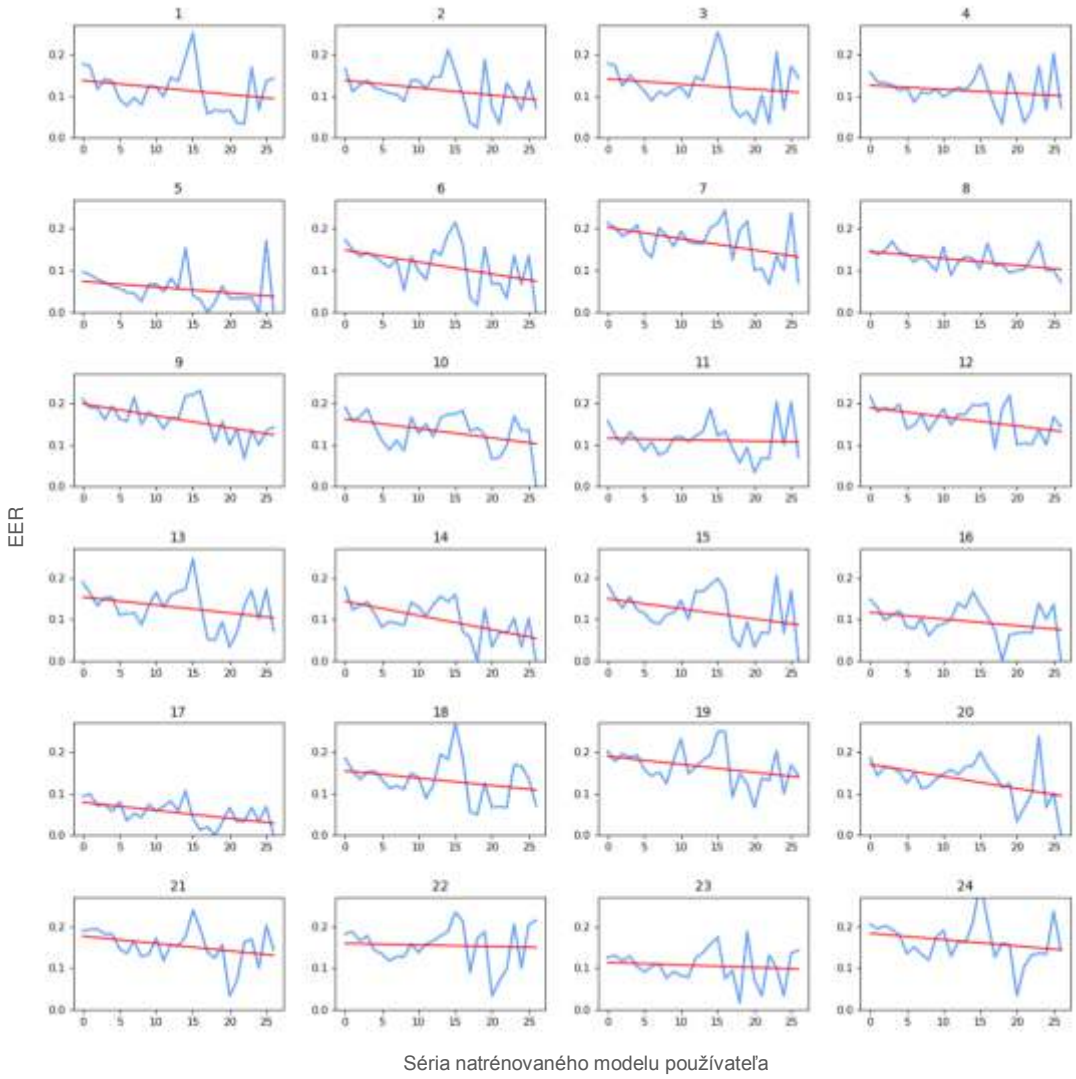


Obr. 15 Porovnanie parametrov klasifikačných metód pre rozlišovanie a nerozlišovanie vzorovo závislých a nezávislých charakteristík

Túto hypotézu však musíme na základe porovnania hodnôt chýb EER pre autentifikáciu používateľa pomocou informačnej fúzie na úrovni porovnávacieho skóre a bez nej zamietnuť. Fúzia na úrovni porovnávacieho skóre v prípade „One Class“ klasifikátora v našom prípade nemá význam pri zvyšovaní celkovej úspešnosti biometrického systému.

Hypotéza 3. Overenie platnosti tejto hypotézy sme vykonali postupným trénovaním biometrického modelu používateľa pomocou dát získaných v EXP2 (dlhodobý experiment). Postupne pre jednotlivé série odomykaní (rozdelené do širšieho časového obdobia) sme pre každého požívateľa postupne natrénovali biometrický model a sledovali sme vývoj úspešnosti systému pomocou hodnoty chyby EER bez dodatočnej úpravy množiny sledovaných charakteristík. Pre určenie hodnoty chyby EER sme vždy pre natrénovaný klasifikátor ako množinu testovacích dát využili najbližšiu sériu odomknutí nasledujúcu po sériách, na ktorých bol klasifikátor natrénovaný.

Pre jednotlivé použité metódy (označenie metódy sa nachádza nad daných grafom vývoja chyby EER, zoznam použitých prístupov pre jednotlivé metódy sa nachádza v Príloha M: Výsledky autentifikácie – EXP2) sme na Obr. 16 Vývoj hodnoty chyby EER pri postupnom trénovaní modelov používateľov znázornili priemernú hodnotu chyby medzi jednotlivými sériami odomykania. Hodnota chyby EER sa takmer u všetkých použitých metód postupne znižovala, pričom toto zlepšenie bolo viditeľné už od samotného začiatku dlhodobého experimentu (prvých sérií odomykaní). Môžeme teda predpokladať, že úspešnosť správnej autentifikácie používateľov je ovplyvnená aj dobou používania odomykacieho vzoru a počtom zadaných odomykacích vzorov, a teda model používateľa je vhodné postupom času aktualizovať.



Obr. 16 Vývoj hodnoty chyby EER pri postupnom trénovaní modelov používateľov

Na základe vývoja hodnoty chyby EER pre postupné prispôsobovanie modelu používateľa môžeme pokladať túto hypotézu za pravdivú.

6.8 Zhodnotenie experimentov

Na základe vykonaných experimentov, v ktorých sme určovali možnosti identifikácie kontextu odomykania a presnosť biometrického systému pri autentifikácii používateľa, môžeme povedať, že využitie identifikácie spôsobu zadania odomykacieho vzoru dokážeme vykonať s vysokou úspešnosťou, čo môže mať pozitívny vplyv na celkovú presnosť výsledku autentifikácie používateľov.

V uskutočnených experimentoch sme na verifikáciu („Single-Class“ klasifikáciu) používateľov v prvotných fázach experimentovania (EXP1) použili ohodnotenie dôležitosti

jednotlivých charakteristík bez minimalizácie optimálneho počtu charakteristík pri budovaní biometrického modelu používateľa, čo sa prejavilo na zvýšenej hodnote chyby FAR, a teda navrhnutý systém neakceptoval väčšinu vstupov od používateľov. Síce sa do systému nedostal neoprávnený používateľ, no s vysokou pravdepodobnosťou bol zamietnutý prístup aj oprávnenému používateľovi.

V ďalších fázach experimentovania sme sa preto zamerali na možnosti využitia viacerých metód pre predspracovanie dát, vyhľadanie outlierov, vyrovnanie početnosti jednotlivých tried pri určení kontextu a autentifikácie používateľa, navrhnutie dokonalejšej metódy na výber a minimalizáciu signifikantných charakteristík a využitie informačnej fúzie na úrovni porovnávacieho skóre. Pôvodné nevyvážené hodnoty chýb FAR a FRR sa nám podarilo vyvážiť (pre najlepšiu metódu s najnižšou hodnotou chyby EER sme dosiahli chyby **FAR = 0.218237** a **FRR = 0.289009**), pričom finálna hodnota určujúca úspešnosť navrhnutého biometrického systému dosahovala hodnotu **EER = 0.057182** (kompletné výsledky jednotlivých metód uvádzame v Tab. 13 Výsledky autentifikácie používateľa využitím viacerých metód v procese návrhu systému).

Porovnanie s existujúcimi prístupmi. Pre porovnanie dosiahnutých výsledkov s existujúcimi riešeniami uvádzanými v analýze stavu problematiky (v Tab. 4 Dosahované výsledky analyzovaných prác) sme vybrali iba tie prístupy, ktoré sa zaoberali autentifikáciou používateľa na mobilných zariadeniach. Tieto prístupy sa odlišovali okrem typu sledovaných charakteristík aj počtom ľudí zapojených do experimentu a počtom sledovaných charakteristík.

Vzhľadom na počet ľudí zapojených do experimentu a typ experimentovanie (neriadený experiment v domácich podmienkach) môžeme usúdiť, že úspešnosť nami navrhnutého biometrického systému určená na základe hodnoty chyby EER je vyššia ako v podobných prácach uvádzaných v analytickej časti tejto práce (2.7 Podobné práce). Výnimkou je práca od [GIOFFRIDA14] a [RAO14], tieto práce však vykonávali autentifikáciu používateľov iba na malom množstve ľudí zapojených do experimentu, a tak sú tieto výsledky ovplyvnené priamo veľkosťou dát, pomocou ktorých bola hodnota chyby EER určená (vo všeobecnosti sa dá tvrdiť, že čím je počet ľudí zapojených do experimentu nižší, tým je spoľahlivosť určeného výsledku presnosti biometrického systému nižšia).

Tab. 8 Porovnanie výsledkov analyzovaných prác s dosiahnutými výsledkami v tejto práci

Práca	**Typ[6]**	**Zapojených ľudí do experimentu**	**Počet sledovaných charakteristík**	**FAR**	**FRR**	**EER**
[NGUYEN17]	3, 4, 6	10	-	-	-	0,070
[RAO14]	3, 4, 8	4	-	0,03	0,03	0,010
[CORPUS16]	1, 2, 8	30	-	0,07	0,4	-
[GIOFFRIDA14]	1, 2, 3, 7	10	-	-	-	0,008
[ALARIKI16]	3, 4	13	84	0,01	0,08	0,083
[BURIRO16]	3, 4, 8	26	-	0,11	0,04	0,076
Dosiahnuté výsledky	3, 4, 7, 8	33	136 (optim.)	0,22	0,29	**0,057**

Nami navrhnutú metódu pre budovanie modelov používateľov pre biometrickú autentifikáciu hľadaním signifikantných charakteristík z veľkého počtu sledovaných charakteristík pomocou spätnej eliminácie na základe ohodnotenia dôležitosti jednotlivých charakteristík pomocou viacerých typov klasifikátorov tak pokladáme za úspešnú, nakoľko sa nám podarilo minimalizovať hodnotu chyby EER so zachovaním vyváženosti chýb FAR a FRR. Nami navrhnutý systém teda nie je aj napriek použití „One Class“ klasifikátora náchylný na akceptovanie neautorizovaných a neakceptovanie autorizovaných prístupov do systému.

[6] Typ práce je určený podľa Zn. v Tab. 3 Sumarizácia existujúcich prístupov.

7 Zhodnotenie

V tejto diplomovej práci sme analyzovali existujúce prístupy a metódy budovania a overovania biometrického modelu používateľa za účelom zvýšenia zabezpečenia mobilných zariadení. Skúmali sme možnosti budovania biometrických systémov a zachytávania biometrických charakteristík na mobilných zariadeniach prostredníctvom dotykovej obrazovky a mobilných polohovacích senzorov.

V rámci vytvorenia predstavy o procese biometrickej autentifikácie sme analyzovali základné charakteristiky biometrických systémov a základné typy procesov autentifikácie používateľov. Zamerali sme na možnosti budovania biometrického modelu používateľa a výber vhodných charakteristík, ktoré najviac dokáže prispieť k výsledku autentifikácie.

Pri analýze existujúcich riešení sme sa zamerali na práce, ktoré skúmali využitie behaviorálnych biometrických charakteristík používateľov pre ich autentifikáciu. Zhodnotili a porovnali sme výsledky týchto prác a vytvorili sme zhrnutie existujúcich prístupov na základe spôsobu tvorby a overovania používateľského modelu.

V praktickej časti tejto práce sme zadefinovali požiadavky na vytváraný biometrický systém, vytvorili sme návrh architektúry, procesu budovania biometrického modelu používateľa a procesu autentifikácie používateľov s využitím informačnej fúzie na úrovni porovnávacieho skóre.

Pre overenie navrhnutého riešenia autentifikácie používateľov sme vykonali sadu experimentov, pomocou ktorých sme zozbierali dostatočne veľkú množinu používateľských odomknutí zariadení, ktorú sme ďalej využili v návrhu procesu autentifikácie pri budovaní kontextových a používateľských biometrických modelov. Tento proces pozostával z predspracovania dát za účelom získania ďalších biometrických charakteristík, vyhľadania a odstránenia anomálií v dátach, experimentov pri vyhľadávaní vhodných (signifikantných) biometrických charakteristík a samotnej klasifikácie. Pre navrhnutý proces autentifikácie používateľov sme overili vhodnosť navrhnutých metód, ktoré pozostávali z identifikácie referenčného modelu používateľa na základe spôsobu práce so zariadením (kontextu odomykania), a následne zo „Single-Class“ klasifikácie používateľa pomocou tohto modelu. Najvyššia dosiahnutá presnosť biometrického systému vyjadrená pomocou miery *EER* bola *0.057,* čo je v porovnaní s prácami zaoberajúcimi sa podobnou problematikou porovnateľne lepší výsledok (nižšia hodnota EER), čo znamená, že presnosť nami navrhnutého biometrického systému bola vyššia.

V rámci overovania stanovených hypotéz, ktoré vyplynuli z analytickej časti tejto

práce (uvádzané v časti 3 Ciele práce a výskumné hypotézy) sme dospeli k zisteniu, že veľkosť vybranej množiny charakteristík môže mať nepriamy vplyv na výslednú úspešnosť biometrického systému (hodnotu chyby EER), a teda zväčšovanie množiny sledovaných biometrických charakteristík môže mať negatívny dopad na výsledok autentifikácie používateľa.

Pre zvýšenie úspešnosti autentifikácie používateľov sme v procese autentifikácie navrhli spôsob vykonania informačnej fúzie na úrovni porovnávacieho skóre pre rôzne modely používateľov určené na základe množín vzorovo závislých a nezávislých charakteristík. Síce sa náročnosť trénovania modelov pomocou takto rozdelených modelov pre vzorovo závislé a nezávislé charakteristiky znížila, výsledná úspešnosť biometrického systému bola nižšia, čo znamená, že nami navrhnutá fúzia na úrovni porovnávacieho skóre neprispela k zvýšeniu úspešnosti navrhnutého biometrického systému.

Na základe pozorovaní sme taktiež predpokladali, že sa presnosť biometrického systému môže prirodzene zlepšovať v priebehu času a so zvyšujúcim sa množstvom zadaných odomykacích vzorov, nakoľko sa pre používateľov stane odomykanie zariadenia a používanie vybraného odomykacieho vzoru prirodzené. Túto hypotézu sa nám podarilo dokázať pozorovaním prirodzeného znižovania hodnoty EER pre postupné trénovanie modelov používateľov na dátach z dlhodobého experimentu (úspešnosť biometrického systému sa prirodzene zlepšovala, hodnota EER postupne klesala).

Pokračovanie tejto diplomovej práce vidíme v navrhnutí úspešnejšej metódy informačnej fúzie na úrovni nielen porovnávacieho skóre, ale aj na úrovní zbieraných biometrických charakteristík (vlastností). Aj keď nami navrhnutý spôsob informačnej fúzie nebol úspešný, tento prístup má určite vysoký potenciál (možností využitia informačnej fúzie je hneď niekoľko).

Literatúra

[ABARI08] ABARI, A., THORPE, J., OORSCHOT, P. *On Purely Automated Attacks and Click-Based Graphical Passwords*. In: ACSAC ’08, Proceedings of the 2008 Annual Computer Security Applications Conference. Washington: IEEE, 2008. ISBN 978-0-7695-3447-3, s. 111-120.

[ALARIKI16] ALARIKI, A., MANAF, A., MOUSAVI, S. *Features Extraction Scheme for Behavioural Biometric Authentication in Touchscreen Mobile Devices*. In: International Journal of Applied Engineering Research, Volume 11, Research India Publications, 2016. ISSN 0973-4562, s. 9331-9344.

[ANTAL15] ANTAL, M., SZABÓ, L., LÁSZLÓ, I. *Keystroke Dynamics on Android Platform*, In: Procedia Technology, Volume 19, 2015. ISSN 2212-0173, s. 820-826.

[ARONOWITZ14] ARONOWITZ, A., LI, M., TOLEDO-RONEN, O. et al. *Multi-modal biometrics for mobile authentication*. In: IEEE International Joint Conference on Biometrics. Clearwater, USA: IEEE, 2014. ISBN: 978-1-4799-3584-0, s. 1-8.

[BERGADANO02] BERGADANO, F., GUNETTI, D., PICARDI, C. User Authentication Through Keystroke Dynamics. In: ACM Trans. Inf. Syst. Secur., New York: ACM, 2002. ISSN 1094-9224, s. 367-397.

[BIDDLE12] BIDDLE, R., CHIASSON, S., OORSCHOT, P. *Graphical Passwords: Learning from the First Twelve Years*. In: ACM Computing Surveys. Volume 44, New York: ACM, 2012. ISSN 0360-0300, 25 s.

[BURIRO16] BURIRO, A., CRISPO, B., FRARI, F. et al. *ITSME: Multi-modal and Unobtrusive Behavioural User Authentication for Smartphones.* Lecture Notes in Computer Science. Volume 9551, Cham: Springer, 2016. ISBN: 978-3-319-29938-9.

[CORPUS16] CORPUS, K., GONZALES, R., MORADA, A. et al. *Mobile user identification through authentication using keystroke dynamics and accelerometer biometrics*. In: MOBILESoft ’16, Mobile Software Engineering and Systems. Austin: IEEE, 2016. ISBN 978-1-4503-4178-3, s. 11-12.

[FRANK13] FRANK, M., BIEDERT, R., MA, E. et al. *Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication.* In: IEEE Transactions on Information Forensics and Security, Volume 8. Washington: IEEE, 2013. S. 136-148.

[GAMBERGER97] GAMBERGER, D., LAVRAČ, N. *Conditions for Occam's razor applicability and noise elimination.* In: ECML-97, European Conference on Machine Learning, 1997. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN 978-3-540-68708-5, s. 108-123.

[GIOFFRIDA14] GIOFFRIDA, C., MAJDANIK, K., CONTI, M. et al. *I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics*. In: DIMVA ‘14, Dietrich S. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. Cham: SPRINGER, 2014. ISBN 978-3-319-08508-1, s. 92-111.

[JOSEPH10] JOSEPH, N. et al. *Biometric Recognition: Challenges and Opportunities.* Washington, DC: The National Academies Press, 2010. ISBN: 978-0-309-14207-7.

[KIRA92] KIRA, K., RENDELL, L. The Feature Selection Problem: Traditional Methods and a New Algorithm. In: AAAI ’92 Proceedings of the tenth national conference on Artificial intelligence. San Jose, California, 1992. ISBN 0-262-51063-4, s. 129-134.

[LIN12] LIN, CH., CHANG, CH., LIANG, D. *A New Non-Intrusive Authentication Method based on the Orientation Sensor for*

Smartphone Users. In: SERE ’12, Software Security and Reliability, Gaithersburg: IEEE, 2012. ISBN 978-1-4673-2067-2, s. 245-252.

[MANORANJAN03] MANORANJAN, D., LIU, H. *Consistency-based search in feature selection.* In: Artificial Intelligence. Volume 151, 2003. s. 155-176.

[MESZAROS07] MESZAROS, A., BANKO, Z., CZUNI, L. *Strengthening Passwords by Keystroke Dynamics*. In: IDAACS ’07, Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IEEE 2007. ISBN 978-1-4244-1347-8.

[NGUYEN17] NGUYEN, T., VORIS, J. *Touchscreen Biometrics Across Multiple Devices*. In: SOUPS ’17, Thirteenth Symposium on Usable Privacy and Security, Santa Clara: USENIX, 2017.

[PARK16] PARK, J., KIM, T., IM, E. *Touch Gesture Data Based Authentication Method for Smartphone Users*. In: RACS ‘16, Proceedings of the International Conference on Research in Adaptive and Convergent Systems. New York: ACM, 2016. ISBN 978-1-4503-4455-5, s. 136-141.

[RAO14] RAO, K., ANNE, V., SAI, CH. et al. *Inclination and Pressure Based Authentication for Touch Devices*. In: AISC ’14, Proceedings of the 48th Annual Convention of Computer Society of India, Volume 1, Cham: SPRINGER, 2014. ISBN 978-3-319-03107-1, s. 781-788.

[RAK08] RAK, R., MATYÁŠ, V., ZDENĚK, Ř. et al. *Biometrie a identita člověka – ve forenzních a komerčních aplikacích.* Praha: Grada Publishing, a.s., 2008. ISBN 978-80-247-2365-5, s. 104-106.

[ROSS06] ROSS, A., KARTHIK, N., ANIL, J. *Handbook of Multibiometrics (International Series on Biometrics).* Berlin: Springer-Verlag, 2006. ISBN 0387222960.

[ROSS07] ROSS, A. *Introduction to Multibiometrics.* In: EUSIPCO, Proc. of the 15th European Signal Processing Conference, 2007. Poznan, Poland, 2007. s. 271-292.

[SANDERSON02] SANDERSON, C., PALIWAL, K. *Information fusion and person verification using speech and face information.* Research Paper IDIAP-RR 02-33, IDIAP, 2002.

[SANDHYA16] SANDHYA, A., TANUSHREE, S. *Biometric Authentication Techniques: A Study on Keystroke Dynamics.* In: IJSEAS ‘16, International Journal of Scientific Engineering and Applied Science, Volume 2, 2016. ISSN 2395-3470, s. 215-221.

[SCHLENKER13] SCHLENKER, A., SAREK, M. *Neural Networks in Keystroke Dynamics for Multi-Factor Authentication in Biomedicine*. In: MEASUREMENT 2013, Proceedings of the 9th International Conference, Bratislava: Institute of Measurement Science SAS, 2013. ISBN 978-80-969672-5-4, s. 109-112.

[STALLINGS05] STALLINGS, W. *Cryptography and Network Security (4th Edition)*. New Jersey, USA: Prentice Hall, Inc., 2005. ISBN 0131873164.

[UNNIKRISHAN14] UNNIKRISHAN, P. *Feature selection and Classification Approaches for Biometric and Biodecimal Applications.* RMIT University, 2014. 96 s.

[VIELHAUER06] VIELHAUER, C. *Biometric User Authentication for IT Security.* Megdeburg, Nemecko: Springer Science+Business Media, Inc., 2006. ISBN: 0-387-28094-4.

[WILK16] WILK, B., OLBRYCHT S. *Assessment of a hand tremor based on analysis of the accelerometer signal.* In: Przeglad Elektrotechniczny 2016. s. 146-149

Príloha A: Príklad zaznamenanej biometrickej vzorky

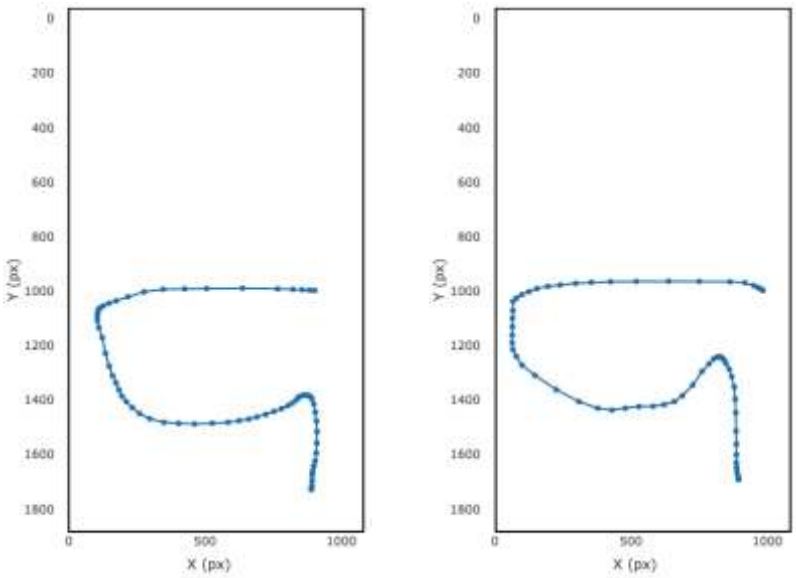
Táto príloha obsahuje príklad zaznamenaných biometrických údajov používateľa. Fig. 1 Zaznamenaná udalosť odomknutia (JSON) znázorňuje dáta posielané na server vo formáte JSON, ktoré sme zredukovali o zaznamenané dotykové, akceleračné a pohybové udalosti kvôli veľkej dĺžke záznamu.

V samotných dátach sa už nachádzajú predvypočítané charakteristiky, ktoré sú určené priamo na zariadení používateľa (atribút *metrics* (sl. metriky)).


```
{
  "_id": "5ae7056bbeb35e839bdded9b",
  "user": "5ace253ae8acbc8786cfc73a",
  "timestamp": "2018-04-30T11:59:51.072Z",
  "correct": false,
  "correctPattern": {
    "pattern": "247"
  },
  "enteredPattern": {
    "pattern": "5478"
  },
  "sequelNum": 2,
  "unlockContext": {
    "finger": "thumb",
    "hand": "right",
    "posture": "sitting",
    "testId": 1542805640535
  },
  "metrics": {
    "touchTime": 1326000000,
    "acceleration": {
      "avgAcceleration": 9.711156,
      ...
  },
    "rotation": {
      ...,
      "maxRotationX": 1.2278391,
      "maxRotationY": 0.20525073,
      ...
  },
    "touch": {
      "avgMotionVelocity": 2564.5916,
      "maxMotionVelocity": 7581.336,
      "minMotionVelocityX": -3171.0134,
      ...
    }
  },
  "touchEvents": [
    {
      "timestamp": 3169000000,
      "orientation": 0,
      "pressure": 1,
      "size": 0.003921569,
      "touchMajor": 1,
      "touchMinor": 1,
```

```
      "x": 904,
      "xVelocity": 0,
      "y": 1124,
      "yVelocity": 0
    }, ...
  ],
  "accelerationEvents": [
    {
      "timestamp": 0,
      "x": -1.5729905,
      "y": 3.0142999,
      "z": 9.167398
    }, ...
  ],
  "rotationEvents": [
    {
      "timestamp": 4965192,
      "x": -0.19914207,
      "y": -0.08674286,
      "z": 0.13133603
    }, ...
  ],
  "patternEvents": [
    {
      "timestamp": 4969192,
      "dotIndex": "4",
      "prevDotIndex": "5"
    }
...
  ]
}
```

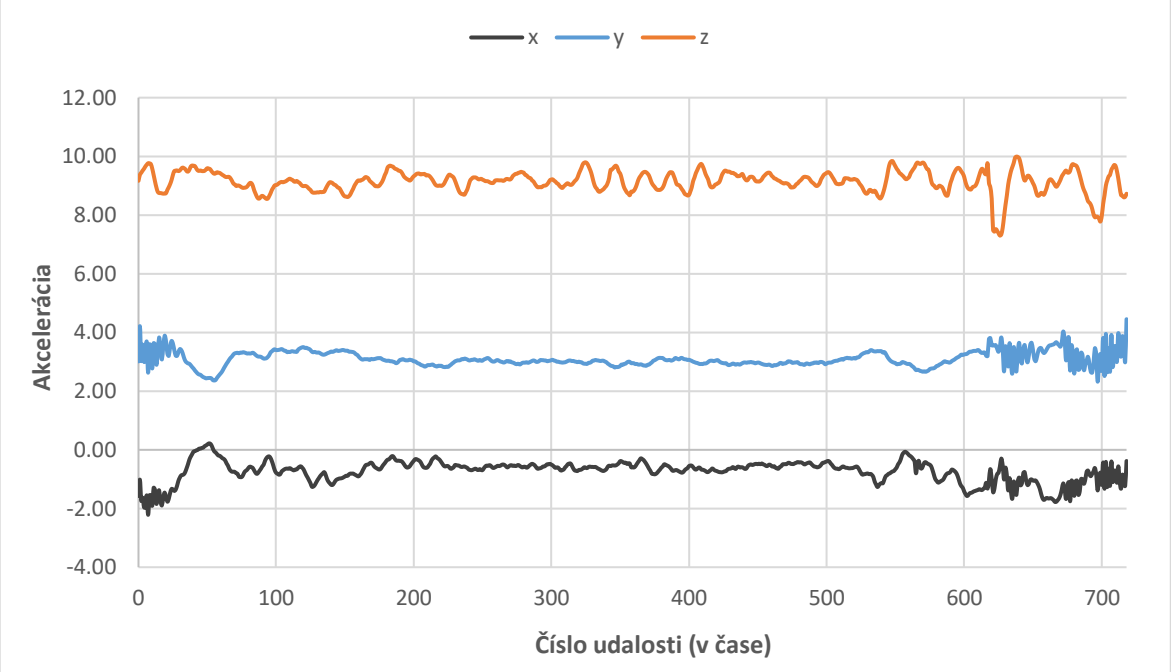

Fig. 1 Zaznamenaná udalosť odomknutia (JSON)



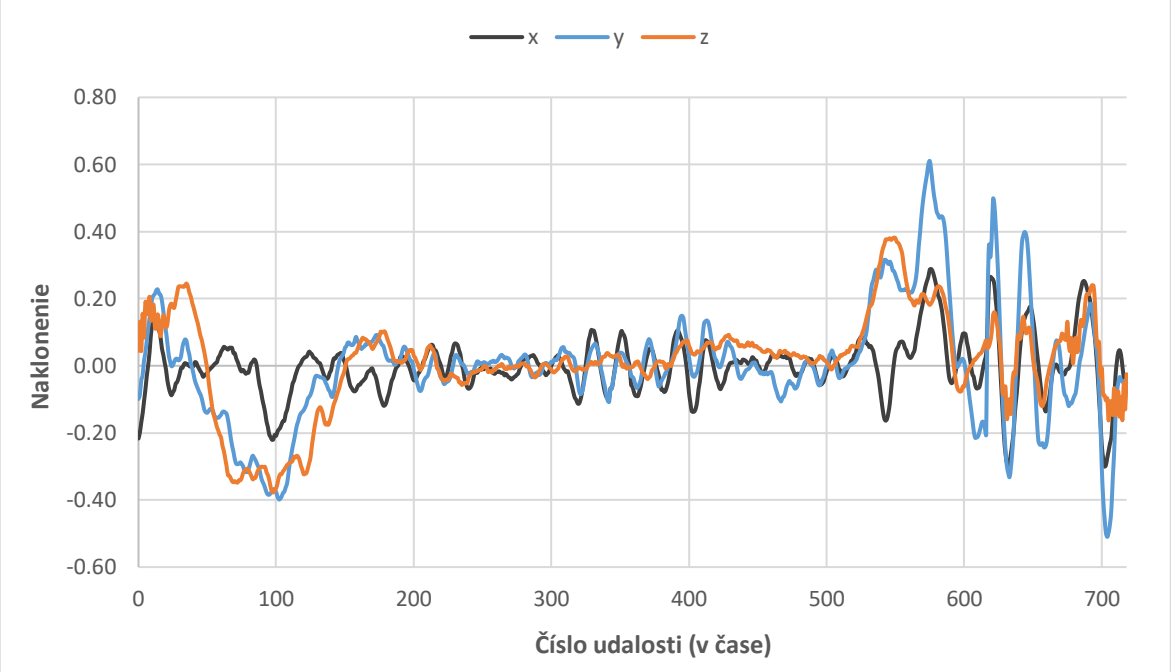
Obr. 17 Príklad vzorky – dráha odomykacieho vzoru (1 používateľ)

Na Obr. 17 Príklad vzorky – dráha odomykacieho vzoru (1 používateľ) sa ďalej nachádza dráha odomknutia zariadenia pre odomykací vzor *2103458* (index bodky) vytvorená z dát

na Fig. 1 Zaznamenaná udalosť odomknutia (JSON). Na obrázku Obr. 18 Príklad vzorky – akcelerácia je zachytená akcelerácia pohybu a na obrázku Obr. 19 Príklad vzorky – naklonenie je zachytené naklonenie zariadenia pri zadávaní odomykacieho vzoru.



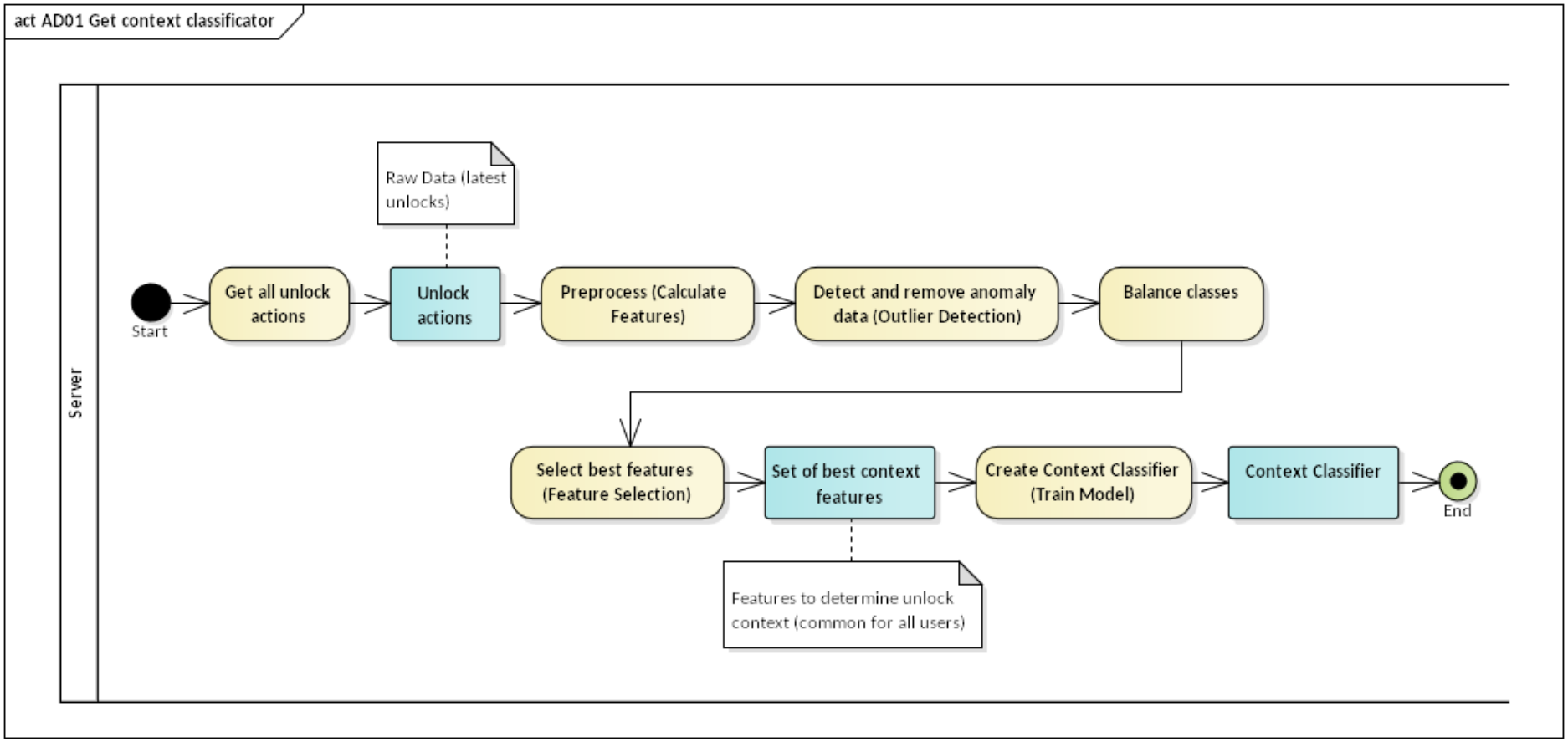
Obr. 18 Príklad vzorky – akcelerácia



Obr. 19 Príklad vzorky – naklonenie

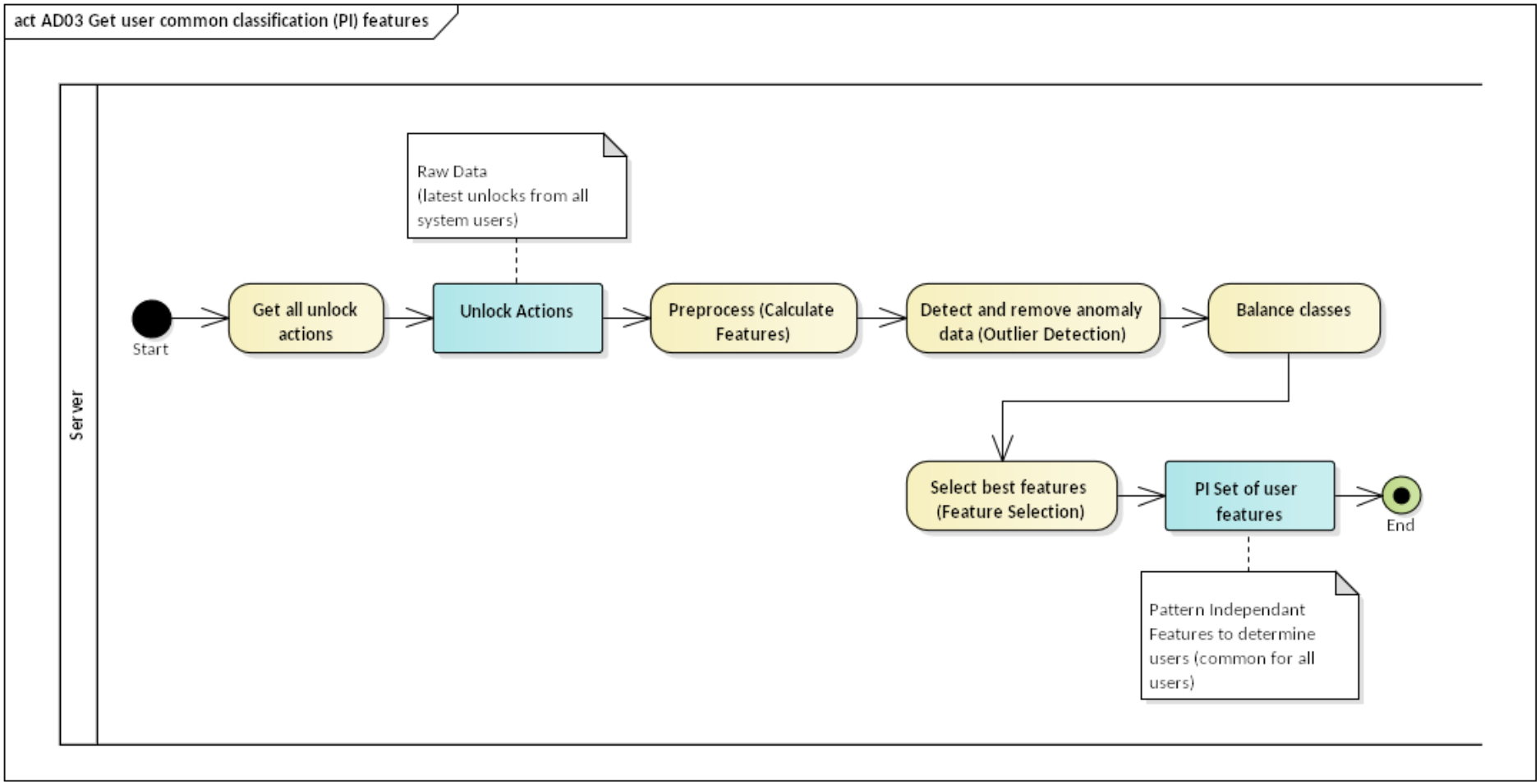
Príloha B: Procesy biometrického systému

P1 Trénovanie klasifikátora kontextu odomknutia



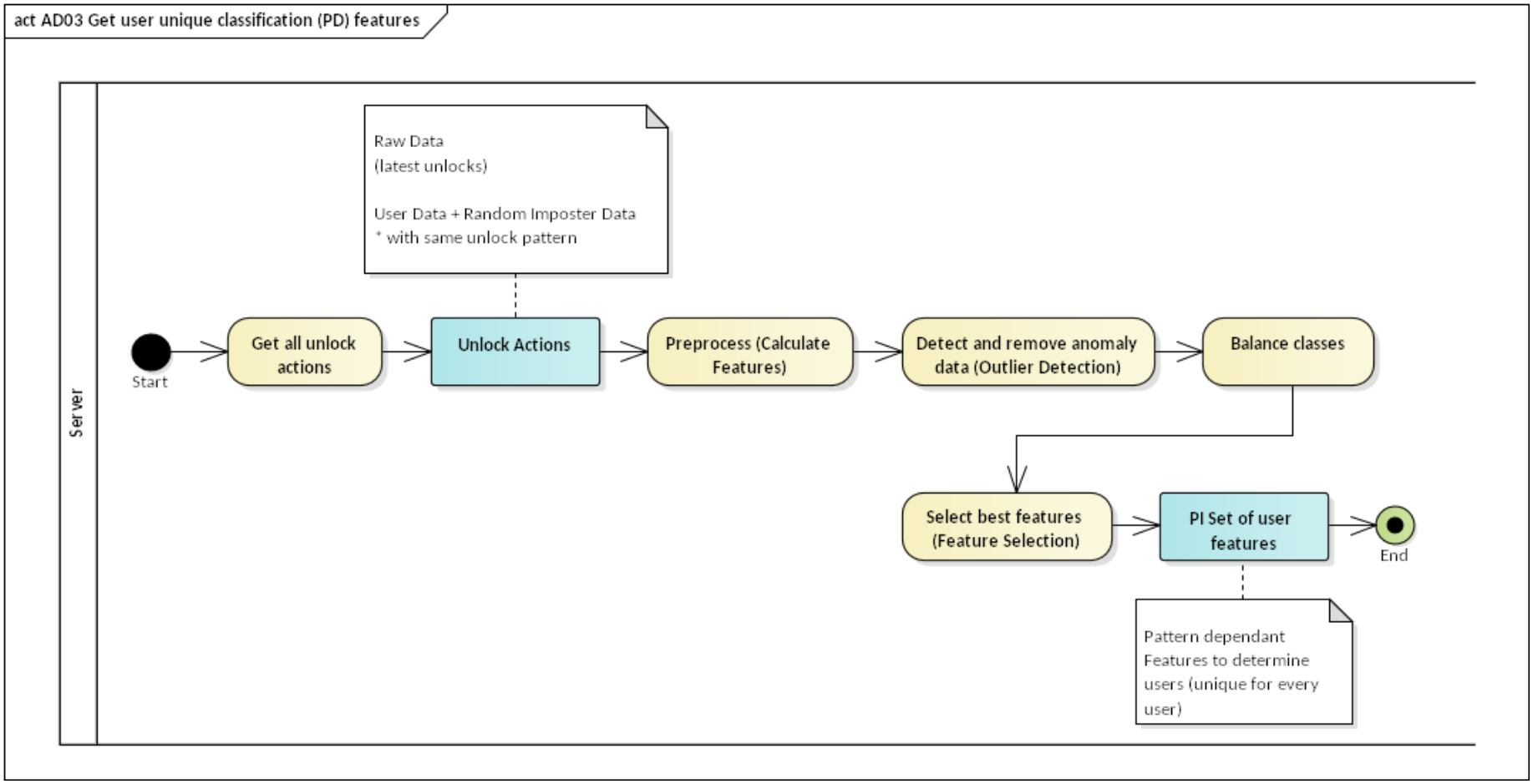
Obr. 20 AD01 Proces trénovania klasifikátora kontextu odomknutia (diagram aktivít)

P2 Získanie vzorovo nezávislých čŕt pre budovanie vzorovo nezávislého modelu používateľa



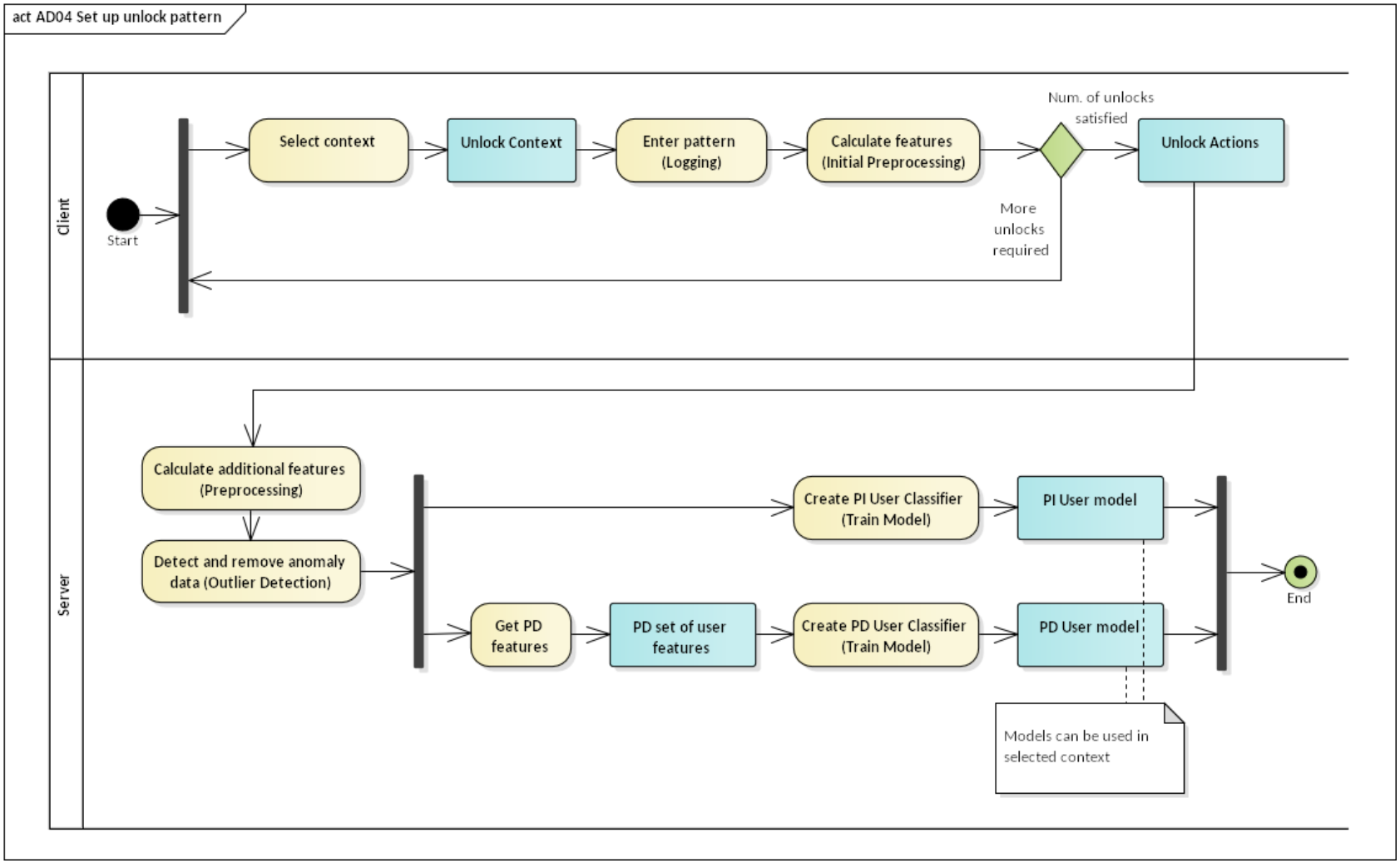
Obr. 21 AD02 Proces získania vzorovo závislých čŕt pre budovanie modelu používateľa (diagram aktivít)

P3 Získanie vzorovo závislých čŕt pre budovanie vzorovo závislého modelu používateľa



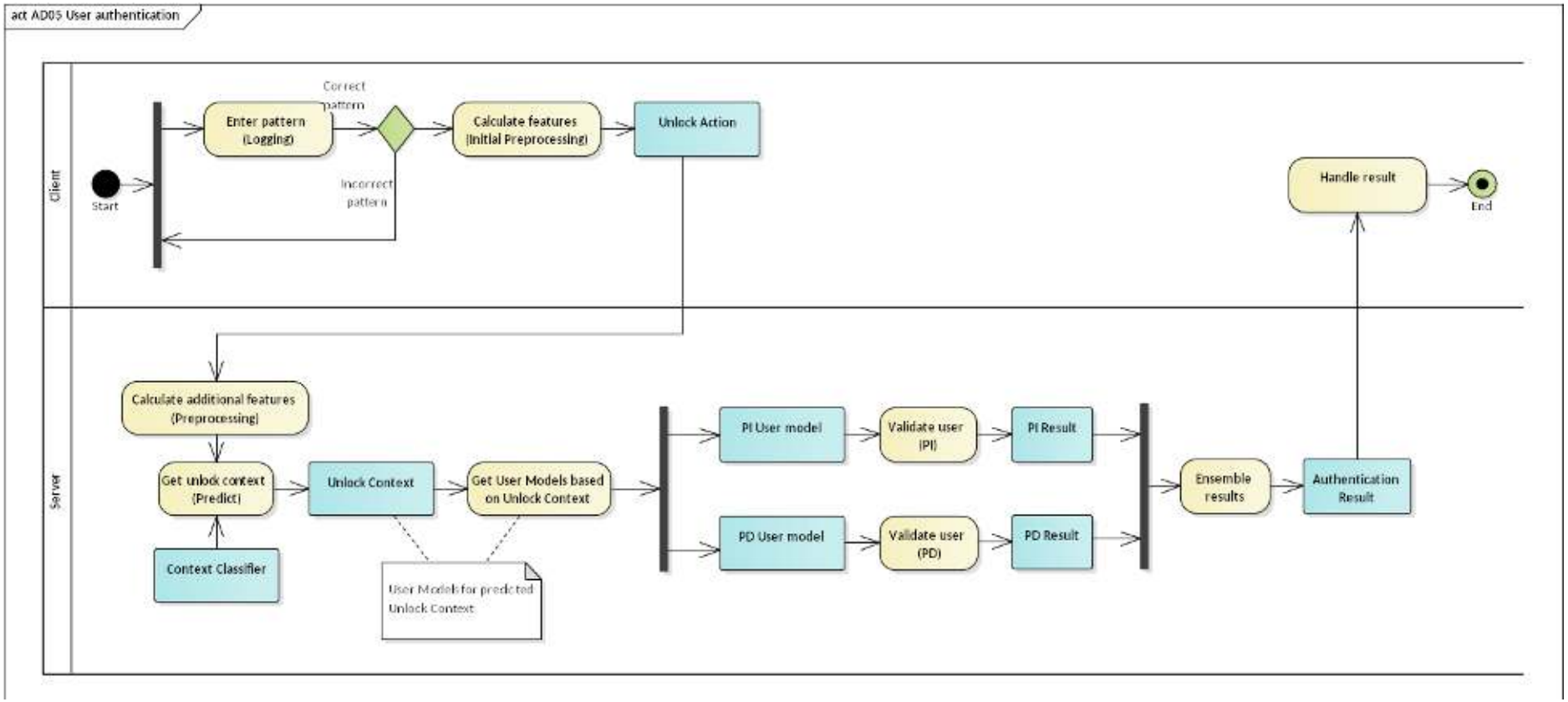
Obr. 22 AD03 Proces získania vzorovo nezávislých čŕt pre budovanie modelu používateľa (diagram aktivít)

P4 Nastavenie odomykacieho vzoru používateľom



Obr. 23 AD04 Proces nastavenia odomykacieho vzoru používateľom (diagram aktivít)

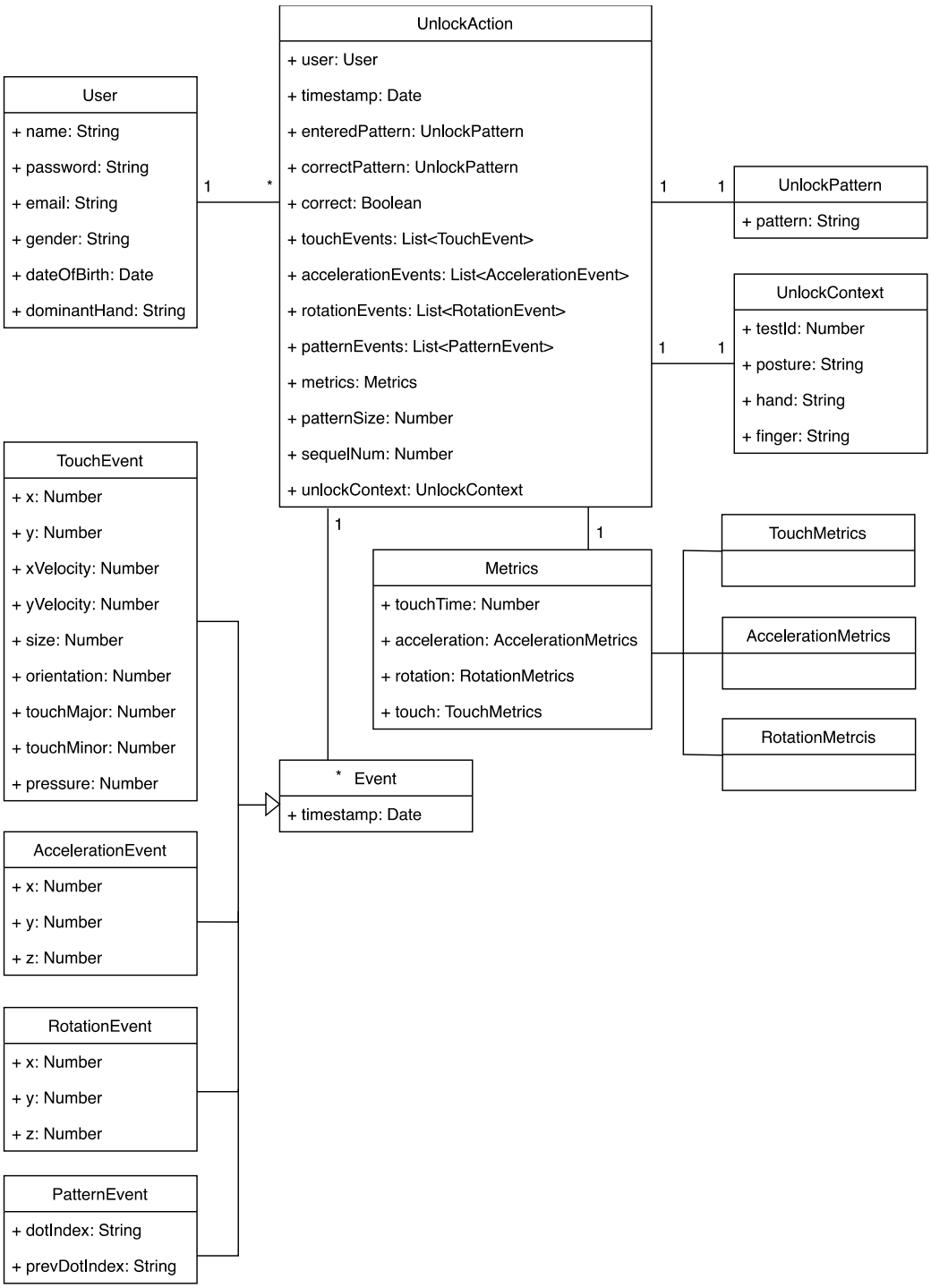
P5 Autentifikácia používateľa pri prihlásení



Obr. 24 AD05 Proces autentifikácie používateľa pri prihlásení (diagram aktivít)

Príloha C: Dátový model

Nasledujúci diagram znázorňuje dátový model vytváraného biometrického systému.



Obr. 25 Dátový model navrhnutého biometrického systému

Príloha D: Rozpis serverových API

V nasledujúcej tabuľke Tab. 9 Zoznam serverových API uvádzame zoznam podporovaných serverových API volaní, ktoré slúžia na správu používateľov a zaznamenávanie biometrických vzoriek používateľov na vzdialenom serveri. Schémy používateľa a akcie odomknutia (uvádzané v nasledujúcej tabuľke v stĺpcoch *Vstup* a *Výstup* ako *User* a *UnlockAction*) sú uvedené v prílohe Príloha C: Dátový model.

Tab. 9 Zoznam serverových API

API volanie	**Popis**	**Vstup**	**Výstup**
/users/createUser	Vytvorenie používateľa	user: User	user: User
/users/getUser/:userName	Získanie používateľa podľa mena	userName: String	user: User
/users/getUserById/:userId	Získanie používateľa podľa ID		user: User
/users/updateUser/:userId	Aktualizácia používateľa na základe ID	userId: String user: User	user: User
/users/deleteUser/:userId	Vymazanie používateľa na základe ID	userId: String	res: String
/users/listAllUsers	Získanie všetkých používateľov	-	users<User>: List
/unlockActions/createUnlockAction	Vytvorenie akcie odomknutia	uAct: UnlockAction	uAct: UnlockAction
/unlockActions/listUnlockAction/:unlockActionId	Získanie akcie odomknutia na základe ID	uActId: String	uAct: UnlockAction
/unlockActions/updateUnlockAction/:unlockActionId	Aktualizácia akcie odomknutia na základe ID	uActId: String uAct: UnlockAction	uAct: UnlockAction

/unlockActions/deleteUnlockAction/:unlockActionId	Vymazanie akcie odomknutia na základe ID	uActId: String	res: String
/unlockActions/listAllUnlockActions'	Získanie všetkých akcií odomknutia	-	uActs< uAct >: List
/unlockActions/listAllUserUnlockActions/:userId	Získanie všetkých akcií odomknutia používateľa na základe jeho ID	userId: String	uActs< uAct >: List

Príloha E: Dorátané biometrické charakteristiky

Táto príloha obsahuje zoznam biometrických charakteristík, ktoré sú dorátané zo surových biometrických dát.

Charakteristiky 68-91 sú využívané ako charakteristiky prvotného dotyku používateľa so zariadením.

Tab. 10 Dorátané biometrické charakteristiky a ich opis

Ref. dáta	**#**	**Označenie**	**Opis**
accelerationEvents	1	avg_acceleration	*priemerná akcelerácia*
	2	avg_acceleration_{A}	*priemerná akcelerácia pre jednotlivé osi A ; A = {x, y, z}*
	3	max_acceleration	*maximálna akcelerácia*
	4	max_acceleration_{A}	*maximálna akcelerácia pre jednotlivé osi A ; A = {x, y, z}*
	5	min_acceleration	*minimálna akcelerácia*
	6	min_acceleration_{A}	*minimálna akcelerácia pre jednotlivé osi A ; A = {x, y, z}*
	7	total_acceleration	*celková akcelerácia*
	8	total_acceleration_{A}	*minimálna akcelerácia pre jednotlivé osi A ; A = {x, y, z}*
rotationEvents	9	avg_rotation	*priemerná rotácia*
	10	avg_rotation_{A}	*priemerná rotácia pre jednotlivé osi A ; A = {x, y, z}*
	11	max_rotation	*maximálna rotácia*
	12	max_rotation_{A}	*maximálna rotácia pre jednotlivé osi A ; A = {x, y, z}*
	13	min_rotation	*minimálna rotácia*

	14	min_rotation_{A}	*minimálna rotácia pre jednotlivé osi A ; A = {x, y, z}*
	15	total_rotation	*celková rotácia*
	16	total_rotation_{A}	*celková rotácia pre jednotlivé osi A ; A = {x, y, z}*
touchEvents	17	avg_motion_velocity	*priemerná rýchlosť*
	18	avg_motion_velocity_{A}	*priemerná rýchlosť pre jednotlivé osi A ; A = {x, y}*
	19	max_motion_velocity	*maximálna rýchlosť*
	20	max_motion_velocity_{A}	*maximálna rýchlosť pre jednotlivé osi A ; A = {x, y}*
	21	min_motion_velocity_{A}	*minimálna rýchlosť pre jednotlivé osi A ; A = {x, y}*
	22	total_motion_velocity	*celková rýchlosť*
	23	total_motion_velocity_{A}	*celková rýchlosť pre jednotlivé osi A ; A = {x, y}*
	24	total_unlock_time	*celkový čas odomknutia*
	25	trajectory_length	*dĺžka trajektórie*
	26	starting_velocity_{A}	*začiatočná rýchlosť pre jednotlivé osi A ; A = {x, y}*
	27	starting_velocity	*začiatočná rýchlosť (z prvých n udalostí dotyku)*
	28	ending_velocity_{A}	*ukončovacia rýchlosť pre jednotlivé osi A ; A = {x, y}*
	29	ending_velocity	*ukončovacia rýchlosť (z posledných n udalostí dotyku)*
	30	average_touch_size_minor	*priemerná veľkosť dotyku (vedľajšia os)*
	31	average_touch_size_major	*priemerná veľkosť dotyku*

			(hlavná os)
	32	average_touch_size	*priemerná veľkosť dotyku*
	33	max_touch_size_minor	*maximálna veľkosť dotyku (vedľajšia os)*
	34	max_touch_size_major	*maximálna veľkosť dotyku (hlavná os)*
	35	min_roc	*minimálny polomer na trajektórii odomknutia (v px)*
	36	min_roc_center_{A}	*stred minimálneho polomeru na trajektórii odomknutia ; A = {x, y}*
touchEvents, patternEvents	37	distance_{A}{A}	*vzdialenosť medzi 2 bodmi vzoru z množiny A (veľkosť vzoru 3x3 = 9) ; A = {0...8}*
	38	time_{A}{A}	*čas medzi 2 bodmi vzoru z množiny A ; A = {0...8}*
	39	velocity_{A}{A}	*rýchlosť medzi 2 bodmi vzoru z množiny A ; A = {0...8}*
	40	min_roc_{A}{A}{A}	*minimálny polomer na trajektórii odomknutia (v px) z množiny A (medzi 3 bodmi) ; A = {0...8}*
	41	min_roc_center_{A}_{B}{B}{B}	*minimálny polomer na trajektórii odomknutia (v px) z množiny A (medzi 3 bodmi) ; A = {x, y} ; B = {0...8}*
touchEvents, rotationEvents	42	d_rotation_{A}_{B}{B}	*zmena A rotácie medzi bodmi vzoru z množiny B ; A = {x, y, z} ; B = {0...8}*

touchEvents, accelerationEvents	43	d_acceleration_{A}_{B}{B}	*zmena A akcelerácie medzi bodmi vzoru z množiny B* *; A = {x, y, z}* *; B = {0...8}*
accelerationEvents	44	acc_{A}_dominant_freq	*dominantná frekvencia akcelerácie v smere osi A* *; A = {x, y, z}*
	45	acc_{A}_dominant_freq_amp	*amplitúda dominantnej frekvencie akcelerácie v smere osi A* *; A = {x, y, z}*
	46	acc_{A}_mean_freq	*modus hodnota frekvencií akcelerácie v smere osi A* *; A = {x, y, z}*
	47	acc_{A}_med_freq	*stredná hodnota frekvencií akcelerácie v smere osi A* *; A = {x, y, z}*
	48	acc_{A}_avg_freq	*priemerná hodnota frekvencií akcelerácie v smere osi A* *; A = {x, y, z}*
	49	acc_{A}_total_ampl	*celková hodnota frekvencií akcelerácie v smere osi A* *; A = {x, y, z}*
	50	acc_{A}_avg_ampl	*priemerná hodnota amplitúd frekvencií akcelerácie v smere osi A* *; A = {x, y, z}*
	51	acc_{A}_freq_sum_1	*súčet amplitúd frekvencií akcelerácie v smere osi A v rozmedzí indexov <0-50)* *; A = {x, y, z}*
	52	acc_{A}_freq_sum_2	*súčet amplitúd frekvencií akcelerácie v smere osi A v rozmedzí indexov <50-100)* *; A = {x, y, z}*
	53	acc_{A}_freq_sum_3	*súčet amplitúd frekvencií akcelerácie v smere osi A v rozmedzí indexov <100-150)*

			; A = {x, y, z}
	54	acc_{A}_freq_sum_4	*súčet amplitúd frekvencií akcelerácie v smere osi A v rozmedzí indexov <150-200)* *; A = {x, y, z}*
	55	acc_{A}_freq_sum_5	*súčet amplitúd frekvencií akcelerácie v smere osi A v rozmedzí indexov <200-...)* *; A = {x, y, z}*
rotationEvents	56	rot_{A}_dominant_freq	*dominantná frekvencia rotácie v smere osi A* *; A = {x, y, z}*
	57	rot_{A}_dominant_freq_amp	*amplitúda dominantnej frekvencie rotácie v smere osi A* *; A = {x, y, z}*
	58	rot_{A}_mean_freq	*modus hodnota frekvencií rotácie v smere osi A* *; A = {x, y, z}*
	59	rot_{A}_med_freq	*stredná hodnota frekvencií rotácie v smere osi A* *; A = {x, y, z}*
	60	rot_{A}_avg_freq	*priemerná hodnota frekvencií rotácie v smere osi A* *; A = {x, y, z}*
	61	rot_{A}_total_ampl	*celková hodnota frekvencií rotácie v smere osi A* *; A = {x, y, z}*
	62	rot_{A}_avg_ampl	*priemerná hodnota amplitúd frekvencií rotácie v smere osi A* *; A = {x, y, z}*
	63	rot_{A}_freq_sum_1	*súčet amplitúd frekvencií rotácie v smere osi A v rozmedzí indexov <0-50)* *; A = {x, y, z}*
	64	rot_{A}_freq_sum_2	*súčet amplitúd frekvencií rotácie v smere osi A v rozmedzí indexov <50-100)* *; A = {x, y, z}*

	65	rot_{A}_freq_sum_3	*súčet amplitúd frekvencií rotácie v smere osi A v rozmedzí indexov <100-150) ; A = {x, y, z}*
	66	rot_{A}_freq_sum_4	*súčet amplitúd frekvencií rotácie v smere osi A v rozmedzí indexov <150-200) ; A = {x, y, z}*
	67	rot_{A}_freq_sum_5	*súčet amplitúd frekvencií rotácie v smere osi A v rozmedzí indexov <200-...) ; A = {x, y, z}*
touchEvents, accelerationEvents	68	first_touch_acc_{A}_dominant_freq	*dominantná frekvencia akcelerácie prvotného dotyku v smere osi A ; A = {x, y, z}*
	69	first_touch_acc_{A}_dominant_freq_amp	*amplitúda dominantnej frekvencie akcelerácie v smere osi A ; A = {x, y, z}*
	70	first_touch_acc_{A}_mean_freq	*modus hodnota frekvencií akcelerácie v smere osi A ; A = {x, y, z}*
	71	first_touch_acc_{A}_med_freq	*stredná hodnota frekvencií akcelerácie prvotného dotyku v smere osi A ; A = {x, y, z}*
	72	first_touch_acc_{A}_avg_freq	*priemerná hodnota frekvencií akcelerácie prvotného dotyku v smere osi A ; A = {x, y, z}*
	73	first_touch_acc_{A}_total_ampl	*celková hodnota frekvencií akcelerácie prvotného dotyku v smere osi A ; A = {x, y, z}*
	74	first_touch_acc_{A}_avg_ampl	*priemerná hodnota amplitúd frekvencií akcelerácie prvotného dotyku v smere osi A ; A = {x, y, z}*
	75	first_touch_acc_{A}_freq_sum_1	*súčet amplitúd frekvencií*

			akcelerácie prvotného dotyku v smere osi A v rozmedzí indexov <0-50) *; A = {x, y, z}*
	76	first_touch_acc_{A}_freq_sum_2	*súčet amplitúd frekvencií akcelerácie prvotného dotyku v smere osi A v rozmedzí indexov <50-100)* *; A = {x, y, z}*
	77	first_touch_acc_{A}_freq_sum_3	*súčet amplitúd frekvencií akcelerácie prvotného dotyku v smere osi A v rozmedzí indexov <100-150)* *; A = {x, y, z}*
	78	first_touch_acc_{A}_freq_sum_4	*súčet amplitúd frekvencií akcelerácie prvotného dotyku v smere osi A v rozmedzí indexov <150-200)* *; A = {x, y, z}*
	79	first_touch_acc_{A}_freq_sum_5	*súčet amplitúd frekvencií akcelerácie prvotného dotyku v smere osi A v rozmedzí indexov <200-...)* *; A = {x, y, z}*
touchEvents, accelerationEvents	80	first_touch_rot_{A}_dominant_freq	*dominantná frekvencia rotácie prvotného dotyku v smere osi A* *; A = {x, y, z}*
	81	first_touch_rot_{A}_dominant_freq_amp	*amplitúda dominantnej frekvencie rotácie v smere osi A* *; A = {x, y, z}*
	82	first_touch_rot_{A}_mean_freq	*modus hodnota frekvencií rotácie v smere osi A* *; A = {x, y, z}*
	83	first_touch_rot_{A}_med_freq	*stredná hodnota frekvencií rotácie prvotného dotyku v smere osi A* *; A = {x, y, z}*
	84	first_touch_rot_{A}_avg_freq	*priemerná hodnota frekvencií rotácie prvotného dotyku v smere osi A*

			; A = {x, y, z}
	85	first_touch_rot_{A}_total_ampl	*celková hodnota frekvencií rotácie prvotného dotyku v smere osi A* *; A = {x, y, z}*
	86	first_touch_rot_{A}_avg_ampl	*priemerná hodnota amplitúd frekvencií akcelerácie prvotného dotyku v smere osi A* *; A = {x, y, z}*
	87	first_touch_rot_{A}_freq_sum_1	*súčet amplitúd frekvencií rotácie v smere osi A v rozmedzí indexov <0-50)* *; A = {x, y, z}*
	88	first_touch_rot_{A}_freq_sum_2	*súčet amplitúd frekvencií rotácie v smere osi A v rozmedzí indexov <50-100)* *; A = {x, y, z}*
	89	first_touch_rot_{A}_freq_sum_3	*súčet amplitúd frekvencií rotácie v smere osi A v rozmedzí indexov <100-150)* *; A = {x, y, z}*
	90	first_touch_rot_{A}_freq_sum_4	*súčet amplitúd frekvencií rotácie v smere osi A v rozmedzí indexov <150-200)* *; A = {x, y, z}*
	91	first_touch_rot_{A}_freq_sum_5	*súčet amplitúd frekvencií rotácie v smere osi A v rozmedzí indexov <200-...)* *; A = {x, y, z}*

Príloha F: Opis modulov pre autentifikáciu používateľa

Umiestnenie: source codes/dpLockJupiterNotebook/modules/

Moduly a metódy dostupné v jednotlivých moduloch boli vytvorené pre účely návrhu a overenia riešenia biometrického systému na autentifikáciu používateľov.

Vytvorenie spojenia s databázou

Súbor: db_connection.py

Dostupné triedy:

- DBConnection(db_url, port): *vytvorí pripojenie k databáze pre danú url a port*

Dostupne metódy:

- DBConnection.connect(db_name): *nadviaže spojenie s databázou (daná menom db_name)*
- DBConnection.close(): *ukonči spojenie s databázou*

Export dát z databázy do DataFrame pre účely experimentov

Súbor: export_db_to_df_functions.py

Dostupné metódy:

- get_identificators(unlock_action): *získa sadu identifikačných charakteristík akcie odomknutia*
- get_acceleration_metrics(unlock_action): *získa sadu akceleračných metrík vypoćítaných na klientsom zariadení*
- get_rotation_metrics(unlock_action): *získa sadu rotačných metrík vypočítaných na klientsom zariadení*
- get_touch_metrics(unlock_action): *získa sadu dotykových metrík vypočítaných na klientsom zariadení*

Predspracovanie dát (rátanie dodatočných charakteristík)

Súbor: preprocess_functions.py

Dostupné metódy:

- get_total_unlock_time(unlock_action): *získa celkový čas zadávania odomykacieho*

vzoru (v ms)

- get_trajectory_length(unlock_action): *získa celkovú dĺžku trajektórie odomykacieho vzoru (v px)*
- get_starting_velocity(unlock_action, starting_events_num): *získa začiatočnu rýchlosť kreslenia vzoru (v px/s) pre zadaný počet štartovacích udalostí*
- get_ending_velocity(unlock_action, ending_events_num): *získa ukončovaciu rýchlosť kreslenia vzoru (v px/s) pre zadaný počet ukončovacích udalostí*
- get_pressure_metrics(unlock_action): *získa metriky tlaku*
- get_touch_size_metrics(unlock_action): *získa metriky veľkosti dotyku (prsta)*
- get_touch_time_map(unlock_action): *získa mapu všetkých sekvencií (dvojíc) bodov vzoru s časovými metrikami pre tieto sekvencie*
- get_rotation_deltas_map(unlock_action): *získa mapu všetkých sekvencií (dvojíc) bodov vzoru s metrikami rotácie pre tieto sekvencie*
- get_acceleration_deltas_map(unlock_action): *získa mapu všetkých sekvencií (dvojíc) bodov vzoru s metrikami akcelerácie pre tieto sekvencie*
- do_calc_ROC(curv_point_list): *pre zadaný zoznam dotykových udalostí vypočíta minimálny polomer a stred minimálneho polomeru*
- get_minimum_curvature(unlock_action): *vráti metriky zatočení v rámci dotykových udalostí odomknutia*
- get_minimum_curvature_triples(unlock_action): *vráti metriky zatočení v rámci dotykových udalostí odomknutia pre všetky trojice bodov v rámci vzoru*
- get_touch_start_events(unlock_action, padd_time, min_num_events, events_type): *pre vybraný typ udalostí (akceleračné, rotačné) vráti zoznam začiatočných udalosti odomknutia pre zadaný časový rozsah od prvej dotykovej udalosti s minimálnym počtom udalostí*
- get_frequency_analysis_metrics(unlock_action, x, y, type): *vráti metriky, ktoré sú výsledko frekvenčnej analýzy vybraného typu udalostí (akceleračné, rotačné)*

Predspracovanie dát (vyhľadávanie outlierov, vyrovnanie početnosti tried pre výber charakteristík a klasifikáciu)

Súbor: outliers_functions.py

Dostupné metódy:

- get_unique_hour_identifier(unlock_action): *vráti unikátny identifikátor pre akciu*

odomknutia na základe atribútu test_id akcie odomknutia (dátumová pečiatka vytvorenia akcie odomknutia)

- find_outliers(df, feature_names): *pre dané dáta urči outlierov pomocou Z-SCORE a IQR metódy*

Výber dominantnej množiny charakteristík

Súbor: feature_selection_functions.py

Dostupné metódy:

- calculate_vif(X, num_samples=1000, thresh=5): *pre dané dáta vyberie na základe počtu vzoriek a zvoleného thresholdu korelované charakteristiky*
- get_k_best(X, Y, k): *vráti ohodnotenie zoznamu charakteristík pomocou algoritmu k-best*
- get_rec_elimination(X, Y, max_iter=1000, n_features=3): *vráti ohodnotenie zoznamu charakteristík pomocou algoritmu rekurzívnej eliminácie*
- get_extra_tree(X, Y, n_estimators): *vráti ohodnotenie zoznamu charakteristík pomocou algoritmu extra-tree*
- minimize_num_of_features(clf, X, Y, best_features, cv=10): *pre vybraný klasifikátor minimalizuje počet charakteristík na základe iniciálneho zoznamu najlepších charakteristík (spoločne s krížovou validáciou výsledkov) určením presnosti (angl. accuracy) jednotlivých podmnožín charakteristík*

Súbor: genetic_feature_selection.py

- tento modul bol vytvorený na základe dostupného riešenia pre výber dominantných charakteristík pomocou genetického algoritmu dostupného online a prispôsobený pre účely optimalizácie nášho riešenia (zdroj: dkopczyk.quantee.co.uk/genetic-algorithm/).

Dostupné triedy:

- GeneticSelector(estimator, n_gen, size, n_best, n_rand, n_children, mutation_rate): *vykoná výber dominantných charakteristík pomocou genetického algoritmu*
    - *estimator: klasifikátor pre určovanie úspešnosti trénovania*
    - *n_gen:maximálny počet generácií*
    - *size:veľkosť chromozómu (iniciálny počet charakteristík)*
    - *n_best: želaný počet chormozómov (finálny počet charakteristík)*

- *n_rand:pravdepodobnosť mutácie chromozómu*
- *n_children: veľkosť populácie*
- *mutation_rate: pravdepodobnosť mutácie chromozómu*

Dostupné metódy:

- initilize(self): *vytvorí iniciálnu populáciu*
- fitness(self, population): *určí fitness skóre danej populácie*
- select(self, population_sorted): *vyberie najlepšie jedince z populácie (s najvyššou hodnotou fitness)*
- crossover(self, population): *vykoná kríženie populácie*
- mutate(self, population): *vykoná náhodnú mutáciu v populácii (zmenu jedincov)*
- generate(self, population): *vykoná simuláciu 1 životného cyklu populácie*
- fit(self, X, y): *vykoná simuláciu genetického algoritmu*
- plot_scores(self): *zobrazí postup na vyhľadávaní optimálneho riešenia (fitness)*

Klasifikácia používateľov

Súbor: classification_functions.py

Dostupné metódy:

- get_EER(user_scores, imposter_scores): *na základe skóre pri klasifikácii používateľa a útočníkov vypočíta FAR, FRR, TAR, TRR a ERR skóre biometrického systému*

Príloha G: Opis jednotlivých častí overenia riešenia dostupných v nástroji Jupyter Notebook

Umiestnenie: source codes/dpLockJupiterNotebook

V tejto prílohe uvádzame opis jednotlivých časti vypracovaného Jupyter Notebook-u, v rámci ktorého sme vykonali experimentovanie a overenie navrhnutého riešenia. Pre spustenie pripravených skriptov je potrebná inštalácia rozhrania Jupyter Notebook[7] a všetkých potrebných knižníc uvedených vo vrchnej časti skriptov (časť *imports*).

Klasifikácia kontextu odomykania

Umiestnenie: source codes/dpLockJupiterNotebook/Context classification

- 00 export db to df: *export dát z databázy pre účely ďalšieho spracovania*
- 01 preprocessing: *predspracovanie dát a dopočítanie dodatočných charakteristík*
- 02 outlier detection: *identifikácia outlierov a vyváženie jednotlivých tried pre výber dominantných charakteristík a klasifikáciu*
- 03 feature selection: *vymazanie korelovaných charakteristík a výber dominantných množín charakteristík*
- data: *výstupné dáta z jednotlivých krokov budovania modelu pre určovanie kontextu odomykania*
- feature_sets: *množiny dostupných charakteristík (všetky + vypočítané minimálne množiny)*
- results: *výsledky jednotlivých krokov budovania modelu kontextu odomykania*

Klasifikácia používateľa

Umiestnenie: source codes/dpLockJupiterNotebook/User classification

- data exploration: *prvotná vizualizácia získaných dát*
- 00 export db to df: *export dát z databázy pre účely ďalšieho spracovania*
- 01 preprocessing: *predspracovanie dát a dopočítanie dodatočných charakteristík*
- 02 outlier detection: *identifikácia outlierov a vyváženie jednotlivých tried pre výber dominantných charakteristík a klasifikáciu*

[7] Inštalácia a samotný postup inštalácie je dostupný online na https://jupyter.org/install

- 03 feature selection: *vymazanie korelovaných charakteristík a výber dominantných množín charakteristík*
- 04 classification: *klasifikácia používateľa a určovanie úspešnosti biometrického systému*
- data: *výstupné dáta z jednotlivých krokov budovania biometrického modelu používateľa*
- feature_sets: *množiny dostupných charakteristík (všetky + vypočítané minimálne množiny)*
- results: *výsledky jednotlivých krokov budovania modelov používateľov*
- *PI, PD search.ipynb: vyhľadávanie vzorovo závislých a nezávislých charakteristík*

Príloha H: Inštalačná príručka

Klientska Android aplikácia

Umiestnenie zdrojových kódov: source codes/dpLockAndroid

1) Pre zobrazenie a kompiláciu zdrojových kódov je potrebné mať nainštalované rozhranie Android Studio[8];
2) Zdrojové kódy nachádzajúce sa v tomto adresári je potrebné naimportovať do prostredia Android Studio;
    a. Vyberte *Súbor -> Nový -> Importovať projekt...*;
    b. Vyberte adresá projektu Eclipse ADT so súborom AndroidManifest.xml;
3) Projekt je naimportovaný a je možné ho skompilovať a spustiť.

Serverová časť aplikácie:

Umiestnenie zdrojových kódov: source codes/dpLockApi

1) Pre spustenie serverovej časti aplikácie je potrebné mať nainštalovanú MongoDB databázu a knižnicu NodeJs;
2) Po nainštalovaní MongoDB databázy je potrebné spustiť databázového klienta (pomocou príkazu mongod);
3) Po nainštalovaní NodeJs knižnice je potrebné stiahnuť a nainštalovať knižnice používané v NodeJS aplikácii (pomocou príkazu *npm install*);
4) Po nainštalovaní NodeJs knižníc a spustení MongoDb databázy je možné spustiť lokálny server (po spustení servera sa zobrazí URL adresa, na ktorej aktuálne spustený server beží);
5) Po spustení server je možné sa naň dopytovať pomocou REST Api volaní uvedených v Príloha D: Rozpis serverových API.

Nahratie lokálnych dát do databázy:

Umiestnenie zdrojových kódov: source codes/dpLockJupyterNotebook/Unlock uploading

1) Z umiestnenia, v ktorom sa nachádzajú zozbierané biometrické dáta od používateľov je pre nahratie týchto dát do databázy potrebné spustenie nasledujúceho Python skriptu: *user_unlocks_uploader.py*;

[8] Inštalačný súbor a postup inštalácie sa nachádza na oficiálnej stránke vydavateľa programu Android Studio: https://developer.android.com/studio/install

2) Priamo v tomto skripte je možne nastaviť, dáta ktorého používateľa a do ktorej databázy chceme nahrať;
3) Podmienkou pre úspešné nahratie používateľských dát je spustená MongoDB databáza.
4) Po úspešnom nahratí používateľských dát bude možné vykonať predspracovanie používateľských dát priamo v Jupyter Notebook-u pomocou priložených skriptov.
5) V prípade, že nie je potrebné nahratie lokálnych súborov s dátami používateľov, tak je možné používať Jupyter Notebook skripty pomocou už predspracovaných dát uložených v zložke *data* príslušného notebook-u.

Príloha I: Experiment 1

Typ experimentu: riadený experiment

Očakávaný počet vzoriek od každého účastníka: 80

Kroky experimentu

1. Účastníka posadíme na stoličku mimo stola, aby nemal ruky opreté o žiaden predmet.
2. Účastník sa zaregistruje do aplikácie (v prípade, že nemá ešte vytvorený účet). Ak už účastník zaregistrovaný je, môže pokračovať na krok 3.
3. Účastníkovi sú postupne ukázané odomykacie vzory, ktoré bude do zariadenia zadávať (podľa Tab. 11 Odomykacie vzory a spôsob odomykania). V aplikácii spustí zadávanie vzorov, vyberie kontext, v ktorom sa práve nachádza a prejde na zadanie referenčného vzoru v kroku 4.
4. Najprv účastník zadá odomykací vzor podľa predlohy do aplikácie, aby aplikácia vedela rozpoznať správne zadanie odomykacieho vzoru.
5. Následne účastník do aplikácie niekoľko-krát (podľa aplikácie, v tomto experimente nastavené na 20 opakovaní pre každý vzor) zadáva odomykacie vzory podľa zadanej predlohy (všetky pokusy sú zaznamenávané).
6. Po ukončení zadávania vzoru prejde účastník na krok 3 až kým nie sú zaznamenané všetky vzory experimentu.

Odomykacie vzory a spôsob odomykania

Tab. 11 Odomykacie vzory a spôsob odomykania

#	Vzor	Kontext		
		Poloha	**Ruka**	**Prst**
1	3x3 EASY (2103458)	*Sed (sitting)*	*Pravá (right)*	*Ukazovák (pointer)*
2	3x3 EASY (2103458)	*Sed (sitting)*	*Pravá (right)*	*Palec (thumb)*
3	3x3 HARD (124678530)	*Sed (sitting)*	*Pravá (right)*	*Ukazovák (pointer)*
4	3x3 HARD (124678530)	*Sed (sitting)*	*Pravá (right)*	*Palec (thumb)*

Príloha J: Experiment 2

Typ experimentu: neriadený + riadený experiment (začiatok a koniec experimentu)
Trvanie experimentu pre 1 účastníka: 7 dní (min 5)
Očakávaný počet vzoriek od každého účastníka: min 150

Princípom tohto experimentu bolo získanie biometrických údajov od používateľov v širšom časovom období a v prirodzenom prostredí používateľov. Dlhodobým odomykaním zariadenia dosiahneme, aby sa používateľ daný vzor prirodzene naučil a používal ho ako vlastný.

Súčasťou experimentu je aj získavanie vzorov, ktoré sú podobné alebo odlišné ako vzor, ktorý sa účastník naučí počas trvania experimentu (tieto vzory získame od účastníka pri ukončení experimentu).

POZNÁMKA:
Pre úplnosť experimentu je potrebné vykonať všetky kroky uvedené v častiach A, B a C (opísané v nižšie).

Podmienky zadávania vzoru riadene a neriadene (doma)

- účastník sedí pri zadávaní vzoru mimo stola, ruky nemá opreté o žiadny predmet
- účastník zadáva odomykacie vzory v kľudovom stave (nie v dopravnom prostriedku, pri chôdzi a podobne – podľa nastaveného spôsobu odomykania)
- účastník zadáva odomykacie vzory pravidelne (min. 1x za dva dni)
- účastník zadá počas experimentu aspoň 90 vzorov

A: Získanie vstupných dát

1. Účastníka posadíme na stoličku a vysvetlíme mu princíp experimentu a podmienky zadávania vzorov doma.
2. Účastník sa zaregistruje do aplikácie (v prípade, že nemá ešte vytvorený účet). Ak už účastník zaregistrovaný je, môže pokračovať na krok 3.
3. Zaregistrujeme pre účastníka experiment (podľa odomykacieho vzoru a spôsobu odomykania pre *#1* v tabuľke Tab. 11 Odomykacie vzory a spôsob odomykania).
4. Účastník zadá 15x odomykací vzor nastavený v experimente.

B: Dlhodobý experiment (domáce podmienky)

1. Účastník si berie pridelené zariadenie domov.
2. Účastník sa pred začatím experimentu doma prihlási do aplikácie a zobrazí si prebiehajúci experiment (informácie o experimente, kontexte odomykania a vzore).
3. Účastník v aplikácii spustí zadávanie vzorov a niekoľko-krát (podľa aplikácie, v tomto experimente nastavené na 15 opakovaní pre 1 sekvenciu) zadáva odomykacie vzory podľa zadanej predlohy (všetky pokusy sú zaznamenávané) bez prerušenia.
4. Po ukončení zadávania vzoru môže účastník pokračovať v odomykaní (ďalšia séria, krok 3) alebo zadávanie vzorov ukončí.
5. Tento postup opakuje účastník po celú dobu experimentu.

C: Získanie dát pre podobný a nepodobný vzor

1. Účastník posadíme na stoličku a vysvetlíme mu princíp ukončenia experimentu.
2. Účastník vykoná zadávanie vzorov *#2* a *#3* z tabuľky Tab. 11 Odomykacie vzory a spôsob odomykania klasickým spôsobom (podľa časti B).

Odomykacie vzory a spôsob odomykania

Tab. 12 Odomykacie vzory a spôsob odomykania

#	Vzor	Kontext		
		Poloha	**Ruka**	**Prst**
1	3x3 – 124678530	*Sed (sitting)*	*Dominantná (right/left)*	*Palec (thumb)*
2	3x3 – 01246785 (podobný so vzorom 1)	*Sed (sitting)*	*Dominantná (right/left)*	*Palec (thumb)*
3	3x3 – 6785243 (nepodobný so vzorom 1)	*Sed (sitting)*	*Dominantná (right/left)*	*Palec (thumb)*

Výsledkom tohto experimentu sú dlhodobo zaznamenávané dáta od používateľov pre 1 odomykací vzor a dáta pre 2 ďalšie odomykacie vzory (1 podobný, 1 nepodobný).

Príloha K: Scenáre pri klasifikácii používateľov – EXP1

SC1 - Jednoduchý vzor (EASY)

Výsledky: priečinok *experiments/experiment 1/evaluation/SC1*

Postup overenia:

1. predspracovanie dát
2. vyhľadanie a vymazanie outlierov pomocou Z-skóre
3. výber biometrických charakteristík
4. klasifikácia prsta
    a. pomocou 3 setov signifikantných charakteristík (30 najvýznamnejších)
5. klasifikácia používateľov
    a. pomocou 3 setov signifikantných charakteristík (30 najvýznamnejších)
    b. s aj bez využitia detekcie prsta

SC2 - Jednoduchý vzor (EASY)

Výsledky: priečinok *experiments/experiment 1/evaluation/SC2*

Postup overenia:

1. predspracovanie dát
2. vyhľadanie a vymazanie outlierov pomocou IQR
3. výber biometrických charakteristík
4. klasifikácia prsta
    a. pomocou 3 setov signifikantných charakteristík (30 najvýznamnejších)
5. klasifikácia používateľov
    a. pomocou 3 setov signifikantných charakteristík (30 najvýznamnejších)
    b. s aj bez využitia detekcie prsta

SC3 – Zložitý vzor (HARD)

Výsledky: priečinok *experiments/experiment 1/evaluation/SC3*

Postup overenia:

1. predspracovanie dát
2. vyhľadanie a vymazanie outlierov pomocou Z-skóre
3. výber biometrických charakteristík
4. klasifikácia prsta
    a. pomocou 3 setov signifikantných charakteristík (30 najvýznamnejších)

5. klasifikácia používateľov
    a. pomocou 3 setov signifikantných charakteristík (30 najvýznamnejších)
    b. s aj bez využitia detekcie prsta

SC4 – Zložitý vzor (HARD)

Výsledky: priečinok *experiments/experiment 1/evaluation/SC4*

Postup overenia:

1. predspracovanie dát
2. vyhľadanie a vymazanie outlierov pomocou IQR
3. výber biometrických charakteristík
4. klasifikácia prsta
    a. pomocou 3 setov signifikantných charakteristík (30 najvýznamnejších)
5. klasifikácia používateľov
    a. pomocou 3 setov signifikantných charakteristík (30 najvýznamnejších)
    b. s aj bez využitia detekcie prsta

Príloha L: Výsledky autentifikácie – EXP1 prvotný experiment

V tejto prílohe sa nachádza zhodnotenie úspešnosti autentifikácie pomocou kombinácie rôznych algoritmov výberu biometrických charakteristík a následnej „Single-Class“ klasifikácie pomocou SVM klasifikátora (pre rôzne typy jadier (angl. Kernel)) v prvotných experimentoch.

Výsledky uvádzané v tejto prílohe sú pôvodné výsledky, ktoré sa nám podarilo dosiahnuť pri použití základných metód pre výber signifikantných charakteristík a nepredstavujú finálnu úspešnosť navrhnutého systému.

Použité sety charakteristík (rozdelené na základe spôsobu určenia signifikantnosti):

A. k-best,
B. logistická regresia,
C. extra tree.

SC1 - Jednoduchý vzor (EASY)

Odstránenie outlierov z dát: prvých 5 + Z-score

Výsledky: priečinok *evaluation/SC1*

Set	Typ jadra	Rozlišovanie prsta	FAR	FRR	Priemerné EER
A	rbf	N	0.00000	1.00000	0.56991
		A	0.00000	1.00000	0.60374
	sigmoid	N	0.01434	0.83902	0.22383
		A	0.00321	0.88785	0.19458
	poly	N	0.01434	0.83902	0.22383
		A	0.00321	0.88785	0.19458
B	rbf	N	0.00000	1.00000	0.79732
		A	0.00000	1.00000	0.69030
	sigmoid	N	0.00892	0.94146	0.62770
		A	0.00050	0.95794	0.39488
	poly	N	0.00892	0.94146	0.62770
		A	0.00050	0.95794	0.39488
C	rbf	N	0.06888	0.94146	0.82014

		A	0.00000	1.00000	0.58122
	sigmoid	N	0.02983	0.84878	0.54048
		A	0.02038	0.87850	0.39625
	poly	N	0.02983	0.84878	0.54048
		A	0.02038	0.87850	0.39625

SC2 - Jednoduchý vzor (EASY)

Odstránenie outlierov z dát: prvých 5 + IQR

Výsledky: priečinok *evaluation/SC2*

Set	Typ jadra	Rozlišovanie prsta	FAR	FRR	Priemerné EER
A	rbf	N	0.00000	1.00000	0.64210
		A	0.00000	1.00000	0.64328
	sigmoid	N	0.00197	0.85135	0.22069
		A	0.00111	0.92405	0.20840
	poly	N	0.00197	0.85135	0.22069
		A	0. 00111	0.92405	0.20840
B	rbf	N	0.00000	1.00000	0.79766
		A	0.00000	1.00000	0.65693
	sigmoid	N	0.00000	0.95270	0.44919
		A	0.00076	0.98734	0.40338
	poly	N	0.00000	0.95270	0.44919
		A	0.00076	0.98734	0.40338
C	rbf	N	0.00000	1.00000	0.81094
		A	0.00000	1.00000	0.59588
	sigmoid	N	0.03376	0.83784	0.41788
		A	0.01428	0.94936	0.37688
	poly	N	0.03376	0.83784	0.41788
		A	0.01428	0.94936	0.37688

SC3 – Zložitý vzor (HARD)

Odstránenie outlierov z dát: prvých 5 + Z-score

Výsledky: priečinok *evaluation/SC3*

Set	Typ jadra	Rozlišovanie prsta	FAR	FRR	Priemerné EER
A	rbf	N	0.00000	1.00000	0.63251
		A	0.00000	1.00000	0.57434
	sigmoid	N	0.00128	0.92788	0.21217
		A	0.00117	0.88837	0.17032
	poly	N	0.00128	0.92788	0.21217
		A	0.00117	0.88837	0.17032
B	rbf	N	0.00000	1.00000	0.83893
		A	0.00000	1.00000	0.67927
	sigmoid	N	0.00122	0.94230	0.64415
		A	0.00058	0.99069	0.46766
	poly	N	0.00122	0.94230	0.64415
		A	0.00058	0.99069	0.46766
C	rbf	N	0.00000	1.00000	0.87011
		A	0.00000	1.00000	0.57122
	sigmoid	N	0.00574	0.90865	0.54537
		A	0.00348	0.93488	0.25212
	poly	N	0.00574	0.90865	0.54537
		A	0.00348	0.93488	0.25212

SC4 – Zložitý vzor (HARD)

Odstránenie outlierov z dát: prvých 5 + IQR

Výsledky: priečinok *evaluation/SC4*

Set	Typ jadra	Rozlišovanie prsta	FAR	FRR	Priemerné EER
A	rbf	N	0.00000	1.00000	0.57437
		A	0.00000	1.00000	0.58017
	sigmoid	N	0.00516	0.85256	0.19459
		A	0.00145	0.86747	0.14673
	poly	N	0.00516	0.85256	0.19459
		A	0.00145	0.86747	0.14673
B	rbf	N	0.00000	1.00000	0.82853
		A	0.00000	1.00000	0.71466
	sigmoid	N	0.00264	0.89743	0.52125
		A	0.00053	0.98795	0.41541
	poly	N	0.00264	0.89743	0.52125
		A	0.00053	0.98795	0.41541
C	rbf	N	0.00000	1.00000	0.83121
		A	0.00000	1.00000	0.62621
	sigmoid	N	0.00880	0.86538	0.42690
		A	0.00278	0.91566	0.31545
	poly	N	0.00880	0.86538	0.42690
		A	0.00278	0.91566	0.31545

Príloha M: Výsledky autentifikácie – EXP2

V tejto prílohe sa nachádza zhodnotenie úspešnosti autentifikácie pomocou kombinácie rôznych algoritmov výberu biometrických charakteristík a následnej „Single-Class“ klasifikácie pomocou SVM klasifikátora (pre rôzne typy jadier (angl. Kernel)) v navrhnutom procese autentifikácie používateľov.

Výsledky uvádzané v tejto prílohe sú finálne výsledky, ktoré sa nám podarilo dosiahnuť pri použití pokročilejších metód pre výber signifikantných charakteristík a predstavujú finálnu (najvyššiu dosiahnutú) úspešnosť navrhnutého systému.

Tab. 13 Výsledky autentifikácie používateľa využitím viacerých metód v procese návrhu systému

Metóda	Vyhľadanie outlierov	Metóda odstránenia korelovaných charakteristík	Počet dekorelovaných charakteristík	Metóda určenie skóre charakteristík	Metóda minimalizácie počtu charakteristík	Optimálny počet charakteristík	Typ jadra SVM klasifikátora	FAR	FRR	EER
7	iqr	korelačná matica	176	extra-tree	GNB	136	sigmoid	0,2182	0,2890	0,0572
31	z_score	korelačná matica	178	extra-tree	GNB	134	sigmoid	0,2284	0,2873	0,0592
29	z_score	korelačná matica	178	k-best	LDA	171	sigmoid	0,2136	0,2813	0,0595
25	z_score	korelačná matica	178	k-best	GNB	177	sigmoid	0,2119	0,2852	0,0600
11	iqr	korelačná matica	176	extra-tree	LDA	163	sigmoid	0,2243	0,2886	0,0611
35	z_score	korelačná matica	178	extra-tree	LDA	177	sigmoid	0,2138	0,2826	0,0639
1	iqr	korelačná matica	176	k-best	GNB	167	sigmoid	0,2271	0,2801	0,0642
5	iqr	korelačná matica	176	k-best	LDA	167	sigmoid	0,2317	0,2819	0,0645

32	z_score	korelačná matica	178	extra-tree	decision_tree	46	rbf	0,1759	0,3140	0,0754
8	iqr	korelačná matica	176	extra-tree	decision_tree	43	rbf	0,1808	0,3098	0,0772
3	iqr	korelačná matica	176	k-best	decision_tree	116	sigmoid	0,2373	0,2631	0,0781
43	z_score	vif	82	extra-tree	GNB	64	sigmoid	0,2226	0,2739	0,0850
27	z_score	korelačná matica	178	k-best	decision_tree	118	sigmoid	0,2462	0,2738	0,0856
9	iqr	korelačná matica	176	extra-tree	decision_tree	43	sigmoid	0,2439	0,2763	0,0875
33	z_score	korelačná matica	178	extra-tree	decision_tree	46	sigmoid	0,2514	0,2760	0,0898
19	iqr	vif	86	extra-tree	GNB	67	sigmoid	0,2321	0,2664	0,0924
23	iqr	vif	86	extra-tree	LDA	84	sigmoid	0,2333	0,2562	0,0927
37	z_score	vif	82	k-best	GNB	81	sigmoid	0,2419	0,2689	0,1006
17	iqr	vif	86	k-best	LDA	85	sigmoid	0,2330	0,2575	0,1012
13	iqr	vif	86	k-best	GNB	85	sigmoid	0,2379	0,2576	0,1027
47	z_score	vif	82	extra-tree	LDA	79	sigmoid	0,2444	0,2685	0,1047
41	z_score	vif	82	k-best	LDA	81	sigmoid	0,2448	0,2645	0,1060
30	z_score	korelačná matica	178	extra-tree	GNB	134	rbf	0,1841	0,3169	0,1069
44	z_score	vif	82	extra-tree	decision_tree	20	rbf	0,1994	0,2853	0,1070
20	iqr	vif	86	extra-tree	decision_tree	37	rbf	0,1938	0,3043	0,1093
6	iqr	korelačná matica	176	extra-tree	GNB	136	rbf	0,1829	0,3229	0,1095
21	iqr	vif	86	extra-tree	decision_tree	37	sigmoid	0,2442	0,2764	0,1098
26	z_score	korelačná matica	178	k-best	decision_tree	118	rbf	0,1914	0,3076	0,1158

10	iqr	korelačná matica	176	extra-tree	LDA	163	rbf	0,1888	0,3186	0,1172
39	z_score	vif	82	k-best	decision_tree	65	sigmoid	0,2489	0,2740	0,1190
2	iqr	korelačná matica	176	k-best	decision_tree	116	rbf	0,1938	0,3044	0,1207
34	z_score	korelačná matica	178	extra-tree	LDA	177	rbf	0,1950	0,3186	0,1239
4	iqr	korelačná matica	176	k-best	LDA	167	rbf	0,1959	0,3179	0,1242
0	iqr	korelačná matica	176	k-best	GNB	167	rbf	0,1927	0,3193	0,1244
28	z_score	korelačná matica	178	k-best	LDA	171	rbf	0,1937	0,3165	0,1251
15	iqr	vif	86	k-best	decision_tree	52	sigmoid	0,2565	0,2703	0,1271
24	z_score	korelačná matica	178	k-best	GNB	177	rbf	0,1989	0,3169	0,1303
18	iqr	vif	86	extra-tree	GNB	67	rbf	0,2186	0,3046	0,1430
14	iqr	vif	86	k-best	decision_tree	52	rbf	0,2213	0,2881	0,1457
38	z_score	vif	82	k-best	decision_tree	65	rbf	0,2237	0,2954	0,1468
45	z_score	vif	82	extra-tree	decision_tree	20	sigmoid	0,2970	0,2855	0,1496
42	z_score	vif	82	extra-tree	GNB	64	rbf	0,2183	0,3039	0,1527
46	z_score	vif	82	extra-tree	LDA	79	rbf	0,2324	0,3125	0,1628
22	iqr	vif	86	extra-tree	LDA	84	rbf	0,2403	0,3094	0,1681
16	iqr	vif	86	k-best	LDA	85	rbf	0,2325	0,3054	0,1682
12	iqr	vif	86	k-best	GNB	85	rbf	0,2373	0,3069	0,1691
36	z_score	vif	82	k-best	GNB	81	rbf	0,2426	0,3068	0,1720
40	z_score	vif	82	k-best	LDA	81	rbf	0,2411	0,3068	0,1730

Príloha N: Plán práce na riešení DP1

Táto príloha obsahuje zhrnutie plánu práce, podľa ktorého sme postupovali pri práci na našej diplomovej práci časti DP1 v akademickom roku 2017/2018.

Ako sme už spomínali v časti 3 Ciele práce a výskumné hypotézy, výsledkom tejto diplomovej práce má byť vytvorenie biometrického systému na autentifikáciu používateľov na mobilných zariadeniach. Rozpis jednotlivých naplánovaných úloh spolu s postupom ich plnenia rozdelených do jednotlivých týždňov semestra je uvedený v nasledujúcej tabuľke (Tab. 15 Plán rozdelenia práce pri riešení DP2 spolu s vyjadrením k jeho plneniu).

Tab. 14 Plán rozdelenia práce pri riešení DP1 spolu s vyjadrením k jeho plneniu

Týždeň semestra	**Naplánované úlohy**	**Vyjadrenie k splneniu úlohy**
1.	Zapracovanie pripomienok a návrhov vedúceho práce do časti analýzy, špecifikácia požiadaviek vytváraného biometrického systému.	Doplnené pripomienky vedúceho práce a vytvorená špecifikácia požiadaviek vytváraného systému, vytvorenie UML diagramov.
2.	Implementácia prototypu klientskej časti (evolučný prototyp), skúmanie problematiky biometrických systémov.	Implementácia prototypu Android aplikácie v nástroji Android Studio, zadefinovanie grafických rozhraní, vytvorenie základnej logiky programu, integrácia odomykacieho vzoru do aplikácie.
3.	Implementácia prototypu serverovej časti, skúmanie problematiky biometrických systémov.	Výber implementačných prostredí a jazykov, v ktorých bude implementovaný biometrický systém. Prototypovanie klientskej časti v rámcoch ReactNative, Angular a jazyku Kotlin.
4.	Návrh a implementácia získavania biometrických charakteristík.	Implementácia sledovania a ukladania udalostí odomykania zariadenia (dotyk, akcelerácia, naklonenie) v zariadení Android.

5.	Integrácia klientskej a serverovej časti.	Integrácia serverových API v klientskej časti Android aplikácie na ukladanie biometrických vzoriek používateľov.
6.	Prezentovanie dosiahnutých výsledkov a zapracovanie pripomienok.	Prezentácia výsledkov vedúcemu diplomovej práce a zapracovanie pripomienok k vytvorenému systému.
7.	Integrácia predspracovania získaných surových dát zo senzorov.	Integrácia spracovávania dát zo senzorov do zmysluplných metrík a vyriešenie zaznamenávania času v rovnakých jednotkách pri zaznamenaných udalostiach.
8.	Prvé experimenty a overenie správnosti získaných biometrických údajov.	Vykonávanie experimentov pre overenie zaznamenávania biometrických charakteristík.
9.	Zhodnotenie prvotných experimentov.	Zhodnotenie prvotných experimentov.
10.	Finalizácia DP1.	Písanie diplomovej práce, finalizácia časti DP1.
11.	Prezentovanie diplomovej práce, zapracovanie pripomienok, finalizácia časti DP1 diplomovej práce.	Prezentovanie diplomovej práce, zapracovanie pripomienok, finalizácia časti DP1diplomovej práce.
12.	Odovzdanie časti DP1 diplomovej práce.	Odovzdanie časti DP1 diplomovej práce.

Príloha O: Plán práce na riešení DP2

Táto príloha obsahuje zhrnutie plánu práce, podľa ktorého sme postupovali pri práci na našej diplomovej práci časti DP2 v akademickom roku 2018/2019.

Ako sme už spomínali v časti 3 Ciele práce a výskumné hypotézy, výsledkom našej diplomovej práce má byť vytvorenie biometrického systému na autentifikáciu používateľov na mobilných zariadeniach. Rozpis jednotlivých naplánovaných úloh spolu s postupom ich plnenia rozdelených do jednotlivých týždňov semestra je uvedený v nasledujúcej tabuľke (Tab. 15 Plán rozdelenia práce pri riešení DP2 spolu s vyjadrením k jeho plneniu).

Tab. 15 Plán rozdelenia práce pri riešení DP2 spolu s vyjadrením k jeho plneniu

Týždeň semestra	**Naplánované úlohy**	**Vyjadrenie k splneniu úlohy**
1.	Zapracovanie pripomienok a návrhov vedúceho práce na základe DP1.	Doplnené pripomienky vedúceho práce a vytvorená špecifikácia požiadaviek vytváraného systému, dopracovanie UML diagramov.
2.	Návrh procesov registrácie, zaznamenávania a aktualizácie biometrického používateľského modelu.	Navrhnuté procesy pre registráciu a zaznamenávanie biometrického modelu používateľa. Proces aktualizácie biometrického modelu bude navrhnutý neskôr.
3.	Získavanie prvých reálnych dát od používateľov.	Získané dáta o používateľov (ľudia z okolia, 5 používateľov)
4.	Experimenty so získanými dátami (prvé klasifikácie).	Prvé klasifikácie pre určenie spôsobu odomknutia.
5.	Experimenty so získanými dátami	Experimenty s výberom vhodných biometrických charakteristík.
6.	Návrh a implementácia informačnej fúzie na úrovni porovnávacieho skóre.	Navrhnutá metóda „ensemble“ metóda s 2 úrovňami.
7.	Prezentovanie dosiahnutých výsledkov	Prezentácia výsledkov vedúcemu diplomovej práce a zapracovanie

	a zapracovanie pripomienok.	pripomienok k vytvorenému systému.
8.	Zbieranie ďalších biometrických dát (experimenty).	Zbieranie dát a experimentovanie (feature selection, spektrálna analýza, Single-Class klasifikácia)
9.	Pilotné overovanie o hodnotenie hypotéz, písanie diplomovej práce a vyhodnocovanie experimentov, zhodnotenie dosiahnutých výsledkov.	Experimentovanie so získanými dátami.
10.	Finalizácia časti DP2 diplomovej práce, návrhy na pokračovanie v práci.	Písanie diplomovej práce, finalizácia časti DP2.
11.	Prezentovanie diplomovej práce, zapracovanie pripomienok, finalizácia časti DP2 diplomovej práce.	Prezentovanie diplomovej práce, zapracovanie pripomienok, finalizácia časti DP2diplomovej práce.
12.	Odovzdanie časti DP2 diplomovej práce.	Odovzdanie časti DP2 diplomovej práce.

Príloha P: Plán práce na riešení DP3

V rámci plánovania práce na tejto diplomovej práci sme vytvorili plán úloh, ktoré budú viesť k ďalšiemu riešeniu skúmanej problematiky, návrhu a vytvoreniu biometrického systému na autentifikáciu používateľov. Plán riešenia projektu finálnej časti DP3 našej diplomovej práce spolu s vyjadrením k splneniu jednotlivých úloh uvádzame v Tab. 16 Plán rozdelenia práce pri riešení DP3.

Tab. 16 Plán rozdelenia práce pri riešení DP3

Týždeň semestra	**Naplánované úlohy**	**Vyjadrenie k splneniu úlohy**
1.	Zapracovanie pripomienok a návrhov vedúceho práce na základe DP2.	Doplnené pripomienky vedúceho práce
2.	Návrh procesov aktualizácie biometrického používateľského modelu.	Úprava aplikácie pre logovanie dát (pre dlhodobý experiment, nové zariadenia). Príprava experimentu pre dlhodobé získavanie dát.
3.	Získavanie dlhodobých dát od používateľov.	Táto etapa trvala viacero týždňov semestra. Dopracovanie procesov pre autentifikáciu používateľa.
4.	Experimenty so získanými dátami (klasifikácie, sledovanie zlepšovania klasifikátora).	Overenie správnosti získaných dát, pokračovanie v experimentoch. Príprava programových kódov pre evaluáciu výsledkov.
5.	Návrh a implementácia informačnej fúzie na úrovni vlastností.	Implementácia fúzie na úrovni porovnávacieho skóre. Implementácia genetického algoritmu pre výber množiny sledovaných charakteristík. Experimenty s minimalizáciou počtu charakteristík.
6.	Prezentovanie dosiahnutých výsledkov a zapracovanie pripomienok.	Prezentovanie výsledkov pri autentifikácii používateľov, hľadanie ďalších ľudí pre zapojenie sa do experimentu. Oprava chýb v klasifikačných metódach/algoritmoch.
7.	Overovanie a hodnotenie hypotéz, vyhodnocovanie	Vyhodnocovanie dát, úprava algoritmov.

	experimentov.	
8.	Overovanie a hodnotenie hypotéz, písanie diplomovej práce a vyhodnocovanie experimentov.	Vyhodnocovanie experimentov, overovanie hypotéz. Čistenie dát. Doplnenie vzorovo závislých charakteristík. Transformácia dát pre Jupyter Notebook. Prepis Python skriptov do Jupyter Notebooku.
9.	Overovanie a hodnotenie hypotéz, písanie diplomovej práce a vyhodnocovanie experimentov, zhodnotenie dosiahnutých výsledkov.	Ďalšie zbieranie dát a experimentovanie (feature selection, spektrálna analýza, Single-Class klasifikácia). Overovanie hypotéz, simulácia viacerých spôsobov predspracovania dát, výberu dominantných charakteristík a klasifikácie.
10.	Finalizácia časti DP3 diplomovej práce, návrhy na pokračovanie v práci.	Hľadanie možných vylepšení výsledkov autentifikácie. Návrh a implementácia procesu pre minimalizáciu počtu sledovaných charakteristík. Optimalizácia výpočtu.
11.	Prezentovanie diplomovej práce, zapracovanie pripomienok, finalizácia časti DP3 diplomovej práce.	Finalizácia výsledkov, hodnotenie hypotéz. Prezentácia výsledkov vedúcej diplomovej práce a zapracovanie pripomienok.
12.	Odovzdanie časti DP3 diplomovej práce.	Odovzdanie časti DP3 diplomovej práce.

Príloha Q: Opis digitálnej časti práce

Evidenčné číslo práce v informačnom systéme: FIIT-182905-74357

Obsah digitálnej časti práce (archív ZIP):

Priečinok	Obsah
doc	***Dokumentácia***
DP3_74357_VNENCAK.docx	*Diplomová práca*
DP3_74357_VNENCAK.pdf	*Diplomová práca*
ea model	***Model v EA***
dp.eap	*Návrh architektúry a procesov biometrického systému*
dp.eap	*Návrh architektúry a procesov biometrického systému*
source codes	***Zdrojové kódy***
dpLockApi	*BE časť aplikácie (NodeJS server, Databáza)*
dpLockAndroid	*FE časť aplikácie - Android Aplikácia*
dpLockJupyterNotebook	***Jupyter Notebook skripty s vytvorenými Python modulmi - použité v procese budovania a overovania biom. Systému***
User classification	*Postup a výsledky z budovania biometrického modelu používateľa*
Context classification	*Postup a výsledky z budovania biometrického modelu kontextu odomykania*
experiments	***Výsledky experimentov pre DP3***
experiment 1	*Dáta k prvotnému experimentu EXP1*
data	*Získané biometrické dáta z prvotného experimetu (dump MongoDB databázy)*
evaluation	***Evaluácia výsledkov***
SC1	***Výsledky evaluácie - Scenár 1, hľadané outliery: Z-Score***

unlock_actions_124678530_removed_outliers_result	*Výsledok odstránenia outlierov z dát vzoru 124678530*
unlock_actions_124678530_removed_outliers_by_user_result	*Počet vzoriek podľa typu odomknutia pre každého používateľa*
features_k_best	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti algoritmom k-best)*
features_extra_tree	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti algoritmom extra-tree)*
features_logistic_regression	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti logistickou regresiou)*
features_finger_k_best	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti algoritmom k-best)*
features_finger_extra_tree	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti algoritmom extra-tree)*
features_finger_logistic_regression	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti logistickou regresiou)*
user_finger_classification_per_user	*Výsledok klasifikácie spôsobu odomknutia - prstu (pre každého používateľa zvlášť)*
user_finger_classification_global	*Výsledok klasifikácie spôsobu odomknutia - prstu (pre všetkých používateľov spoločne)*
user_classification_results	*Výsledok klasifikácie používateľov pre rôzne algoritmy bez detekcie spôsobu odomknutia - prsta*
user_classification_determining_fingers_results	*Výsledok klasifikácie používateľov pre rôzne algoritmy s detekciou spôsobu odomknutia - prsta*
SC2	***Výsledky evaluácie - Scenár 2, hľadané outliery: IQR***
unlock_actions_124678530_removed_outliers_result	*Výsledok odstránenia outlierov z dát vzoru 124678530*
unlock_actions_124678530_removed_outliers_by_user_result	*Počet vzoriek podľa typu odomknutia pre každého používateľa*
features_k_best	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti algoritmom k-best)*
features_extra_tree	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti algoritmom extra-tree)*

features_logistic_regression	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti logistickou regresiou)*
features_finger_k_best	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti algoritmom k-best)*
features_finger_extra_tree	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti algoritmom extra-tree)*
features_finger_logistic_regression	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti logistickou regresiou)*
user_finger_classification_per_user	*Výsledok klasifikácie spôsobu odomknutia - prstu (pre každého používateľa zvlášť)*
user_finger_classification_global	*Výsledok klasifikácie spôsobu odomknutia - prstu (pre všetkých používateľov spoločne)*
user_classification_results	*Výsledok klasifikácie používateľov pre rôzne algoritmy bez detekcie spôsobu odomknutia - prsta*
user_classification_determining_fingers_results	*Výsledok klasifikácie používateľov pre rôzne algoritmy s detekciou spôsobu odomknutia - prsta*
SC3	***Výsledky evaluácie - Scenár 3, hľadané outliery: Z-Score***
unlock_actions_2103458_removed_outliers_result	*Výsledok odstránenia outlierov z dát vzoru 2103458*
unlock_actions_2103458_removed_outliers_by_user_result	*Počet vzoriek podľa typu odomknutia pre každého používateľa*
features_k_best	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti algoritmom k-best)*
features_extra_tree	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti algoritmom extra-tree)*
features_logistic_regression	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti logistickou regresiou)*
features_finger_k_best	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti algoritmom k-best)*
features_finger_extra_tree	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti algoritmom extra-tree)*

features_finger_logistic_regression	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti logistickou regresiou)*
user_finger_classification_per_user	*Výsledok klasifikácie spôsobu odomknutia - prstu (pre každého používateľa zvlášť)*
user_finger_classification_global	*Výsledok klasifikácie spôsobu odomknutia - prstu (pre všetkých používateľov spoločne)*
user_classification_results	*Výsledok klasifikácie používateľov pre rôzne algoritmy bez detekcie spôsobu odomknutia - prsta*
user_classification_determining_fingers_results	*Výsledok klasifikácie používateľov pre rôzne algoritmy s detekciou spôsobu odomknutia - prsta*
SC4	***Výsledky evaluácie - Scenár 4, hľadané outliery: IQR***
unlock_actions_2103458_removed_outliers_result	*Výsledok odstránenia outlierov z dát vzoru 2103458*
unlock_actions_2103458_removed_outliers_by_user_result	*Počet vzoriek podľa typu odomknutia pre každého používateľa*
features_k_best	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti algoritmom k-best)*
features_extra_tree	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti algoritmom extra-tree)*
features_logistic_regression	*Zoznam charakteristík na klasifikáciu používateľov (zoradené podľa významnosti logistickou regresiou)*
features_finger_k_best	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti algoritmom k-best)*
features_finger_extra_tree	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti algoritmom extra-tree)*
features_finger_logistic_regression	*Zoznam charakteristík na klasifikáciu typu odomknutia - prstu (zoradené podľa významnosti logistickou regresiou)*
user_finger_classification_per_user	*Výsledok klasifikácie spôsobu odomknutia - prstu (pre každého používateľa zvlášť)*
user_finger_classification_global	*Výsledok klasifikácie spôsobu odomknutia - prstu (pre všetkých používateľov spoločne)*

	user_classification_results	*Výsledok klasifikácie používateľov pre rôzne algoritmy bez detekcie spôsobu odomknutia - prsta*
	user_classification_determining_fingers_results	*Výsledok klasifikácie používateľov pre rôzne algoritmy s detekciou spôsobu odomknutia - prsta*
experiment 2		***Dáta k dlhodobému experimentu EXP2***
data		*Získané biometrické dáta (JSON súbory)*

Digitálna časť práce má veľkosť 0.728 GB.

Názov odovzdaného archívu: DP_prilohy_digital_stanislav_vnencak.zip