Kauno technologijos universitetas

Informatikos fakultetas

Adaptyvus identifikavimo ir autentifikavimo metodas neįgaliesiems

Baigiamasis magistro projektas

Projektą parengė

Paulius Eidimtas

Projektui vadovavo

Prof. Algimantas Venčkauskas

Kaunas, 2026

Kauno technologijos universitetas

Informatikos fakultetas

Adaptyvus identifikavimo ir autentifikavimo metodas neįgaliesiems

Baigiamasis magistro projektas

Informacijos ir informacinių technologijų sauga (6211BX008)

Projektą parengė
Paulius Eidimtas

Projektui vadovavo
Prof. Algimantas Venčkauskas

Projektą recenzavo
doc. Audronė Janavičiūtė

Kaunas, 2026

Kauno technologijos universitetas

Informatikos fakultetas

Paulius Eidimtas

Adaptyvus identifikavimo ir autentifikavimo metodas neįgaliesiems

Akademinio sąžiningumo deklaracija

Patvirtinu, kad:

1. baigiamąjį projektą parengiau savarankiškai ir sąžiningai, nepažeisdamas (-a) kitų asmenų autoriaus ar kitų teisių, laikydamasis (-i) Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo, Kauno technologijos universiteto (toliau – Universitetas) intelektinės nuosavybės valdymo ir perdavimo nuostatų bei Universiteto akademinės etikos kodekse nustatytų etikos reikalavimų;

2. visi baigiamajame projekte pateikti duomenys ir tyrimų rezultatai yra teisingi ir gauti teisėtai, nei viena projekto dalis nėra plagijuota nuo spausdintinių ar elektroninių šaltinių, o visos baigiamojo projekto tekste pateiktos citatos ir nuorodos yra nurodytos literatūros sąraše;

3. baigiamajame projekte tinkamai laikiausi asmens duomenų apsaugos reikalavimų, nenaudojau neskelbtinų ar konfidencialių duomenų be teisėto pagrindo, o jei juos naudojau, jie yra tinkamai nuasmeninti;

4. jei rengiant baigiamąjį projektą naudojausi dirbtinio intelekto (toliau – DI) ar kitais automatizuotais įrankiais, juos taikiau pagal Universitete nustatytą tvarką, nepažeisdamas (-a) akademinio sąžiningumo principų;

5. nesumokėjau ir nesu įsipareigojęs (-usi) mokėti jokių įstatymų nenumatytų piniginių sumų už baigiamąjį projektą ar jo dalis jokiam fiziniam ar juridiniam asmeniui;

6. suprantu, kad išaiškėjus akademinio nesąžiningumo ar kitų asmenų teisių pažeidimo faktui, man bus taikoma atsakomybė pagal Universitete nustatytą tvarką ir galiu būti pašalintas (-a) iš Universiteto; akademinio nesąžiningumo atvejis gali būti nagrinėjamas ir po studijų baigimo, inicijuojant kvalifikacinio laipsnio atšaukimo procedūrą.

Paulius Eidimtas. Adaptyvus identifikavimo ir autentifikavimo metodas neįgaliesiems. Magistro baigiamasis projektas / projektui vadovavo Prof. Algimantas Venčkauskas; Kauno technologijos universitetas, Informatikos fakultetas fakultetas.

Studijų kryptis ir studijų krypčių grupė: Informatikos mokslai, Informacijos ir informacinių technologijų sauga.

Reikšminiai žodžiai: Adaptyvus autentifikavimas, asmenys su negalia, daugiametodis autentifikavimas, kontekstinis vertinimas.

Kaunas, 2026. 74 p.

Santrauka

Darbe nagrinėjama prieinamo autentifikavimo problema asmenims su negalia ir pristatomas siūlomas adaptyvus identifikavimo ir autentifikavimo metodas, skirtas pagerinti naudojimosi skaitmeninėmis paslaugomis prieinamumą. Temos aktualumą lemia tai, kad tradiciniai autentifikavimo metodai, tokie kaip tekstiniai slaptažodžiai, PIN kodai ar tikslia įvestimi grindžiami veiksmai, ne visada yra vienodai tinkami naudotojams, turintiems regos, motorikos ar teksto apdorojimo sunkumų. Dėl to autentifikavimo sprendimai turi būti vertinami ne tik saugumo, bet ir praktinio prieinamumo, naudojimo lankstumo bei atsarginių autentifikavimo būdų požiūriu.

Darbo tikslas – sukurti saugų ir naudotojui draugišką adaptyvų autentifikavimo modelį, orientuotą į didesnį prieinamumą asmenims su negalia. Tikslui pasiekti buvo analizuotos tradicinių autentifikavimo metodų keliamos problemos, nagrinėtos esamos biometrinio, daugiametodžio ir adaptyvaus autentifikavimo sprendimų kryptys, suformuoti siūlomo modelio reikalavimai, sukurtas jo koncepcinis modelis ir realizuotas prototipas, apimantis balso, gestais pagrįstą lytėjimo, biometrinį ir vienkartinio slaptažodžio autentifikavimą. Taip pat atliktas siūlomo modelio kokybinis palyginimas su analizuotomis autentifikavimo sprendimų kryptimis ir eksperimentinis vertinimas.

Pirmojoje darbo dalyje analizuojami autentifikavimo iššūkiai, kylantys skirtingoms naudotojų grupėms ir nagrinėjamos esamos autentifikavimo sprendimų kryptys. Remiantis atlikta analize nustatyta, kad vienas autentifikavimo metodas negali būti laikomas universaliu sprendimu visiems naudotojams, todėl prieinamas autentifikavimas turi derinti kelis metodus, prisitaikymą prie konteksto ir atsarginius autentifikavimo kelius.

Antrojoje darbo dalyje pateikiamas siūlomas adaptyvaus autentifikavimo modelis, apibrėžiami jo reikalavimai, veikimo principai ir konceptuali architektūra. Modelis grindžiamas aktyviojo ir pasyviojo adaptyvumo deriniu: aktyvusis adaptyvumas reaguoja į aplinkos pokyčius, o pasyvusis formuoja naudotojo pasitikėjimo profilį pagal prisijungimo kontekstą.

Trečiojoje darbo dalyje aprašoma sukurto prototipo realizacija „Android“ platformoje, pristatoma sistemos architektūra, pagrindiniai moduliai ir atskirų autentifikavimo metodų

įgyvendinimas. Prototipe realizuotas balso, gestais pagrįstas lytėjimo, biometrinis ir vienkartinio slaptažodžio autentifikavimas, taip pat aktyviojo ir pasyviojo adaptyvumo logika, leidžianti sistemai reaguoti į aplinkos pokyčius ir kaupti naudotojo pasitikėjimo profilį.

Ketvirtojoje darbo dalyje atliekamas siūlomo modelio kokybinis ir eksperimentinis vertinimas. Kokybinis palyginimas leidžia įvertinti modelio vietą tarp analizuotų autentifikavimo sprendimų krypčių, o eksperimentinis vertinimas parodo, kaip prototipas veikia skirtingomis naudojimo sąlygomis. Vertinimo metu analizuojamas profilio formavimasis, pasitikėjimo lygio stabilumas, reakcija į konteksto pokyčius, prisitaikymas prie elgsenos pokyčių, laipsniškas silpnėjimas ir balso autentifikavimo priklausomybė nuo aplinkos triukšmo.

Atliktas tyrimas leidžia daryti išvadą, kad siūlomas adaptyvus autentifikavimo modelis gali būti laikomas praktiškai pagrįstu sprendimu, siekiančiu derinti saugumą, prieinamumą ir naudojimo patogumą. Modelio vertė atsiskleidžia ne vien atskirų autentifikavimo metodų pasirinkime, bet jų derinime su kontekstiniu vertinimu ir sprendimų logika.

Paulius Eidimtas. Adaptive Authentication Method for People with Disabilities. Master‘s Final Degree Project supervisor prof. Algimantas Venčkauskas; Faculty of Informatics, Kaunas University of Technology.

Study field and study field group: Computer Sciences, Information and information technology security.

Keywords: Adaptive authentication, people with disabilities, multi-method authentication, context based evaluation.

Kaunas, 2026. 74.

Summary

Paper addresses the problem of accessible authentication for people with disabilities and presents a proposed adaptive identification and authentication method aimed at improving access to digital services. The relevance of the topic is determined by the fact that traditional authentication methods, such as text-based passwords, PIN codes, or actions requiring precise input, are not equally suitable for users with visual, motor, or text processing impairments. Therefore, authentication solutions must be evaluated not only in terms of security, but also in terms of practical accessibility, flexibility of use, and the availability of fallback authentication methods.

The aim of the thesis is to develop a secure and user friendly adaptive authentication model oriented toward greater accessibility for people with disabilities. To achieve this aim, the problems caused by traditional authentication methods were analyzed, existing biometric, multi method, and adaptive authentication approaches were examined, the requirements for the proposed model were defined, its conceptual model was developed, and a prototype was implemented, including voice, gesture based, biometric, and one time password authentication. In addition, a qualitative comparison of the proposed model with the analyzed authentication solution approaches and an experimental evaluation were carried out.

First part of the thesis analyzes authentication challenges faced by different user groups and reviews existing authentication solution approaches. The analysis showed that a single authentication method cannot be considered a universal solution for all users, therefore, accessible authentication must combine multiple methods, context awareness, and fallback authentication options.

Second part presents the proposed adaptive authentication model, defines its requirements, operating principles, and conceptual architecture. The model is based on a combination of active and passive adaptivity: active adaptivity responds to environmental changes, while passive adaptivity forms a user trust profile based on login context.

Third part describes the implementation of the developed prototype on the Android platform, presents the system architecture, the main modules, and the implementation of individual authentication methods. The prototype includes voice, gesture based, biometric, and one time password authentication, as well as active and passive adaptivity logic that

allows the system to respond to environmental changes and accumulate the user’s trust profile.

Fourth part provides a qualitative and experimental evaluation of the proposed model. The qualitative comparison allows the position of the model among the analyzed authentication solution approaches to be assessed, while the experimental evaluation shows how the prototype operates under different usage conditions. The evaluation analyzes profile formation, trust level stability, response to context changes, adaptation to behavioral changes, time based decay, and the dependence of voice authentication on environmental noise.

The conducted research leads to the conclusion that the proposed adaptive authentication model can be regarded as a practically justified solution aimed at balancing security, accessibility, and usability. The value of the model lies not only in the choice of individual authentication methods, but also in their combination with context aware evaluation and decision logic.

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Santrumpų ir terminų sąrašas

CAPTCHA – iššūkio ir atsako testas naudojamas kompiuterijoje siekiant nustatyti, ar naudotojas yra žmogus.
FIDO – standartas, sukurtas siekiant padidinti interneto saugumą ir autentifikavimą, sumažinant priklausomybę nuo tradicinių slaptažodžių.
WCAG – gairės pateikiančios įvairias rekomendacijas, kaip padaryti žiniatinklio turinį prieinamesnį.
FIDO UAF – universali autentifikavimo sistema platesnės iniciatyvos FIDO kuria siekiama padidinti interneto saugumą ir autentiškumo nustatymą, dalis.
SSID – „Wi-Fi“ tinklo pavadinimas, kuris leidžia jį atskirti nuo kitų netoliese esančių tinklų.
Zero-trust – kibernetinio saugumo strategija, kuri vadovaujantis principu „niekada nepasitikėk, visada tikrink“.
RMS (*root-mean-square*) – signalo stiprumo įvertinimo metodas, parodantis vidutinį garso signalo energijos lygį per tam tikrą laiko intervalą. Šiame darbe RMS naudojamas aplinkos triukšmo lygiui įvertinti prieš balso autentifikaciją, siekiant nustatyti, ar aplinkos sąlygos yra pakankamai tinkamos balso metodo naudojimui.
OTP – slaptažodis, galiojantis tik vienai prisijungimo sesijai arba operacijai kompiuterinėje sistemoje ar kitame skaitmeniniame įrenginyje.
SIM kortelė – kortelė skirta nustatyti naudotojo tapatybei mobiliojo ryšio tinkle ir ryšio paslaugoms aktyvuoti.
TTS – technologija, kuri paverčia skaitmeninėje sąsajoje esantį tekstą natūraliai skambančiu garso įrašu.
Haptika – kompiuterijoje mokslas, tiriantis vartotojo sąsają, susijusią su elektroniškai jautraus įrenginio lietimo pojūčiu.

Įvadas

Daugelis žmonių, turinčių negalią, susiduria su sunkumais bandydami naudotis IT paslaugomis ir įrenginiais. Tradiciniai slaptažodžiais paremti autentifikavimo metodai, kuriems reikia tikslių motorinių įgūdžių, teksto suvokimo ir nuoseklios įvesties veiksmų, gali tapti kliūtimi tokiems asmenims. Tai skatina būtinybę kurti naudotojui draugiškus identifikavimo ir autentifikavimo metodus, kurie derintų saugumą, prieinamumą bei praktinį naudojamumą.

Atsižvelgiant į didėjantį informacinių technologijų vaidmenį kasdieniame gyvenime ir į asmenų su negalia poreikį savarankiškai naudotis skaitmeninėmis paslaugomis, šiame darbe nagrinėjamos problemos, susijusios su tradiciniais autentifikavimo metodais ir jų keliamais iššūkiais skirtingoms naudotojų grupėms. Daugiausia dėmesio skiriama asmenims turintiems regos, motorikos sutrikimų, disleksiją ar kitų teksto apdorojimo sunkumų. Atliekant analizę vertinama, kaip esami autentifikavimo sprendimai atitinka prieinamumo, saugumo ir privatumo reikalavimus, taip pat atsižvelgiama į Europos Sąjungos ir Lietuvos Respublikos teisines nuostatas, susijusias su asmenų su negalia teisėmis ir duomenų apsauga.

Darbo tikslas – sukurti saugų ir naudotojui draugišką adaptyvų autentifikavimo modelį, skirtą neįgaliųjų naudojimosi skaitmeninėmis paslaugomis prieinamumui gerinti.

Norint pasiekti šį tikslą iškelti šie uždaviniai:

1. Išanalizuoti tradicinių autentifikavimo metodų keliamas problemas naudotojams, turintiems regos, motorikos bei teksto apdorojimo sunkumų.
2. Išnagrinėti esamas prieinamo, biometrinio, daugiametodžio ir adaptyvaus autentifikavimo sprendimų kryptis, įvertinant jų tinkamumą pasirinktoms naudotojų grupėms.
3. Apibrėžti siūlomo adaptyvaus autentifikavimo modelio reikalavimus ir suformuoti jo koncepcinį modelį.
4. Realizuoti siūlomo autentifikavimo modelio prototipą, apimantį balso, gestais pagrįstą lytėjimo, biometrinį ir vienkartinio slaptažodžio autentifikavimą.
5. Atlikti siūlomo modelio kokybinį palyginimą su analizuotomis autentifikavimo sprendimų kryptimis.
6. Atlikti eksperimentinį siūlomo modelio vertinimą ir įvertinti gautus rezultatus.

Darbą sudaro keturi pagrindiniai skyriai. Pirmajame skyriuje analizuojamos autentifikavimo problemos, su kuriomis susiduria skirtingų poreikių turintys naudotojai, bei nagrinėjamos esamos autentifikavimo sprendimų kryptys. Antrajame skyriuje formuojamas siūlomas autentifikavimo modelis, apibrėžiami jo reikalavimai ir veikimo principai. Trečiajame skyriuje aprašoma sukurto prototipo realizacija. Ketvirtajame skyriuje pateikiamas siūlomo modelio kokybinis ir eksperimentinis vertinimas.

1. Identifikavimo ir autentifikavimo metodų neįgaliesiems analizė

1.1. Žmonių su negalia įsitraukimo ir integracijos problemos IT srityje

Žmonių su negalia įsitraukimas į informacinių technologijų aplinką vis dar susiduria su dideliais prieinamumo iššūkiais. Praktikoje daugelis programinių aplikacijų, sistemų ir skaitmeninių paslaugų nėra kuriamos taip, kad būtų visapusiškai tinkamos skirtingų poreikių naudotojams. Dėl to asmenims turintiems regėjimo sutrikimų, teksto apdorojimo sunkumų ar judėjimo apribojimų, sudėtingiau visaverčiai naudotis skaitmeninėmis sistemomis. Ši problema ypač svarbi naudotojo identifikavimo ir autentifikavimo procesuose, nes būtent juose dažnai taikomi griežti, standartizuoti ir ne visiems vienodai prieinami identifikavimosi būdai, pavyzdžiui, tekstinių slaptažodžių įvedimas, vizualinių elementų atpažinimas ar tikslūs jutikliniai veiksmai. Todėl analizuojant autentifikavimo metodus svarbu vertinti ne tik jų saugumą, bet ir jų prieinamumą skirtingiems naudotojams. Šiame darbe toliau nagrinėjami būtent tie prieinamumo aspektai, kurie yra tiesiogiai susiję su autentifikavimo naudojamumu ir adaptavimo poreikiu tikslinėms naudotojų grupėms.

1.1.1. Regėjimo sutrikimų turinčių asmenų prieinamumo problemos naudojantis IT sistemomis

Asmenys, turintys regėjimo sutrikimų, naudodamiesi informacinėmis technologijomis dažnai susiduria su kliūtimis, kurios atsiranda dėl vyraujančio vizualiai orientuoto sistemų projektavimo. Nors šiuolaikinės skaitmeninės sistemos tampa vis sudėtingesnės ir funkcionalesnės, jų sąsajos bei informacijos pateikimo būdai ne visada yra vienodai tinkami skirtingų poreikių naudotojams. Wahidinas ir kt. [1] parodė, kad reikšmingų sunkumų gali sukelti vaizdų, diagramų, tam tikrų dokumentų struktūrų, svetainių išdėstymo bei kitų skaitmeninių elementų neprieinamumas, dėl kurio naudotojams tampa sunkiau efektyviai suvokti pateikiamą informaciją ir atlikti reikiamus veiksmus. Tai rodo, kad dalis sistemų kuriamos remiantis prielaida, jog naudotojas informaciją suvoks tik regėjimu, nors toks požiūris nėra tinkamas visoms naudotojų grupėms. Autentifikavimo kontekste ši problema tampa ypač aktuali, nes prisijungimo procesai dažnai grindžiami simbolių atpažinimu, vizualiniais elementais, ekrane pateikiamomis nuorodomis ar kitais veiksmais, kurie paremti žmogaus gebėjimu matyti. Dėl to prieinami autentifikavimo metodai turėtų būti vertinami ne tik pagal jų saugumo lygį, bet ir pagal tai, kiek jie sumažina priklausomybę nuo vien tik vizualaus informacijos suvokimo. Tokie metodai turėtų sudaryti galimybę taikyti alternatyvius sąveikos būdus, kurie leistų naudotojui patogiau ir efektyviau naudotis sistema, atsižvelgiant į jo individualias galimybes.

1.1.2. Asmenų, turinčių disleksiją, problemos naudojantis tekstu grindžiamomis sistemomis

Asmenys, turintys disleksiją, dažnai susiduria su sunkumais skaitmeninėse aplinkose, kuriose naudotojo veikla grindžiama teksto skaitymu, rašymu ir simbolių atpažinimu. Nors tekstinė informacija išlieka svarbi daugelyje informacinių technologijų veiklų, būtent autentifikavimo kontekste šis reikalavimas tampa ypač probleminis, nes naudotojas turi ne tik atpažinti simbolius, bet ir juos tiksliai prisiminti, atkurti bei įvesti be klaidų. Evtimova ir

Nicholson [2] pažymi, kad žmonės, turintys disleksiją, naudodamiesi raidiniais ir skaitiniais slaptažodžiais susiduria su papildomais sunkumais, susijusiais su skaitymu, rašyba, simbolių seka ir atmintimi. Tyrime taip pat nustatyta, kad tokie naudotojai neretai pasitelkia kompensacines strategijas, pavyzdžiui, remiasi lengvai atkartojamais šablonais ar paprastesnėmis kombinacijomis, kurios gali sumažinti autentifikavimo saugumą. Tai rodo, kad tradiciniai tekstu paremti autentifikavimo metodai nėra neutralūs visų naudotojų atžvilgiu, nes daliai jų sukuria papildomą kognityvinę ir praktinę naštą. Dėl to prienamumu paremti autentifikavimo sprendimai turėtų mažinti priklausomybę nuo tikslaus teksto suvokimo ir įsiminimo bei numatyti alternatyvius tapatybės patvirtinimo būdus, kurie būtų patogesni naudotojams, turintiems teksto apdorojimo sunkumų.

1.1.3. Asmenys kurie turi judėjimo problemų ar galūnių trūkumą, problemos naudojantis IT

Asmenys, turintys judėjimo sutrikimų ar viršutinių galūnių funkcinių apribojimų, naudodamiesi informacinėmis technologijomis dažnai susiduria su kliūtimis, kurios kyla dėl standartinio įvesties modelio dominavimo autentfikavimo scenarijuose. Dauguma skaitmeninių sistemų projektuojamos darant prielaidą, kad naudotojas galės tiksliai ir pakankamai greitai naudotis klaviatūra, pele ar jutikliniu ekranu, tačiau tokia prielaida nėra universali. Lewisas ir Venkatasubramanianas [3] parodė, kad žmonėms, turintiems viršutinių galūnių funkcinių sutrikimų, sunkumų kyla ne tik įvedant slaptažodžius ar „PIN“ kodus, bet ir platesniame autentifikavimo procese, įskaitant prisijungimo nustatymą, pakartotinius bandymus bei atsarginių autentifikavimo būdų naudojimą, o tai dažnai skatina rinktis praktiškai patogesnius, tačiau saugumo požiūriu silpnesnius sprendimus. Tokius kaip trumpesnius „PIN“ kodus, lengviau įvedamus slaptažodžių šablonus, autentifikavimo išjungimą dažniau naudojamuose įrenginiuose, bei dalijimąsi prisijungimo duomenimis su pagalbą teikiančiais asmenimis. Andrew ir kt. [4] taip pat pažymi, kad motorikos sutrikimai gali apsunkinti tekstinės įvesties veiksmus, o gestais grindžiama sąveika gali reikalauti daugiau laiko ir pasižymėti mažesniu nuoseklumu. Dėl to autentifikavimo kontekste ypač svarbu, kad naudotojo tapatybės patvirtinimas nepriklausytų vien nuo tikslios smulkiosios motorikos ar griežtai apibrėžtos įvesties būdo. Prieinami autentifikavimo sprendimai turėtų sudaryti sąlygas alternatyviems sąveikos būdams ir būti projektuojami taip, kad sumažintų fizinės kontrolės tikslumo reikalavimus, kartu išlaikydami praktinį naudojamumą skirtingiems naudotojams.

1.2. Esami autentifikavimo metodai ir jų apribojimas neįgaliesiems

Esami autentifikavimo metodai, nors ir sukurti saugumui užtikrinti, dažnai kelia didelių kliūčių įvairią negalią turintiems asmenims. Daugelis plačiai taikomų sprendimų remiasi prielaida, kad neįgalusis galės tiksliai perskaityti ir įsiminti tekstinę informaciją, be klaidų įvesti simbolių sekas, greitai atlikti nuoseklius veiksmus ir patikimai naudotis standartiniais įvesties įrenginiais. Tai gali tapti kliūtimi žmonėms, turintiems regėjimo sutrikimų, disleksiją ar kitų su teksto apdorojimu susijusių sunkumų, taip pat asmenims, turintiems judėjimo ar viršutinių galūnių funkcinių apribojimų. Ribotumai kyla ne tik dėl individualių neįgaliųjų savybių, bet ir dėl pačių autentifikavimo metodų struktūros, kai saugumo užtikrinimas grindžiamas vienu dominuojančiu sąveikos būdu, pavyzdžiui, tekstinių slaptažodžių įvedimu ar tiksliais fiziniais veiksmais. Todėl analizuojant esamus autentifikavimo metodus

svarbu vertinti ne vien jų saugumo lygį, bet ir tai, kiek jie priklauso nuo teksto suvokimo, vizualinės informacijos apdorojimo, tikslios motorinės kontrolės. Būtent šie aspektai leidžia nustatyti, kodėl dalis tradicinių autentifikavimo sprendimų yra nepakankamai prieinami ir pagal kokius kriterijus turėtų būti vertinami alternatyvūs autentifikavimo metodai.

1.2.1. Tekstiniu pagrindu paremtų slaptažodžių naudojimo problemos asmenims, turintiems disleksiją

Tekstiniai slaptažodžiai išlieka viena dažniausiai taikomų naudotojo autentifikavimo priemonių, tačiau jų naudojimas grindžiamas prielaida, kad naudotojas gebės tiksliai perskaityti, įsiminti ir atkurti raidžių, skaičių bei simbolių sekas. Asmenims, turintiems disleksiją, tokie reikalavimai gali tapti reikšminga kliūtimi, nes jiems būdingi sunkumai, susiję su žodžių atpažinimu, simbolių seka, rašyba ir teksto apdorojimu. Evtimova ir Nicholson [2] pažymi, kad disleksijos požymių pasireiškia maždaug 10 % populiacijos, o Jungtinėje Karalystėje apie 4 % gyventojų patiria sunkius šio sutrikimo simptomus. Nepaisant to, ši naudotojų grupė autentifikavimo kontekste ilgą laiką buvo nepakankamai nagrinėta, nors tekstiniai slaptažodžiai yra dominuojantis autentifikavimosi metodas. Jų tyrimas parodė, kad asmenys, turintys disleksiją, autentifikavimo metu dažnai pasitelkia prisitaikymo strategijas, pavyzdžiui, remiasi lengvai atkartojamais šablonais ar paprastesnėmis kombinacijomis, kurios gali sumažinti slaptažodžių saugumą. Be to, įprastos slaptažodžių kūrimo rekomendacijos, akcentuojančios sudėtingumą ir atsitiktinumą, šiai naudotojų grupei gali dar labiau padidinti praktinio naudojimo sudėtingumą ir klaidų tikimybę. Tai rodo, kad tekstu grindžiami autentifikavimo metodai nėra vienodai tinkami visiems naudotojams, todėl vertinant prieinamus autentifikavimo sprendimus svarbu atsižvelgti į tai, kiek jie padeda sumažinti priklausomybę nuo teksto suvokimo, rašymo ir įsiminimo.

1.2.2. Autentifikacijos naudojimo problemos asmenims su judėjimo problemomis arba galūnių trūkumu

Asmenims, turintiems judėjimo sutrikimų ar galūnių trūkumą, tradiciniai autentifikavimo metodai dažnai kelia papildomų kliūčių, nes daugelis jų remiasi tikslia tekstine įvestimi arba nuosekliais fiziniais veiksmais. Slaptažodžių ar „PIN“ kodų įvedimas klaviatūra, jutikliniu ekranu ar kitomis standartinėmis įvesties priemonėmis gali būti sudėtingas tais atvejais, kai naudotojas negali patikimai atlikti veiksmų reikalaujančių tikslios motorikos. Lewisas ir Venkatasubramanianas [3] parodė, kad žmonėms, turintiems viršutinių galūnių funkcinių sutrikimų, problemų kyla ne tik pačio įvedimo metu, bet ir platesniame autentifikavimo procese, įskaitant prisijungimo nustatymą, pakartotinius bandymus, atsarginių autentifikavimo būdų taikymą bei užblokavimo situacijų valdymą. Dėl to dalis naudotojų renkasi fiziškai lengviau pritaikomus, tačiau saugumo požiūriu silpnesnius sprendimus, pavyzdžiui, trumpesnius „PIN“ kodus, paprastesnius slaptažodžių modelius arba autentifikavimo išjungimą tam tikruose įrenginiuose. Vatavuas ir Ungureanas [5] taip pat parodė, kad naudotojai, turintys viršutinės kūno dalies motorikos sutrikimų, gestais grindžiamą įvestį dažnai atlieka lėčiau ir mažiau nuosekliai nei naudotojai be tokių sutrikimų. Vien gesto panaudojimas savaime dar neužtikrina prieinamo autentifikavimo. Be to, biometriniai metodai, tokie kaip pirštų atspaudų ar veido atpažinimas, ne visada yra vienodai tinkami visiems naudotojams, nes jų praktinis naudojimas gali priklausyti nuo

kūno padėties, judesių kontrolės ar konkretaus įrenginio sąsajos. Tai rodo, kad prieinamas autentifikavimas šiai naudotojų grupei negali būti grindžiamas vienu fiksuotu metodu, todėl būtini lankstesni sprendimai, leidžiantys naudoti alternatyvius autentifikavimosi būdus.

1.2.3. Autentifikacijos panaudojimo problemos asmenims su regėjimo problemomis

Asmenims, turintiems regėjimo sutrikimų, tradiciniai autentifikavimo metodai dažnai kelia papildomų prieinamumo ir saugumo problemų, ypač tais atvejais, kai autentifikavimas grindžiamas tekstine įvestimi arba vizualinių elementų atpažinimu. Briotto Faustinas ir Girouardas [6] tyrimas parodė, kad žmonės, turintys regėjimo sutrikimų, slaptažodžių kūrimui dažnai renkasi pažįstamus vardus ir skaičius, nes taip juos lengviau įsiminti, tačiau tokia praktika gali silpninti saugumą. Tas pats tyrimas taip pat atskleidė, kad pirštų atspaudų autentifikavimas šios naudotojų grupės dažnai vertinamas kaip vienas prieinamiausių ir saugiausių metodų, o „PIN“ kodai bei tekstu ar tiksliu ekrano valdymu grindžiami metodai laikomi mažiau patogiais. Be to, naudotojams, turintiems regėjimo sutrikimų, papildomų problemų kyla autentifikuojantis viešose vietose, nes slaptažodžių ar „PIN“ kodų įvedimas gali padidinti tiek vizualinio stebėjimo, tiek garsinio informacijos nutekėjimo riziką, ypač naudojantis ekrano skaitytuvais ar kitomis garsinėmis pagalbos priemonėmis. Taip pat riboto prieinamumo gali turėti metodai, kuriems būtinas tikslus vizualinis sąsajos elementų pasirinkimas, pavyzdžiui, ekrane braižomi šablonai ar tam tikri „CAPTCHA“ sprendimai. Tai rodo, kad autentifikavimo prieinamumas regėjimo sutrikimų turintiems naudotojams priklauso ne tik nuo pasirinkto metodo saugumo, bet ir nuo to, kiek jis remiasi rega. Todėl prieinami autentifikavimo sprendimai turėtų suteikti alternatyvius tapatybės patvirtinimo būdus ir vengti tokio projektavimo, kuriame rega tampa pagrindine ar vienintele sąlyga autentifikavimuisi.

1.3. Autentifikacijos problemas spręsti tinkamų įrenginių ir technologinių sprendimų analizė

Ankstesniuose poskyriuose nustatyta, kad tradiciniai autentifikavimo metodai ne visais atvejais yra tinkami naudotojams, turintiems regėjimo sutrikimų, disleksiją ar kitų su teksto apdorojimu susijusių sunkumų, taip pat asmenims, turintiems judėjimo ar viršutinių galūnių funkcinių apribojimų. Dėl šios priežasties autentifikavimo prieinamumo problema negali būti sprendžiama vienu universaliu metodu, nes skirtingi technologiniai sprendimai pašalina skirtingas naudojimo kliūtis ir kartu sukuria savus apribojimus. Vieni sprendimai mažina priklausomybę nuo tekstinės įvesties, kiti leidžia sumažinti tikslios motorikos poreikį, o dar kiti suteikia galimybę autentifikavimą grįsti ne vien tekstu ar vizualiniais elementais, bet ir balsu, lytėjimu ar kitais alternatyviais sąveikos būdais. Todėl šiame skyriuje tikslinga analizuoti ne tik atskirus įrenginius ar autentifikavimo metodus, bet ir jų praktinį tinkamumą, prieinamumo potencialą bei ribotumus realaus naudojimo kontekste. Toliau bus nagrinėjami pasirinkti technologiniai sprendimai ir autentifikavimo būdai, siūlomi kaip alternatyva tradiciniams metodams. Ši analizė leis įvertinti jų stipriąsias ir silpnąsias puses bei išskirti įžvalgas, svarbias formuojant prieinamesnį autentifikavimo modelį.

1.3.1. Dviejų veiksnių autentifikavimas, pagrįstas haptika, skirtas akliesiems ir silpnaregiams

Vienas iš technologinių sprendimų, siekiančių sumažinti rega ir garsu grindžiamos sąveikos priklausomybę autentifikavimo procese, yra haptika paremti metodai. Bhole ir kt. [7] pasiūlytas „Haptic2FA“ metodas nagrinėja dviejų veiksnių autentifikavimo prieinamumo problemą akliems ir silpnaregiams naudotojams. Tradiciniai „2FA“ scenarijai dažnai remiasi vienkartinių kodų gavimu žinutėmis, elektroniniu paštu ar autentifikavimo programėlėmis, todėl naudotojui tenka atlikti kelis papildomus veiksmus, persijungti tarp programų ar įrenginių ir per ribotą laiką tiksliai įvesti gautą kodą. Toks procesas gali būti ne tik nepatogus, bet ir mažiau saugus, kai ekrano skaitytuvas garsiai perskaito kodą aplinkiniams girdimoje aplinkoje. „Haptic2FA“ siūlo alternatyvą – vietoje įprasto kodo naudotojui pateikiamas vibracija paremtas šablonas, kurį vėliau reikia atpažinti arba įvesti. Tyrimo rezultatai parodė, kad toks sprendimas gali būti naudojamas pakankamai tiksliai ir dalyvių buvo vertinamas kaip prieinamesnis už įprastus „2FA“ metodus, nes sumažina būtinybę naudotis papildomomis vizualinėmis ar garsinėmis priemonėmis. Vis dėlto išlieka ir ribotumų: haptinių šablonų įsiminimas reikalauja priprasti prie pateikimo metodo, ilgesni šablonai didina kognityvinę apkrovą, o pats autentifikavimo procesas gali užtrukti ilgiau nei paprastesnės alternatyvos. Todėl haptika grindžiami sprendimai rodo, kad prieinamas autentifikavimas gali būti kuriamas pasitelkiant alternatyvius autentifikavimosi kanalus, tačiau praktiniam taikymui vis tiek svarbu numatyti kelių metodų derinimą ir lankstesnes atsargines autentifikavimo galimybes.

1.3.2. Vienkartinio slaptažodžio sistema pritaikyta elektroniniai bankininkystei

Kita svarbi prieinamo autentifikavimo kryptis yra vienkartinio slaptažodžio (*OTP*) sistemų pritaikymas naudotojams, kuriems įprasti kodų nuskaitymo ir įvedimo scenarijai kelia kliūčių. Fuglerud ir Dale [8] nagrinėjo mobiliojo autentifikavimo sprendimą, skirtą internetinės bankininkystės aplinkai, kuriame standartinis vizualiai pateikiamas vienkartinis kodas buvo papildytas integruotu garsiniu pateikimu. Toks sprendimas buvo orientuotas į aklus ir silpnaregius naudotojus, taip pat į asmenis, turinčius skaitymo ir rašymo sunkumų, kuriems įprastas tekstu grindžiamas „OTP“ procesas gali būti lėtas, painus arba reikalauti kitų asmenų pagalbos. Tyrimo rezultatai parodė, kad integruotas garsinis kodo perskaitymas gali reikšmingai padidinti prieinamumą, nes naudotojui nebereikia remtis vien rega ar papildoma pagalbine programine įranga. Tačiau kartu išryškėjo ir esminiai šio sprendimo ribotumai: „OTP“ autentifikavimas išlieka kelių žingsnių procesu, kuriame naudotojas turi suprasti veiksmų seką, laiku perkelti kodą iš vieno įrenginio ar sąsajos į kitą ir išvengti klaidų esant laiko apribojimams. Be to, garsinis kodo pateikimas gali kelti papildomų privatumo rizikų, jeigu naudotojas nesinaudoja ausinėmis arba autentifikavimo aplinka nėra pakankamai privati. Todėl tokio tipo sprendimai rodo, kad „OTP“ sistemos gali būti pritaikomos prieinamumui gerinti, ypač integruojant garsinį kodo pateikimą ir pagalbines įvedimo funkcijas, tačiau jos išlieka labiau tinkamos kaip papildomas ar atsarginis autentifikavimo būdas, o ne kaip universaliai patogiausias sprendimas kasdieniam naudojimui.

1.3.3. Dėvimais galvos įrenginiais paremta pasyvioji autentifikacija asmenims, turintiems viršutinių galūnių sutrikimų

Lewis ir kt. [9] tyrime nagrinėjamas autentifikavimo metodas, skirtas asmenims, turintiems viršutinių galūnių sutrikimų, kurie dėl riboto rankų, plaštakų ar pirštų valdymo gali susidurti su sunkumais naudodami tradicinius autentifikavimo būdus. Tyrime nagrinėjama galimybė autentifikacijai naudoti ant galvos nešiojamus išmaniuosius įrenginius, tokius kaip „Google Glass“, kuriuose integruoti akselerometro ir giroskopo jutikliai. Šis metodas paremtas ne aktyviu naudotojo veiksmu, o pasyvia biometrinių signalų analize: naudotojui tereikia dėvėti įrenginį ir trumpą laiką ramiai sėdėti, o sistema iš natūralių galvos judesių išveda balistokardiogramos signalą, atspindintį širdies veiklos sukeltus kūno mikro judesius. Gauti duomenys vėliau apdorojami konvoliuciniais neuroniniais tinklais, kurie naudojami konkretaus naudotojo tapatybei patvirtinti.

Šio sprendimo vertė prieinamumo požiūriu yra ta, kad autentifikavimas nereikalauja nei slaptažodžio įvedimo, nei tikslių rankos judesių, nei balso sąveikos, kuri kai kuriems naudotojams taip pat gali būti apsunkinta. Tyrimo autoriai pabrėžia, kad toks metodas ypač aktualus tais atvejais, kai asmenys su viršutinių galūnių sutrikimais naudojasi dėvimaisiais įrenginiais asistavimo, reabilitacijos ar kasdienės veiklos tikslais, o jų valdomuose įrenginiuose gali būti saugoma jautri informacija. Tyrime buvo naudojami 6 asmenų, turinčių viršutinių galūnių sutrikimų, duomenys, pagal kuriuos buvo kuriami individualūs autentifikavimo modeliai. Papildomai vertinimui pasitelkti 22 dalyviai be tokių sutrikimų, kurių duomenys naudoti palyginimui. Autoriai parodė, kad naudotoją galima autentifikuoti per 4 sekundes. Vidutinė lygiųjų klaidų norma iškart po modelio apmokymo siekė 4,02 %, o maždaug po dviejų mėnesių padidėjo iki 10,02 %. Šie rezultatai rodo, kad metodas yra perspektyvus, tačiau jo tikslumą gali mažinti nevalingi judesiai, silpnesnė kaklo raumenų kontrolė ir laikui bėgant, fiziologiniai pokyčiai. Šis darbas rodo, kad dėvimų įrenginių jutikliais paremta pasyvioji biometrinė autentifikacija gali būti tinkama alternatyva tradiciniams rankinio įvedimo metodams.

1.3.4. Saugaus ir prieinamo autentiškumo patvirtinimo užtikrinimas asmenims su rankų judesių negalia

Price ir Loizidesas [10] nagrinėjo, kaip autentifikavimo procesą būtų galima pritaikyti rankų ar pirštų judesių sutrikimų turintiems asmenims, kuriems tradicinis „PIN“ kodo įvedimas naudojant fizinės ivesties įrenginius gali būti sudėtingas. Autoriai pasiūlė prieinamos autentifikacijos sistemų kūrimo gaires bei sukūrė prototipą, paremtą žvilgsnio sekimu, leidžiantį „PIN“ kodą įvesti nenaudojant rankų. Tyrime šis metodas buvo lyginamas su įprastu įvedimu kompiuterine pele, vertinant tiek naudojimo patogumą, tiek atsparumą stebėjimo per petį (*shoulder-surfing*) atakoms. Gauti rezultatai parodė, kad žvilgsniu paremtas įvedimas buvo sunkiau interpretuojamas stebėtojui nei įvedimas kompiuterine pele, o dalyviai jį vertino kaip prieinamą ir gana lengvai suprantamą. Vis dėlto autoriai pabrėžia, kad tyrimas buvo pilotinis, atliktas su nedidele imtimi, todėl jo rezultatai vertintini kaip preliminarūs. Nepaisant to, šis darbas parodo, kad akių sekimu pagrįsta autentifikacija gali būti perspektyvi kryptis kuriant prieinamesnius sprendimus tiems naudotojams, kuriems rankiniu įvedimu paremti metodai nėra tinkami.

1.3.5. Balsu paremta autentifikacija kaip prieinamo autentifikavimo kryptis

Olaniyi ir kt. [11] tyrime pristatoma „V-Authenticate“ sistema, kurioje balsas naudojamas kaip biometrinis požymis rinkėjų tapatybei patvirtinti. Siūlomas sprendimas skirtas padėti neįgaliems naudotojams dalyvauti elektroninio balsavimo procese, sumažinant priklausomybę nuo tradicinių autentifikavimo priemonių. Sistemoje naudotojo balsas apdorojamas išskiriant balso požymius ir juos lyginant su anksčiau registruotais duomenimis. Autoriai sistemos veikimą vertino pagal balso signalo apdorojimo kokybės rodiklius. Tyrimas rodo, kad balsu paremta autentifikacija gali būti taikoma kaip alternatyvus tapatybės patvirtinimo. Tačiau šį darbą tikslingiau vertinti kaip taikymo pavyzdį, o ne kaip universaliai patvirtintą sprendimą visiems prieinamumo atvejams. Šią kryptį papildo Toussaint ir kt. [12] aprašomas „ALIAS“ projektas, kuriame pabrėžiama, kad akliems ir silpnaregiams naudotojams įprasti autentifikavimo mechanizmai dažnai tampa sunkiai įveikiamais barjerais. Autoriai akcentuoja ne vien techninio saugumo, bet ir prieinamumo bei naudotojo patirties svarbą, siūlydami prieinamas autentifikavimo priemones kurti taikant vartotoją su negalia įtraukiantį į projektavimo procesą. Nors „ALIAS“ dar nepateikia galutinio, pilnai validaus autentifikavimo sprendimo, šis darbas svarbus tuo, kad pagrindžia poreikį kurti autentifikavimo sistemas, kurios būtų ne tik saugios, bet ir pritaikytos realiems aklų ir silpnaregių naudotojų poreikiams. Todėl galima daryti išvadą, kad balsu paremta autentifikacija turi aiškų prieinamumo potencialą, tačiau šiuo metu ji labiau atspindi tolesnių tyrimų kryptį nei galutinai nusistovėjusį autentifikavimo sprendimą, pritaikytą asmenims, turintiems regėjimo negalią

1.4. Esamų autentifikavimo sprendimų krypčių analizė

Šiame skyriuje analizuojamos pagrindinės autentifikavimo sprendimų kryptys, siekiant nustatyti, kokie technologiniai principai yra reikšmingi kuriant prieinamas ir adaptyvias autentifikavimo sistemas. Analizė yra grindžiama ne pavienių komercinių ar atviro kodo produktų aprašymu, bet platesniu autentifikavimo sprendimų kategorijų vertinimu. Vertinant atsižvelgiama į architektūrines savybes, naudojimo lankstumą, prieinamumo aspektus ir taikymo galimybes. Toks požiūris leidžia autentifikavimo sprendimus vertinti ne tik pagal jų saugumo savybes, bet ir pagal tai, kiek jie pritaikyti prie skirtingų naudotojų poreikių, technologinių galimybių ir naudojimo apribojimų.

1.4.1. Vieno metodo prieinamumo sprendimai atskiroms naudotojų grupėms

Kuriant autentifikaciją, orientuotą į specifinę grupę naudotojų dažniausiai kuriami sprendimai, kuriais siekiama sumažinti aiškiai apibrėžtą kliūtį, pavyzdžiui, priklausomybę nuo regimosios informacijos, teksto įvedimo ar tikslių rankų judesių. Šios krypties privalumas yra tas, kad autentifikavimo procesas gali būti reikšmingai pritaikytas konkrečiam prieinamumo poreikiui, tačiau kartu tokie sprendimai dažnai išlieka riboto pritaikomumo, nes jų veiksmingumas tiesiogiai priklauso nuo pasirinktos priemonės ir konkretaus naudotojo galimybių. Toks sprendimo tipas atskleidžiamas Bhole ir kt. [7] sukurtame „Haptic2FA“ sprendime, kuriame dviejų veiksnių autentifikavimas grindžiamas haptiniais modeliais, skirtais akliesiems ir silpnaregiams naudotojams. Tyrime parodyta, kad dalyviai galėjo pakankamai tiksliai atpažinti ir įvesti vibracijomis perteikiamus kodus, o pats metodas buvo vertinamas kaip prieinamesnis nei tradiciniai vienkartinių kodų

sprendimai, nes nereikalavo vizualiai perskaityti ar persijungti į kitą programą norint gauti autentifikavimo kodą. Vis dėlto šio sprendimo prieinamumas siejamas būtent su haptiniais kanalis, gebėjimu įsiminti vibracinius modelius, todėl jo pritaikomumas kitoms naudotojų grupėms ar kitoms naudojimo situacijoms negali būti laikomas universaliu. Panašiai specializuotą kryptį atspindi akių judesių sekimu pagrįstas Price ir Loizidesas [10] pasiūlytu „PIN“ įvedimo sprendimu, skirtu naudotojams, turintiems plaštakų ar pirštų vikrumo sutrikimų. Šiame sprendime autentifikavimo procesas perkeliamas nuo tradicinio fizinio įvedimo prie žvilgsniu valdomos autentifikacijos, taip sumažinant priklausomybę nuo tikslių rankų judesių. Tyrimo rezultatai rodo, kad toks metodas gali būti suvokiamas kaip prieinamas ir saugesnis konkrečiai naudotojų grupei, tačiau jo taikymas priklauso nuo specializuotos akių sekimo įrangos, kalibravimo, aplinkos sąlygų ir ilgesnio autentifikavimo laiko. Dėl to ir šiuo atveju kalbama ne apie universalią prieinamo autentifikavimo priemonę, o apie tikslinei problemai pritaikytą sprendimą. Apibendrinant galima teigti, kad vieno metodo prieinamumo sprendimai gali būti veiksmingi tada, kai autentifikavimo kliūtis yra aiškiai apibrėžta ir siejama su konkrečia naudotojų grupe. Tačiau tokie sprendimai paprastai išlieka siauresnio pritaikomumo, nes jų prieinamumas ir saugumas priklauso nuo vienos dominuojančios sąveikos formos, o tai riboja jų lankstumą platesniame autentifikavimo kontekste, apimančiame skirtingus naudotojų poreikius.

1.4.2. Biometriniai ir slaptažodžių nenaudojantys autentifikavimo sprendimai

Biometriniai ir slaptažodžių nenaudojantys autentifikavimo sprendimai sudaro svarbią šiuolaikinio autentifikavimo kryptį, kuria siekiama mažinti priklausomybę nuo tradicinių slaptažodžių, „PIN“ kodų ar kitų atmintimi grįstų autentifikavimo duomenų. Šie sprendimai dažniausiai remiasi biometrinių požymių naudojimu arba viešojo rakto kriptografijos principais, leidžiančiais autentifikavimo procesą organizuoti be būtinybės perduoti ar saugoti slaptažodžius už įrenginio ribų. Šios krypties technologinį pagrindą gerai atspindi „FIDO“ standartai [13], kurie orientuoti į saugesnį ir nuo slaptažodžių mažiau priklausomą prisijungimo procesą, pasitelkiant lokalius autentifikavimo mechanizmus ir standartizuotas sąsajas. Praktinio diegimo lygmeniu šią kryptį galima sieti su komerciniais sprendimais, tokiais kaip „HYPR“ [14], kuriuose biometrinis ir slaptažodžių nenaudojantis autentifikavimas integruojamas į organizacijos ar platformos infrastruktūrą. Tokie metodai gali reikšmingai pagerinti saugumą, sumažinti apgaulės riziką ir kartu palengvinti autentifikavimo procesą tais atvejais, kai naudotojui sudėtinga įsiminti ar fiziškai įvesti tekstinius prisijungimo duomenis. Nors tokie sprendimai gali sumažinti kai kurias autentifikavimo kliūtis, jų prieinamumas praktikoje priklauso nuo to, kaip jie yra įgyvendinti, kokiame įrenginyje naudojami ir ar išvis juos palaiko naudotojo turimas įrenginys. Dėl šios priežasties biometriniai ir slaptažodžių nenaudojantys sprendimai vertintini kaip techniškai brandi ir saugumo požiūriu stipri autentifikavimo kryptis, tačiau jų realus prieinamumas skirtingoms naudotojų grupėms atsiskleidžia tik konkrečiame taikymo kontekste.

1.4.3. Adaptyvūs, kontekstą vertinantys autentifikavimo sprendimai

Adaptyvūs ir kontekstą vertinantys autentifikavimo sprendimai sudaro atskirą šiuolaikinio autentifikavimo kryptį, kurioje autentifikavimo reikalavimai nėra taikomi vienodai kiekvienu atveju, bet keičiami priklausomai nuo esamos situacijos, konteksto ir įvertintos rizikos. Kaip nurodo Arias-Cabarcos ir kt. [15] skirtingai nuo statinių autentifikavimo modelių, tokie

sprendimai gali atsižvelgti į papildomus požymius, susijusius su naudotojo elgsena, aplinka, kurioje naudojamas įrenginys ir pagal tai dinamiškai nuspręsti, ar pakanka bazinio autentifikavimo, ar reikia papildomo tapatybės patvirtinimo. Tokia logika svarbi tuo, kad leidžia sumažinti autentifikavimo naštą įprastose, mažos rizikos situacijose, kartu išlaikant galimybę taikyti griežtesnius reikalavimus tada, kai prisijungimo aplinkybės nukrypsta nuo įprasto elgesio. Wieflingas ir kt. [16] tyrimai rodo, kad rizika grįsti autentifikavimo sprendimai naudotojų gali būti suvokiami kaip patogesni už tradicinius dviejų veiksnių autentifikavimo metodus. Progonovas ir kt. [17] pabrėžia, kad tokios sistemos turi būti kuriamos atsargiai, nes jų veikimas glaudžiai susijęs su pakartotinio autentifikavimo logika, atsarginių scenarijų numatymu, sprendimų aiškumu ir tuo, kiek elgsenos ar kontekstinių duomenų renkama apie esamą naudotoją. Dėl šios priežasties adaptyvus autentifikavimas yra reikšminga kryptis sistemoms, siekiančioms derinti saugumą, patogumą ir prieinamumą, tačiau jų kokybę lemia ne vien pati adaptavimo idėja, o tai, ar pasirinktas modelis yra pakankamai skaidrus privatumo požiūriu, bei nesukuria perteklinių autentifikavimo kliūčių.

1.4.4. Daugiametodžiai autentifikavimo sprendimai ir atsarginių metodų svarba

Prieinamo autentifikavimo kontekste svarbus ne tik pagrindinis autentifikavimo metodas, bet ir tai, ar sistema numato veiksmingą alternatyvą tuo atveju, kai šis metodas konkrečioje situacijoje tampa neprieinamas. Dėl šios priežasties daugiametodžiai autentifikavimo sprendimai, leidžia naudotojui rinktis iš kelių autentifikavimosi būdų, juos taikyti lanksčiai atsižvelgiant į aplinkybes. Tokia prieiga ypač aktuali naudotojams su negalia, nes sumažina riziką patekti į situaciją, kai autentifikavimo procesas tampa neįveikiamas dėl aplinkos triukšmo, fizinių apribojimų, sąsajos nepritaikymo ar kitų veiksnių. Atsarginių metodų svarba šiuo atveju siejama ne vien su patogumu, bet ir su saugumu, nes nesėkmingai veikiantis vienintelis autentifikavimo būdas gali paskatinti naudotoją ieškoti pavojingu, bet kasdienį naudojima lengvinančių sprendimų, atsisakyti apsaugos priemonių arba pasikliauti kitų asmenų pagalba. Vis dėlto vien kelių metodų buvimas savaime dar neužtikrina prieinamesnio autentifikavimo, kadangi praktinė tokio sprendimo vertė priklauso nuo to, ar alternatyvūs būdai iš tiesų yra pasiekiami, suprantami ir tinkami skirtingose naudojimo situacijose. Daugiametodžių autentifikavimo sprendimų vertė atsiskleidžia tuomet, kai jie leidžia išvengti autentifikavimo aklaviečių. Kitaip tariant, naudotojui turi būti sudaryta reali galimybė pasinaudoti alternatyviu metodu. Tokiu būdu galima lanksčiau derinti saugumą, prieinamumą ir savarankišką naudojimąsi sistema.

1.4.5. Iš autentifikavimo sprendimų analizės išvedami kokybinio palyginimo kriterijai

Ankstesniuose poskyriuose aptartų autentifikavimo sprendimų analizė leidžia išskirti kriterijus, pagal kuriuos galima nuosekliai vertinti esamas autentifikavimo sprendimų kryptis ir vėliau šiame darbe pristatomą adaptyvaus autentifikavimo modelį. Vertinant tokių sprendimų tinkamumą svarbu atsižvelgti į jų prieinamumą skirtingoms tikslinėms naudotojų grupėms, priklausomybę nuo teksto suvokimo, regimosios informacijos apdorojimo ir motorinės kontrolės. Taip pat svarbūs tokie aspektai kaip jautrumas aplinkos sąlygoms, galimybė taikyti atsarginius autentifikavimo būdus, prisitaikymas prie naudojimo konteksto, privatumo užtikrinimas, duomenų kiekio mažinimas ir sprendimo veikimo aiškumas. Šie

kriterijai sudaro pagrindą tolesniam siūlomo modelio kokybiniam palyginimui su analizuotomis autentifikavimo sprendimų kryptimis.

1.5. Adaptyvaus autentifikavimo saugumo ir teisiniai aspektai

Adaptyvių sprendimų taikymas kelia papildomų saugumo bei teisinių klausimų, susijusių su tuo, kokie duomenys apie naudotoją renkami, kaip jie saugomi, kiek laiko naudojami ir ar toks duomenų naudojimas yra būtinas siekiamam tikslui pasiekti. Duomenų apsaugos požiūriu pagal bendrąjį duomenų apsaugos reglamentą [18], adaptyvus autentifikavimas turi būti grindžiamas duomenų kiekio optimizavimo, tikslo apribojimo ir saugojimo trukmės ribojimo principais. Tai reiškia, kad sistema turėtų rinkti tik tuos naudotojo kontekstinius ar elgsenos duomenis, kurie yra būtini autentifikavimo rizikai įvertinti, o pertekliniai, ilgalaikiai ar su konkrečios asmens veiklos istorija tiesiogiai susiejami duomenys neturėtų būti kaupiami be aiškaus pagrindo. Dėl šios priežasties [17] ir kt. teigia, jog kuriant adaptyvias autentifikavimo sistemas svarbus ne tik pats saugumo mechanizmas, bet ir tai, ar sprendimas yra privatumo požiūriu, skaidrus ir paaiškinamas. Teisiniu požiūriu šie aspektai svarbūs ir dėl to, kad skaitmeninė aplinka turi būti prieinama asmenims su negalia. Europos Sąjungos pagrindinių teisių chartijoje [19] pripažįstama asmenų su negalia teisė naudotis priemonėmis, kurios padeda užtikrinti jų savarankiškumą ir dalyvavimą visuomenės gyvenime, o Lietuvos Respublikos asmens su negalia teisių apsaugos pagrindų įstatyme [20] pabrėžiami individualizavimo ir prieinamumo principai, taikytini ir skaitmeninėje erdvėje. Todėl autentifikavimo sistemos turi būti vertinamos ne tik pagal jų atsparumą grėsmėms, bet ir pagal tai, ar jos nesukuria papildomų kliūčių naudotojams, turintiems skirtingų prieigos poreikių. Atsižvelgiant į tai, adaptyvaus autentifikavimo sprendimų kokybę lemia ne vien gebėjimas dinamiškai reaguoti į riziką, bet ir tai, ar toks prisitaikymas įgyvendinamas laikantis privatumo, duomenų apsaugos ir prieinamumo principų. Tai ypač svarbu sistemoms, kurios siekia derinti saugumą su naudotojo savarankiškumu ir išvengti situacijų, kai apsaugos priemonės tampa papildoma skaitmeninės atskirties priežastimi.

1.6. Analizės išvados

1. Analizė parodė, kad tradiciniai statiniai autentifikavimo metodai nėra vienodai tinkami visiems naudotojams, nes jų naudojimas dažnai priklauso nuo teksto suvokimo, regimosios informacijos apdorojimo arba tikslios motorikos. Todėl prieinamas autentifikavimas turi būti vertinamas ne vien pagal jo atsparumą grėsmėms, bet ir pagal realų naudotojo gebėjimą tuo sprendimu pasinaudoti.
2. Kadangi skirtingos naudotojų grupės susiduria su nevienodomis autentifikavimo kliūtimis: asmenims, turintiems regėjimo sutrikimų, problemiški vizualiai paremti metodai, asmenims su disleksija ar teksto apdorojimo sunkumais – tekstu grindžiami slaptažodžiai, o naudotojams, turintiems judėjimo ar viršutinių galūnių apribojimų, – metodai, reikalaujantys tikslių ir nuoseklių fizinių veiksmų. Tai rodo, kad vienas autentifikavimo būdas negali būti laikomas universaliai prieinamu visiems naudotojams.
3. Alternatyvūs autentifikavimo sprendimai gali sumažinti konkrečias prieinamumo kliūtis, tačiau dažniausiai jie padaro autentifikaciją labiau nišine. Haptika, žvilgsnio sekimas, balsu paremta autentifikacija ar pasyvioji biometrinė autentifikacija yra

perspektyvios technologijos tam tikroms naudotojų grupėms, bet jų praktinis taikymas priklauso nuo techninių sąlygų, aplinkos ir individualių naudotojo galimybių. Dėl to tokie sprendimai turėtų būti vertinami kaip tikslingi, bet riboto pritaikomumo metodai.

4. Prieinamas autentifikavimas neturėtų būti grindžiamas vien vieno metodo naudojimu. Analizė rodo, kad svarbu numatyti kelių autentifikavimo būdų derinimą ir veiksmingus atsarginius variantus. Tai aktualu tais atvejais, kai pagrindinis metodas tampa neprieinamas dėl triukšmo, fizinių apribojimų, sąsajos nepritaikymo ar kitų aplinkybių.
5. Analizė parodė, kad adaptyvūs autentifikavimo sprendimai gali sumažinti naudotojo apkrovą tais atvejais, kai rizika yra maža ir kartu išlaikyti griežtesnę apsaugą neįprastose situacijose. Tačiau tokio modelio kokybė priklauso nuo to ar prisitaikymas yra aiškus, proporcingas ir nesukelia naudotojui papildomų kliūčių.
6. Tyrimo metu pastebėta, jog adaptyvaus autentifikavimo sprendimai turi būti vertinami ne tik techniniu, bet ir teisiniu bei privatumo požiūriu. Tokiose sistemose svarbu rinkti tik tiek duomenų, kiek būtina rizikai įvertinti ir kartu užtikrinti, kad prisitaikymas prie rizikos nepažeistų naudotojo privatumo ir nesumažintų sistemos prieinamumo.

2. Identifikavimo ir autentifikavimo metodas neįgaliesiems projektas

Išanalizavus autentifikavimo iššūkius, su kuriais susiduria įvairias negalias turintys, galima pastebėti, kad šios problemos yra nevienodos ir priklauso nuo konkrečių naudotojo gebėjimų bei autentifikavimo proceso struktūros. Analizė buvo būtina tam, kad būtų suprasta bendra negalią turinčių naudotojų situacija ir įvertinta, su kokiais autentifikavimo barjerais dažniausiai susiduria skirtingos naudotojų grupės.

Universalaus sprendimo, kuris galėtų apimti visas išvardintas grupias šiuo metu nėra ir problemos su kuriomis jos susiduria yra pakankamai skirtingos, todėl yra tikslinga susitelkti į autentifikacijos sprendimo būdą, kuris apimtų kuo didesnę dalį bendrų barjerų, pasitaikančių kelioms grupėms vienu metu. Konkrečiai dėmesys skiriamas trims vartotojų grupėms – regos negalią, disleksiją ir motorikos sutrikimus turintiems asmenims. Šios grupės pasirinktos todėl, kad jų patiriamos autentifikavimo problemos dažnai persidengia: visoms joms sudėtinga naudoti tradicinius tekstinius slaptažodžius, sudėtingas kombinacijas ar sąveikauti su standartinėmis įvesties priemonėmis.

Toks pasirinkimas leidžia sukurti sprendimą, kuris, nors ir nėra visiškai universalus, vis dėlto gali būti pritaikomas kelioms skirtingoms naudotojų grupėms. Tai padidina jo praktinę vertę ir suteikia galimybę pasiūlyti autentifikavimo metodą, kuris ne tik atitinka saugumo reikalavimus, bet ir remiasi įtraukties bei prieinamumo principais.

2.1. Reikalavimai siūlomam sprendimui

Atsižvelgiant į analizės dalyje identifikuotų tikslinių naudotojų poreikius, siūlomam autentifikavimo sprendimui keliami reikalavimai apima tiek techninius, tiek prieinamumo aspektus. Šie reikalavimai apibrėžia, kokiomis savybėmis turi pasižymėti kuriamas modelis, kad būtų užtikrintas ne tik saugumas, bet ir praktinis naudojamumas pasirinktoms naudotojų grupėms:

1. Prieinamumas – sistema turi užtikrinti, kad autentifikacijos procesas būtų pasiekiamas skirtingas negalias turintiems vartotojams. Tai reiškia, jog informacija negali būti pateikiama vien tik tekstiniu formatu – būtina alternatyva per garsinius, vizualinius ar haptinius kanalus. Turi būti numatyti alternatvūs sąveikos būdai, pavyzdžiui, balso, lytėjimo ar biometriniai metodai.
2. Daugialypiškumas – sprendimas turi palaikyti daugiau nei vieną autentifikavimo metodą. naudotojas turėtų galėti rinktis tarp biometrinių duomenų ar simbolinio įvedimo, priklausomai nuo jo poreikių ir aplinkybių.
3. Adaptyvumas – autentifikavimo sistema turi būti lanksti ir prisitaikyti prie skirtingų naudotojų situacijų bei poreikių. Pavyzdžiui, triukšmingoje aplinkoje balso atpažinimas gali būti mažiau veiksmingas, todėl vartotojui turėtų būti pasiūlyta alternatyva, biometrinis autentifikavimas ar simbolinis įvedimas. Taip pat pati sistema laikui bėgant turėtų labiau prisitaikyti prie naudotojo, analizuodama jo elgsenos ypatumus. Be to, adaptacija gali būti grindžiama ir kontekstu atsižvelgiant į tai, ar prisijungimas vyksta įprastoje aplinkoje, tam tikru paros metu ar iš atpažįstamo įrenginio. Tokiu būdu sukuriamas papildomas saugumo sluoksnis.

4. Naudojimo paprastumas – autentifikavimo procesas turi būti aiškus, intuityvus ir nereikalauti didelės kognityvinės ar motorinės apkrovos. Sprendime turėtų būti vengiama ilgų, sudėtingų slaptažodžių, tikslios tekstinės įvesties ir kitų veiksmų, kurie pasirinktoms naudotojų grupėms gali tapti reikšminga kliūtimi.
5. Saugumas ir privatumas. Nors prieinamumas yra svarbus aspektas. Visi autentifikavimo duomenys turi būti tvarkomi pagal duomenų apsaugos reikalavimus, užtikrinant, kad vartotojo asmens informacija būtų saugi, o duomenų apdorojimas – skaidrus.
6. Universalumas. Nors vienas sprendimas negali aprėpti visų įmanomų negalių, jis turi būti projektuojamas taip, kad būtų praktiškai pritaikomas pasirinktoms tikslinėms naudotojų grupėms ir apimtų kuo daugiau jų bendrų autentifikavimo kliūčių.

2.2. Koncepcinis autentifikavimo modelis

Norint atitikti iškeltus reikalavimus sprendimui autentifikvaimo modelis turi sudaryti galimybę naudotojui autentifikuotis keliais skirtingais būdais, pasirenkant ar pritaikant metodą pagal individualius poreikius ir esamą kontekstą. Tokiu būdu sprendimas tampa prieinamas regos negalią, disleksiją ar motorikos sutrikimus turintiems naudotojams, nes kiekvienai grupei yra pasiūlomas parankus autentifikavimo metodas.

Siūlomas modelis remiasi keturiais autentifikavimo būdais:

- Autentifikavimas balsu. Balso atpažinimas leidžia vartotojui prisijungti naudojant balsu tariamą frazę ar balso biometrinius požymius. Šis metodas ypač tinkamas regos negalią turintiems asmenims, nes nereikalauja regos sugebėjimų. Disleksijos atveju balso naudojimas padeda išvengti tekstinės informacijos suvokimo problemų. Motorikos sutrikimų turintiems naudotojams tai suteikia galimybę autentifikuotis nesimant tikslių fizinių veiksmų.
- Gestais pagrįstas lytėjimo autentifikavimas. Šis metodas grindžiamas iš anksto apibrėžta perbraukimų seka jutikliniame ekrane. Autentifikavimo metu kiekvienas perbraukimas pirštu priskiriamas vienai iš keturių krypčių: aukštyn, žemyn, kairėn arba dešinėn. Tokiu būdu suformuojamas naudotojo autentifikavimo šablonas. Toks sprendimas sumažina priklausomybę nuo tekstinės įvesties ir gali būti tinkamas naudotojams, kuriems tradiciniai slaptažodžiai ar „PIN“ kodai yra nepatogūs. Be to, šis metodas gali būti pritaikomas atsižvelgiant į naudotojo motorines galimybes, nes nereikalauja tikslaus simbolių įvedimo.
- Vienkartinio slaptažodžio (*OTP*) autentifikavimas. Šis metodas leidžia naudotojui patvirtinti tapatybę naudojant vienkartinį kodą. Kodas gali būti gaunamas išoriniu kanalu, pavyzdžiui, „SMS“ žinute ir panaudojamas autentifikavimo metu. Toks būdas yra svarbus tais atvejais, kai kiti autentifikavimo metodai naudotojui yra mažiau patogūs, laikinai neprieinami arba nepageidaujami. Tokiu būdu „OTP“ tampa viena iš galimų autentifikavimo alternatyvų bendrame daugiametodžiame modelyje.
- Biometrinis autentifikavimas įrenginyje. Modelyje taip pat numatomas biometrinis autentifikavimo būdas, pasitelkiant išmaniajame įrenginyje jau integruotas priemones, pavyzdžiui, piršto atspaudą. Toks metodas leidžia sumažinti tekstinės

įvesties poreikį ir gali būti ypač patogus naudotojams, kuriems svarbus greitas ir mažai veiksmų reikalaujantis prisijungimo būdas. Tokiu būdu biometrinis autentifikavimas tampa viena iš kelių galimų autentifikavimo alternatyvų, taikomų atsižvelgiant į naudotojo poreikius ir konkretų kontekstą.

Kadangi kuriamas autentifikavimo modelis yra adaptyvus, sistema turi gebėti įvertinti naudotojo kontekstą ir pagal jį parinkti tinkamiausią autentifikavimo eigą. Pavyzdžiui, jei konkretus metodas tam tikromis sąlygomis tampa mažiau patogus ar mažiau patikimas, naudotojui gali būti pasiūlyta kita autentifikavimo alternatyva. Be to, modelis turi gebėti atsižvelgti į naudotojo prisijungimo ypatumus, pavyzdžiui, įprastą laiką ar pasikartojantį naudojimo kontekstą. Tokiu būdu autentifikavimo procesas gali būti ne tik saugesnis, bet ir paprastesnis bei greitesnis pačiam naudotojui.

Atsižvelgiant į duomenų saugojimo aspektą, naudotojo autentifikavimo duomenys turėtų būti saugomi asmeniniame įrenginyje, o ne centralizuotame serveryje. Tokiu būdu jautri informacija, tokia kaip biometriniai duomenys ar individualūs autentifikavimo nustatymai, lieka tik naudotojo telefone. Toks sprendimas sumažina masinio duomenų nutekėjimo riziką ir geriau atitinka duomenų apsaugos principus. Be to, išvengiama biurokratinių kliūčių, susijusių su neįgaliųjų asmens duomenų tvarkymu centralizuotose sistemose, o pats vartotojas išlaiko didesnę kontrolę ir skaidrumą, kaip jo informacija yra naudojama.

2.3. Autentifikavimo modelio veikimas

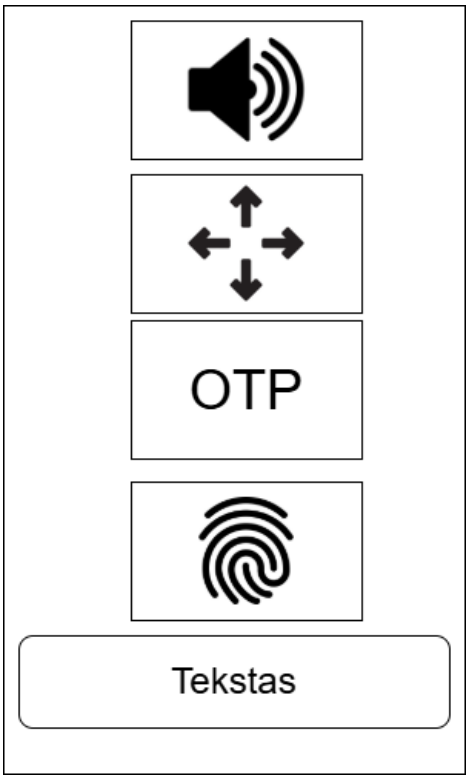
Siūlomas sprendimas turėtų veikti kaip aplikacija išmaniajame įrenginyje, kuri naudotojui užtikrina paprastą, saugią ir prieinamą autentifikacijos patirtį. Pasirinkimas orientuotis į mobiliąją aplikaciją grindžiamas tuo, kad dauguma asmenų naudojasi išmaniaisiais telefonais, o juose yra integruotos įvairios prieinamumo, tokios kaip ekrano skaitytuvai, garsinis grįžtamasis ryšys ar balso komandos. Be to, tokia aplinka leidžia visus duomenis saugoti lokaliai, pačiame įrenginyje, taip išvengiant centralizuotų serverių poreikio ir užtikrinant asmens duomenų apsaugą atitinkančia iškeltuose sprendimo reikalavimuose. Norint suprasti, kaip veiktų ši aplikacija, būtina autentifikacijos procesą išskaidyti į aiškius etapus. Pirmasis etapas yra pradinė konfiguracija, kurios metu vartotojas užregistruoja savo duomenis ir pasirenka prioritetinį autentifikavimo metodą. Toliau seka kasdienio naudojimo eiga, kur modelio adaptatyvumas leidžia pritaikyti autentifikacijos eigą prie naudotoją supančių aplinkybių ir poreikių.

2.3.1. Pradinė konfiguracija

Pirmą kartą paleidus aplikaciją, naudotojas turi būti vedamas per pradinį autentifikavimo paruošimo procesą. Šio etapo tikslas, užregistruoti visus siūlomame modelyje numatytus autentifikavimo būdus ir nustatyti jų asmenine nuožiūra parinktą taikymo eiliškumą. Tokiu būdu sistema iš karto paruošiama vėlesniam adaptyviam veikimui.

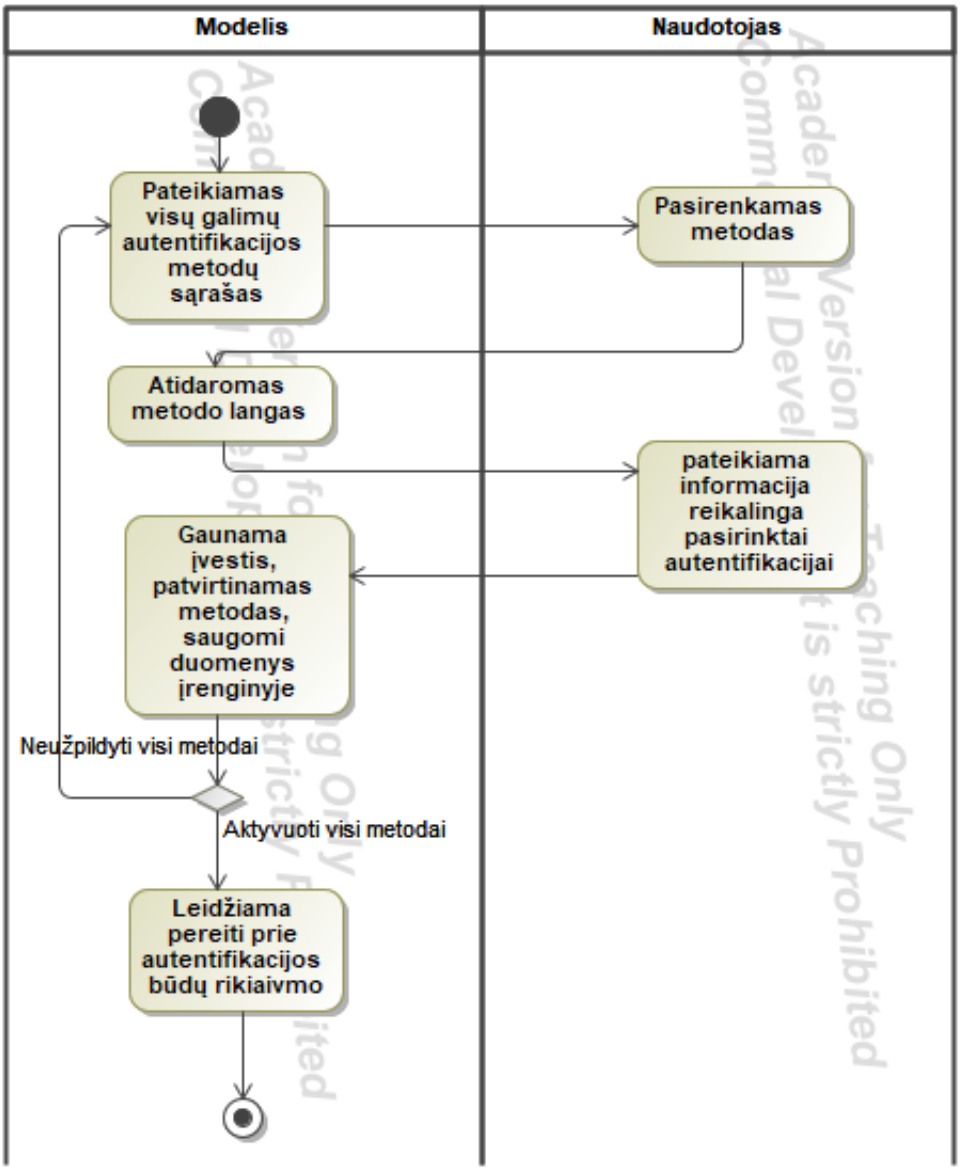
Pradinės konfigūracijos metu naudotojui pateikiamos keturios autentifikavimo parinktys: balsas, gestais pagrįstas lytėjimo metodas, vienkartinis slaptažodis (*OTP*) ir biometrinis metodas įrenginyje (žr. **1 pav.** Pradinės parinktys). Visų parinkčių metu naudotojui turi būti teikiamos aiškios instrukcijos vizualiai ir garsiniu būdu. Tokiu būdu užtikrinama, kad skirtingų poreikių turintys naudotojai galėtų sėkmingai užbaigti registracijos procesą.

Kiekviena parinktis pateikiama kaip atskiras aiškiai pažymėtas pasirinkimo laukas. Be to, atsižvelgiant į regos ar skaitymo sunkumų turinčius naudotojus, kiekvienam pasirinkimui taip pat pateikiamas garsinis paaiškinimas. Motorikos sutrikimų turintiems asmenims visos parinktys pateikiamos dideliuose, lengvai paspaudžiamuose laukeliuose, kad nereikėtų atlikti tikslių judesių.



1 pav. Pradinės parinktys

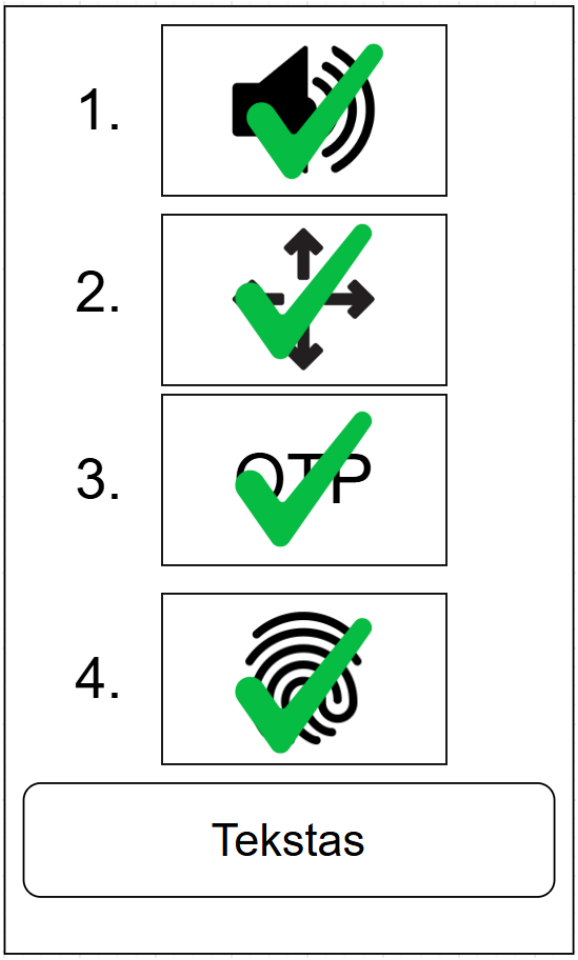
Tokiu būdu užtikrinama, kad pats pasirinkimo žingsnis būtų prieinamas skirtingoms naudotojų grupėms, o registracijos procesas iš karto adaptuojamas individualiems poreikiams. Pasirinkus autentifikavimo metodą, prasideda jo paruošimo procesas, kuris plačiau pavaizduotas (žr. **2 pav.** Naujo naudotojo konfiguracija).



2 pav. Naujo naudotojo konfiguracija

- Jei pasirinktas balsas, vartotojui pateikiama užduotis ištarti frazę ar skaičių seką, kurie naudojami balso pavyzdžiui sukurti. Sistema sugeneruoja balso reprezentaciją ir ją išsaugo įrenginio vidinėje saugykloje.
- Jei registruojamas gestais pagrįstas lytėjimo autentifikavimas, naudotojas atlieka nustatytą perbraukimų seką jutikliniame ekrane. Sistema kiekvieną perbraukimą interpretuoja kaip vieną iš keturių krypčių – aukštyn, žemyn, kairėn arba dešinėn. Iš šių veiksmų sekos suformuojamas autentifikavimo šablonas.
- Jei pasirenkamas vienkartinis slaptažodis (*OTP*), naudotojas susieja aplikaciją su savo telefono numeriu, kad prireikus skambučiu ar žinute galėtų gauti atsarginį prisijungimo kodą.
- Jei registruojamas biometrinis autentifikavimas, naudotojas aktyvuoja išmaniajame įrenginyje jau prieinamą biometrinį metodą, pavyzdžiui, piršto atspaudo atpažinimą. Tokiu būdu autentifikavimo procesui panaudojamos pačiame įrenginyje integruotos saugumo priemonės.

Užregistravus visus keturis autentifikavimo būdus, naudotojas nustato jų asmeninę prioritetų eilę nuo 1 iki 4. Ši eilė parodo, kurie autentifikavimo būdai konkrečiam naudotojui yra priimtiniausi ir patogiausi kasdienio naudojimo metu. Tokiu būdu sistema įgyja pradinį autentifikavimo taikymo pagrindą, kuris vėliau gali būti koreguojamas atsižvelgiant į konkretų naudojimo kontekstą ir adaptyvumo taisykles.



3 pav. Autentifikavimo būdų prioritetų nustatymas

Įvykdžius kiekvieną iš konfiguracijos parinkčių. Surinkti duomenys yra šifruojami ir saugomi naudotojo įrenginyje. Tokiu atveju nekyla poreikis naudoti jokio centralizuoto serverio. Tokiu būdu sumažinama rizika, kad asmeninė informacija bus nutekinta ir užtikrinamas asmens duomenų apsaugos reikalavimų laikymasis. Baigus šį procesą, sistema patvirtina, kad registracija sėkmingai įvykdyta ir pateiks naudotojui trumpą pranešimą (garsinį signalą, vizualų langą ar haptinį vibracijos impulsą). Nuo šiol visi užregistruoti autentifikavimo būdai gali būti naudojami kasdienio autentifikavimo metu, o jų taikymo seka gali būti pritaikoma pagal situaciją.

2.3.2. Įprastas naudojimas

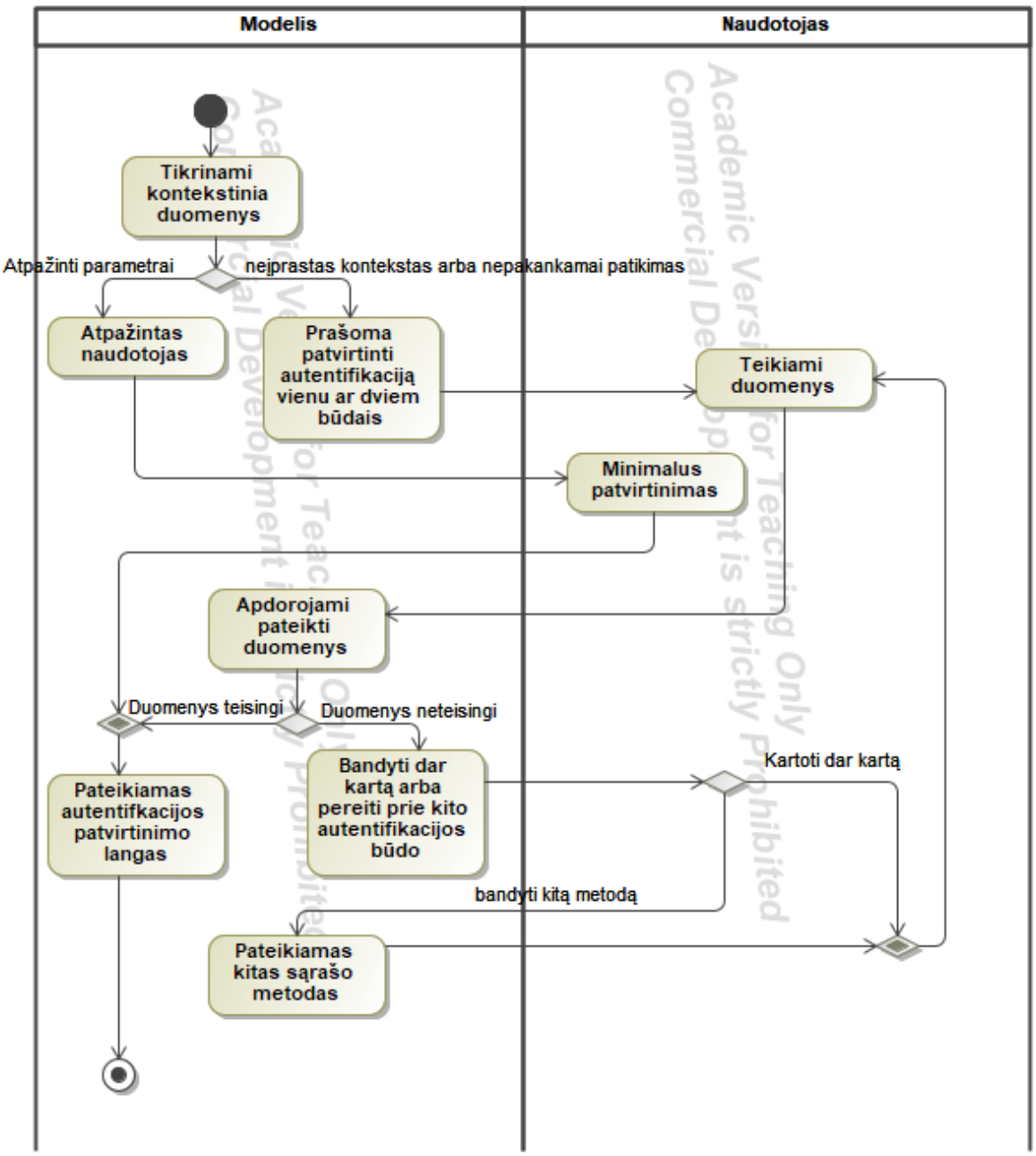
Kai naudotojas yra įvykdęs pradinę konfiguraciją, aplikacija tampa pagrindiniu įrankiu autentifikacijai kasdienėse situacijose. Kiekvieno prisijungimo metu sistema surenka kontekstinius duomenis, reikalingus pasyviam vertinimui. Prisijungimo metu matomas vertinamas „Wi-Fi“ tinklo identifikatorius (*SSID*) ir autentifikavimo laikas. Šie duomenys

leidžia sistemai įvertinti, ar esama situacija atitinka naudotojui būdingą prisijungimo kontekstą.

Per pasikartojančius naudojimus sistema palaipsniui formuoja naudotojo įprasto elgesio profilį. Jei prisijungimo kontekstas atitinka anksčiau susiformavusius dėsningumus, autentifikavimo eiga gali būti laikoma mažesnės rizikos. Jei nustatomas didesnis nukrypimas nuo įprastų sąlygų, sistema autentifikavimo procesą vertina griežčiau. Tokiu būdu siekiama suderinti saugumą ir naudojimo paprastumą.

Kadangi naudotojas pradinės konfigūracijos metu užregistruoja visus keturis autentifikavimo būdus, kasdienio naudojimo metu sistema gali remtis iš anksto nustatyta jų prioritetų eile. Pirmiausia siūlomas aukščiausią prioritetą turintis metodas. Tačiau ši seka nėra visiškai statiška. Atsižvelgdama į konkretų kontekstą, sistema gali laikinai praleisti tam tikrą metodą arba pakeisti jo taikymo eiliškumą, jei jis duotoju momentu tampa nepasiekiamas. Tokia logika leidžia išlaikyti autentifikavimo procesą lankstų ir pritaikomą realioms naudojimo sąlygoms.

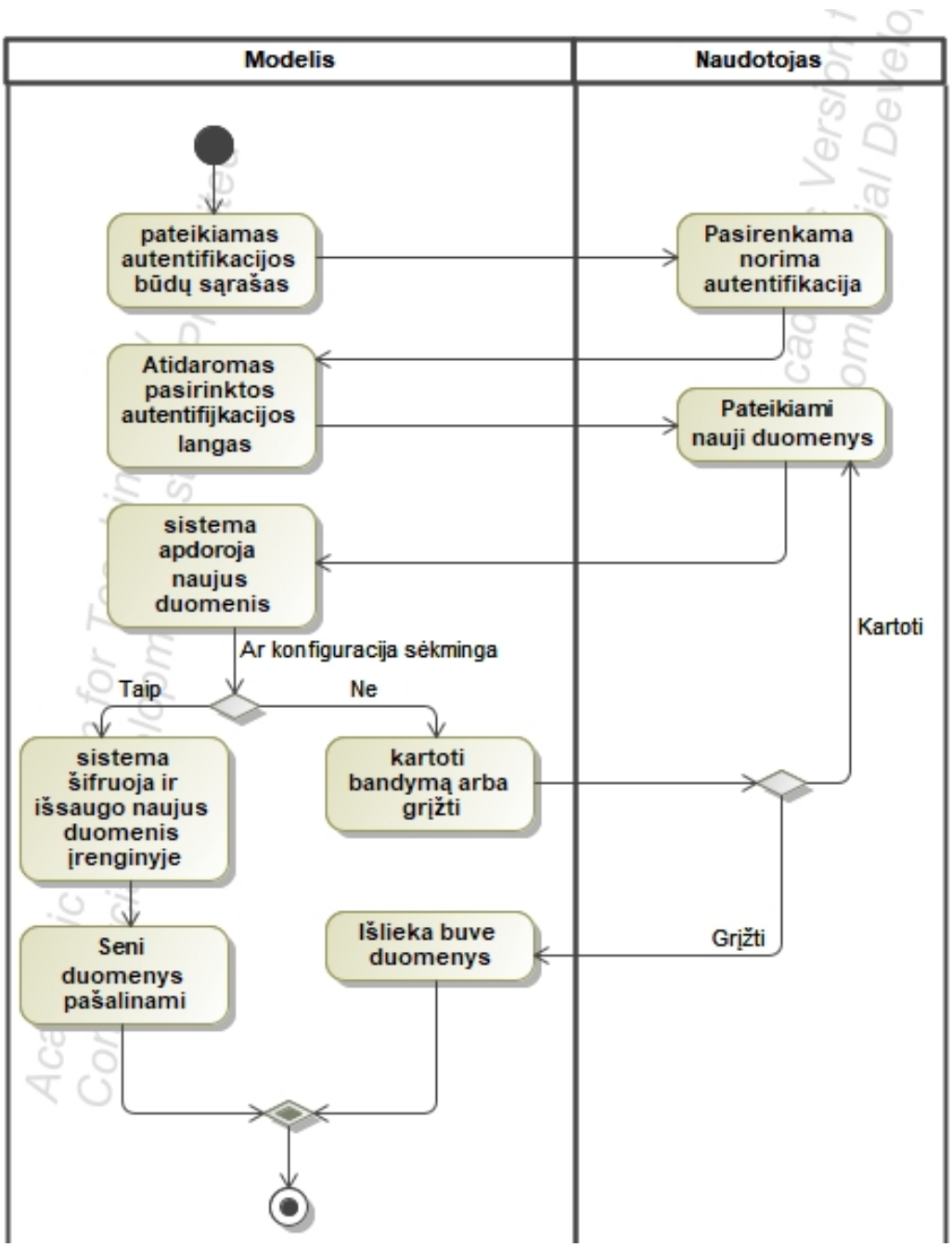
Jei pasirinktas autentifikavimo būdas nesuveikia arba negali būti panaudotas konkrečioje situacijoje, sistema pereina prie kitos galimos autentifikavimo alternatyvos pagal nustatytą arba adaptyviai pakoreguotą prioritetų seką. Tokiu būdu sumažinama rizika, kad naudotojas negalės prisijungti dėl vieno metodo ribotumo. Įprasto naudojimo schema pavaizduota (žr. **4 pav.** Įparastas naudojimas).



4 pav. Įparastas naudojimas

Siekiant išlaikyti sistemos prieinamumą, naudotojui suteikiama galimybė bet kuriuo metu po pradinės konfiguracijos, keisti pagrindinį ar atsarginį autentifikacijos metodą. Aplikacijoje pateikiama nustatymų sritis, kurioje galima inicijuoti naują balso pavyzdžio įrašymą, pakartotinį gestų sekos sudarymą, „OTP“ nustatymų atnaujinimą arba biometrinio būdo pakartotinį susiejimą. Tokia funkcija ypač svarbi tais atvejais, kai keičiasi naudotojo įpročiai, techninės sąlygos ar anksčiau užregistruotas metodas tampa mažiau patogus.

Visi atnaujinti duomenys saugomi vietoje, įrenginio saugykloje, laikantis tų pačių šifravimo ir duomenų apsaugos principų. Sėkmingai atnaujinus konkretų autentifikavimo būdą, ankstesni su juo susiję duomenys gali būti pakeičiami naujais. Nesėkmės atveju naudotojui suteikiama galimybė pakartoti veiksmą. Konfigūracijos keitimo schema pavaizduota (žr. **5 pav.** Konfiguracijos ketimo schema).



5 pav. Konfiguracijos ketimo schema

2.3.3. Adaptyvumas ir rizikos vertinimas

Siekiant padidinti modelio prieinamumą ir sumažinti nereikalingus autentifikavimo veiksmus, aplikacijoje bus taikomas adaptyvumo principas. Tai reiškia, kad autentifikavimo sprendimai priimami atsižvelgiant į kontekstinius veiksnius – laiką, „Wi-Fi“ tinklo identifikatorių (*SSID*). Tokiu būdu modelis gebės dinamiškai reguliuoti autentifikacijos saugumo lygį pagal esamą situaciją: surinkus pakankamai duomenų, kad būtų suformuotas naudotojo modelis bus taikomas tik minimalus patvirtinimo veiksmas, o padidėjus rizikai, autentifikacijai vykstant nebudingomis sąlygomis – aktyvuojamas pilnas autentifikavimo procesas. Taip išlaikant pusiausvyrą tarp saugumo ir prieinamumo.

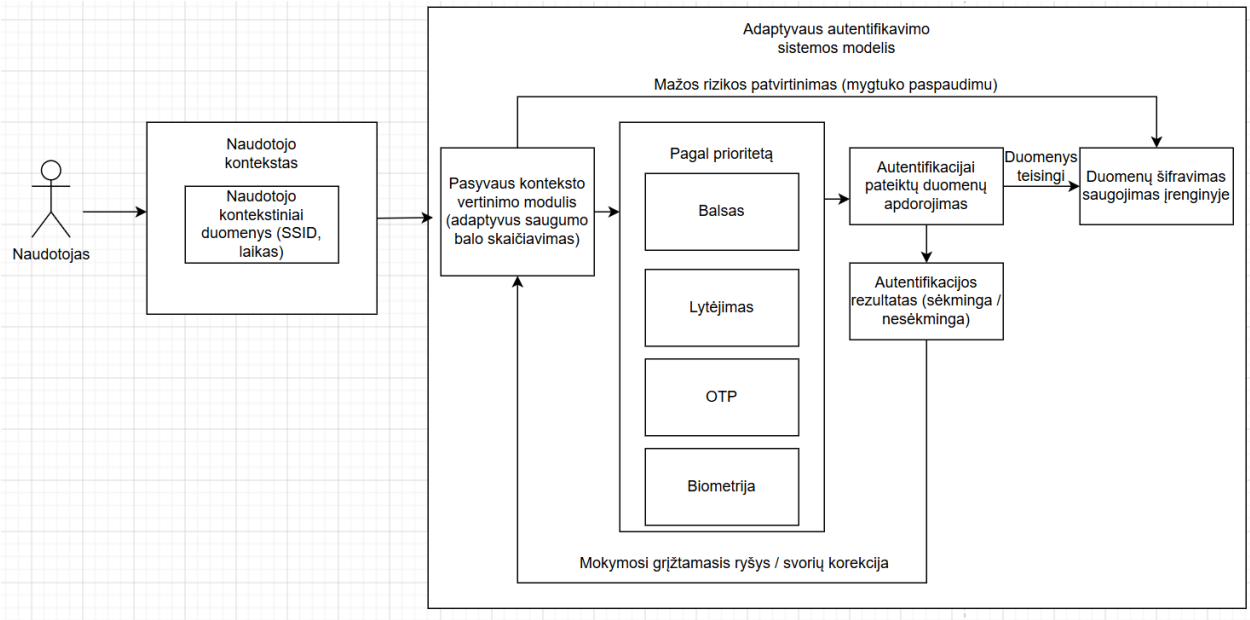
Pradiniame etape sistema kaupia duomenis apie naudotojo prisijungimo aplinkybes ir formuoja pradinį konteksto profilį. Šiuo laikotarpiu adaptyvus vertinimas dar tik mokosi naudotojo įpročių, todėl autentifikavimo eiga negali būti grindžiama vien pasyviais požymiais, laikomasi „Zero-trust“ politikos. Sukaupus daugiau pasikartojančių prisijungimo duomenų, susiformavus naudotojo profiliui, modelis gali tiksliau įvertinti, ar konkretus prisijungimo bandymas atitinka įprastą naudotojo elgseną.

Jei prisijungimo kontekstas atitinka anksčiau susiformavusį profilį, sistema tokį prisijungimą vertina kaip labiau tikėtiną ir gali taikyti paprastesnę autentifikavimo eigą arba netaikyti išvis. Jei kontekstas nuo įprastų sąlygų skiriasi, tokio prisijungimo pasitikėjimas mažėja, todėl sistema gali taikyti greižtensį autentifikavimą. Tokiu būdu adaptyvumas padeda sumažinti nereikalingą autentifikavimo apkrovą įprastose situacijose, kartu išlaikant griežtesnę kontrolę tada, kai prisijungimo aplinkybės tampa mažiau įprastos.

Svarbu ir tai, kad naudotojo elgsena laikui bėgant gali keistis. Dėl šios priežasties modelyje turi būti numatytas prisitaikymas prie naujų naudojimo įpročių. Anksčiau sukauptų kontekstinių požymių reikšmių svoris neturi išlikti nekintamas neribotą laiką, todėl sistema turi palaipsniui daugiau reikšmės teikti naujesniems prisijungimo duomenims. Tai leidžia išlaikyti adaptyvumo mechanizmą aktualų ir geriau atspindintį dabartinį naudotojo elgesį.

2.3.4. Konceptuali sistemos architektūra ir veikimo schema

Apibendrinant anksčiau aptartus autentifikavimo proceso etapus ir adaptyvaus veikimo principus, pateikiama konceptuali adaptyvaus autentifikavimo modelio architektūra (žr. **6 pav.** Adaptyvaus autentifikavimo sistemos modelio konceptuali architektūra). Paveikslėlyje matoma, kaip naudotojo konteksto duomenys integruojami į rizikos vertinimo modulį, kuris kaip šliuzas, remdamasis apskaičiuotu saugumo balu, valdo autentifikacijos procesą, bei jo pralaidumą. Modelis taip pat apima grįžtamojo mokymosi ryšį, leidžiantį sistemai koreguoti savo veikimą pagal ankstesnių autentifikacijų rezultatus ir taip palaipsniui prisitaikyti prie naudotojo elgsenos.



6 pav. Adaptyvaus autentifikavimo sistemos modelio konceptuali architektūra

Naudotojo kontekstas šiame modelyje apima pagrindinius pasyvius požymius – prisijungimo metu matomą tinklo identifikatorių (*SSID*) ir autentifikavimo laiką. Šie duomenys perduodami adaptyvaus vertinimo moduliui, kuris įvertina, kiek konkretus prisijungimo bandymas atitinka anksčiau susiformavusį naudotojo konteksto profilį. Jei rizika vertinama kaip minimali, naudotojui gali pakakti tik paprasto patvirtinimo veiksmo, pavyzdžiui, mygtuko paspaudimo.

Jei prisijungimo situacija nėra vertinama kaip minimali, sistema remiasi naudotojo nustatyta autentifikavimo būdų prioritetų eile. Kadangi naudotojas yra užregistravęs keturis autentifikavimo būdus – balsą, gestais pagrįstą lytėjimo būdą, „OTP“ ir biometrinį metodą, sistema gali pradėti autentifikavimą nuo aukščiausią prioritetą turinčio būdo. Naudotojo nustatyta prioritetų eilė sistemoje naudojama kaip pradinės gairės, tačiau ji nėra taikoma griežtai. Atsižvelgiant į esamą kontekstą, sistema gali pasiūlyti kitą tuo metu tinkamesnį autentifikavimo būdą, o pats naudotojas taip pat gali pasirinkti kitą jam patogesnę alternatyvą. Tokiu būdu autentifikavimo eiga tampa lankstesnė ir geriau pritaikoma realioms naudojimo sąlygoms.

Autentifikacijai pateikti duomenys yra apdorojami ir palyginami su anksčiau užregistruotais duomenimis ar nustatytais autentifikavimo parametrais. Jei autentifikavimas sėkmingas, atitinkami duomenys užšifruojami ir saugomi naudotojo įrenginyje. Lokalus duomenų saugojimas padidina sistemos privatumą ir sumažina centralizuoto jautrių duomenų kaupimo poreikį. Po kiekvienos autentifikacijos rizikos vertinimo modulis gauna grįžtamąjį ryšį apie proceso sėkmę ar nesėkmę, kas leidžia koreguoti modelio svorius ir palaipsniui gerinti autentifikavimo adaptyvumą.

2.4. Išvados

1. Idetifikavus analizės dalyje nagrinėtų įvairių negalių turinčių naudotojų poreikius nustatyta, kad efektyviausias autentifikavimo modelis turi būti daugialypis ir leisti pasirinkti tinkamiausią metodą pagal individualius gebėjimus bei kontekstą. Todėl modelyje integruoti keturi autentifikavimo būdai: balsas, gestais pagrįstas lytėjimo būdas, vienkartinis slaptažodis (*OTP*) ir biometrinis autentifikavimas.
2. Siekiant suderinti prieinamumą ir saugumą, modelyje nuspręsta taikyti adaptyvų pasyvaus konteksto vertinimą. Šiam vertinimui naudojami prisijungimo metu fiksuojami kontekstiniai požymiai, tokie kaip tinklo identifikatorius (*SSID*) ir autentifikavimo laikas, leidžiantys sistemai įvertinti prisijungimo situacijos atitikimą įprastam naudotojo elgesio profiliui.
3. Vertinant autentifikacijos modelio prieinamumo ir saugumo balansą, priimtas sprendimas įtraukti automatinio patvirtinimo mechanizmą mažos rizikos situacijoms, taip sumažinant nereikalingų autentifikavimo veiksmų skaičių.
4. Atsižvelgiant į sistemos poreikį mokytis iš naudotojo elgsenos, modelyje integruotas grįžtamojo mokymosi mechanizmas, kuris leidžia koreguoti rizikos vertinimo svorius pagal ankstesnius prisijungimus ir didinti autentifikacijos modelio adaptyvumą.
5. Dėl skirtingų aplinkos sąlygų (aplinkos triukšmo, ryšio, biometrinių įrenginių veikimo) kai kurie autentifikavimo metodai gali tapti laikinai neprieinami, todėl nuspręsta, kad kiekvienas naudotojas turi būti užregistravęs visus minėtus autentifikacijos būdus. Tokiu būdu sumažinama rizika, kad naudotojas praras prieigą prie sistemos dėl vieno metodo ribotumo.

3. Adaptyvios autentifikacijos modelio protoptipas

Identifikavus teorinius autentifikavimo modelio reikalavimus ir veikimo principus, šiame etape siekiama parodyti, kaip anksčiau apibrėžti aspektai – daugialypiškumas, adaptyvumas, prieinamumas ir privatumas – gali būti įgyvendinti praktikoje, pasitelkiant išmaniojo įrenginio esamą funkcionalumą.

Kuriant prototipą ypatingas dėmesys skiriamas keturiems autentifikavimo metodams: balso, gestais pagrįstam lytėjimo, biometriniam (*piršto atspaudo*) bei vienkartinio slaptažodžio (*OTP*) autentifikavimui. Visi šie būdai sujungiami į vieningą adaptyvų modelį, kuriame autentifikacijos kelias parenkamas automatiškai, atsižvelgiant į vartotojo kontekstą ir aplinkos sąlygas. Tokia realizacija naudoja aktyvų ir pasyvų adaptyvumą. Aktyvus adaptyvumas veikia realiuoju laiku – stebi aplinkos pokyčius (t*riukšmą, tinklo būklę, jutiklių prieinamumą*) ir dinamiškai keičia leidžiamus autentifikavimo metodus. Pasyvus adaptyvumas ilgainiui kaupia informaciją apie vartotojo elgseną ir automatiškai koreguoja rizikos vertinimo ribas, užtikrindamas pusiausvyrą tarp saugumo bei prieinamumo.

3.1. Technologinės realizacijos pasirinkimai

Siekiant šių tikslų, sistemos prototipas kuriamas kaip Android operacinėje sistemoje veikianti mobili aplikacija. Ši platforma pasirinkta dėl kelių priežasčių. Tokia aplinka leidžia pasinaudoti plačiu prieinamų jutiklių ir paslaugų spektru: mikrofonu, biometriniais moduliais, haptiniu grįžtamuoju ryšiu, vietos nustatymo ir tinklo prieigos funkcijomis. Tai leidžia pritaikyti aplikaciją regos, disleksijos ar motorikos sutrikimų turintiems asmenims be papildomų įrenginių.

Kita svarbi priežastis – „Android“ suteikiama galimybė naudoti biometrinius autentifikacijos įrankius, tokius kaip „BiometricPrompt API“, kuri palaiko piršto atspaudų. Tai leidžia realizuoti biometrinį autentifikavimo būdą, kuris ypač tinkamas naudotojams, turintiems motorikos ar regos sutrikimų, nes užtenka vieno lietimo ar įrenginio atpažinimo veiksmų.

Be pačios platformos pasirinkimo, itin svarbi yra patikimų bibliotekų ir „API“ ekosistema, užtikrinanti autentifikavimo sprendimų patikimumą ir veikimo stabilumą. Kiekvienam numatytam metodui pasitelkiami atitinkami technologiniai sprendimai:

- Balso autentifikavimui – naudojama, lokaliai įrenginyje veikianti sistema. Kalbos turinio atpažinimui pasitelkiama „Vosk“ biblioteka, atliekanti kalbos ir frazių atpažinimą be interneto ryšio. Modelis generuoja atsitiktinę skaitmenų seką, kurią naudotojas turi ištarti balsu, taip užtikrinant apsaugą nuo įrašyto balso atkūrimo (*angl. replay attack*). Be ištartos frazės turinio patikros, įgyvendintas ir kalbėtojo tapatybės patvirtinimas, paremtas mašininio mokymo modeliu. Tam naudojamas jau apmokytas „TensorFlow Lite“ pagrindu integruotas kalbėtojo atpažinimo modelis, kuris balsą paverčia į skaitmeninį požymių vektorių (*angl. voice embedding*). Autentifikacijos metu sugeneruotas vektorius lyginamas su balso registracijos metu išsaugotu šablonu, apskaičiuojant kosinuso panašumo reikšmę. Balso šablonų apsaugai naudojamas „Google Tink“ karkasas, realizuojantis AES-GCM šifravimą, o šifravimo raktai valdomi per „Android

Keystore“. Tokiu būdu biometriniai duomenys saugomi lokaliai įrenginyje ir nėra laikomi atviru, tiesiogiai perskaitomu pavidalu.

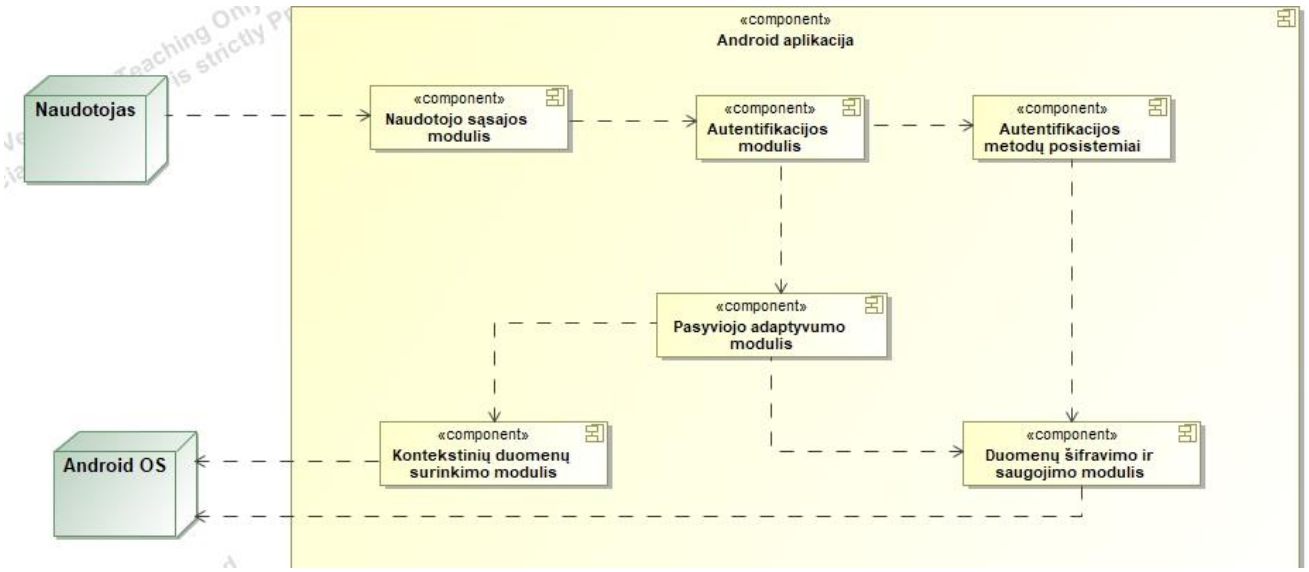
- Gestų ir lytėjimo autentifikacijai naudojami „GestureDetector“ bei „HapticFeedbackConstants“ moduliai, leidžiantys kurti prieinamas sąsajas su dideliais valdymo elementais ir haptiniais signalais. Vietoj tradicinių tekstinių slaptažodžių naudojama normalizuota braukimo krypčių seka (aukštyn, žemyn, kairėn, dešinėn), kuri naudojama autentifikavimo šablono sudarymui. Gestų duomenys saugomi lokaliai, naudojant „Jetpack DataStore“ kartu su „Google Tink“ kriptografijos karkasu, o šifravimo raktai valdomi per „Android Keystore“, užtikrinant duomenų konfidencialumą.
- Biometrijai – „BiometricPrompt API“, užtikrinanti integraciją su operacinės sistemos saugumo infrastruktūra ir leidžianti naudoti tik sertifikuotus biometrinius modulius.
- Vienkartiniams slaptažodžiams (*OTP*) – realizuotas lokalus, įrenginyje veikiantis kodo generavimo ir tikrinimo mechanizmas, kuris imituoja realų „SMS“ patvirtinimo kodo gavimo scenarijų. Prototipe įgyvendinta automatinio kodo užpildymo (*autofill*) simuliacija, siekiant sumažinti naudotojo kognityvinę ir motorinę apkrovą.

Šių technologijų derinys leidžia sukurti sistemą, kuri yra tiek funkcionaliai lanksti, tiek pritaikoma individualiems poreikiams. Tokiu būdu realizuojami ne tik teoriniai adaptyvumo principai, bet ir prieinamumo bei duomenų privatumo reikalavimai, iškelti ankstesniuose projekto etapuose.

3.2. Architektūros schema ir moduliai

Kuriant adaptyvios autentifikacijos modulį, architektūra suprojektuota modulinės struktūros principu. Kiekvienas komponentas atlieka aiškiai apibrėžtą funkciją, tačiau veikia vieningoje valdymo grandinėje. Tokia architektūra leidžia leidžia lengvai tobulinti ir keisti atskirus komponentus nepaveikiant visos modulio logikos.

Modelio architektūra apima šiuos pagrindinius modulius matomus (žr. **7 pav.** Kontekstinė architektūros scehma):



7 pav. Kontekstinė architektūros scehma

1. **Naudotojo sąsajos modulis** – užtikrina sąveiką tarp naudotojo ir sistemos. Sukurtas naudojant Jetpack Compose, modulis palaiko vizualinį, garsinį ir haptinį grįžtamąjį ryšį. Jo tikslas – suteikti prieinamą autentifikavimo patirtį regos, disleksijos ar motorikos sutrikimų turintiems asmenims.
2. **Kontekstinių duomenų surinkimo modulis** – atsakingas už naudotojo aplinkos duomenų (laiko, vietos, tinklo, triukšmo) surinkimą. Šie duomenys perduodami rizikos vertinimo moduliui ir naudojami adaptyvumo sprendimams priimti. Tokiu būdu įgyvendinamas aktyvusis adaptyvumas, leidžiantis sistemai realiu laiku reaguoti į aplinkos pokyčius (pvz., triukšmą, ryšio nebuvimą ar biometrinio jutiklio klaidas).
3. **Pasyviojo adaptyvumo modulis** – šis modulis analizuoja surinktus kontekstinius duomenis ir apskaičiuoja autentifikacijos situacijos rizikos balą, taikydamas euristinį svorinį vertinimą. Kiekvienas kontekstinis signalas, įprastas laikas, pažįstamas tinklas ar saugumo anomalijos turi įtaką bendram rizikos lygiui. Pagal apskaičiuotą balą autentifikacijos situacija priskiriama vienai iš trijų būsenų – mažos, padidintos arba aukštos rizikos.
4. **Autentifikacijos modulis** – tai pagrindinis sprendimų priėmimo centras, kuris, remdamasis rizikos vertinimo modulio pateiktu balu, nustato reikiamą autentifikacijos griežtumą. Mažos rizikos atvejais gali būti taikomas automatinis patvirtinimas, o esant padidintai ar aukštai rizikai – aktyvuojami papildomi autentifikacijos metodai. Šiame modulyje taip pat realizuojamas pasyvusis adaptyvumas, kai sistema palaipsniui mokosi iš naudotojo elgsenos istorijos ir koreguoja rizikos vertinimo logiką laikui bėgant.
5. **Autentifikacijos metodų posistemiai**
    1) Balso autentifikavimas
    2) Lytėjimo autentifikavimas
    3) Biometrinis autentifikavimas
    4) Vienkartinis slaptažodis (*OTP*)
6. **Duomenų šifravimo ir saugojimo modulis** – visi jautrūs naudotojo duomenys, įskaitant autentifikacijos šablonus ir istorinius prisijungimo įvykius, yra šifruojami ir

saugomi tik lokaliai įrenginyje, naudojant „Google Tink“ kriptografijos karkasą. Tokiu būdu užtikrinama, kad asmens duomenys nėra perduodami į išorinius serverius ir laikomasi privatumo principų.

3.3. Autentifikavimo metodų realizacija

3.3.1. Balso autentifikavimo realizacija

Balso autentifikavimas realizuojamas kaip dviejų lygių procesas, kuriame vienu metu tikrinamas ir ištartos frazės turinys ir kalbėtojo tapatybė. Tai leidžia sumažinti atakų tikimybę, kai kitas asmuo bando pakartoti autentifikavimo frazę arba panaudoti įrašytą naudotojo balsą.

Įrašymo metu garsas fiksuojamas naudojant „AudioRecord API“, apdorojamas 16 kHz dažniu ir perduodamas balso atpažinimo posistemiui. Toks dažnis pasirinktas todėl, kad jo pakanka žmogaus kalbos analizei ir tuo pačiu sumažina procesoriaus apkrovą mobiliuose įrenginiuose.

Prieš pradedant vartotojo balso įrašymą, modelis (2s.) įvertina aplinkos foninį triukšmą, pasitelkdama „AudioRecord API“ ir „RMS“ (*root-mean-square*) garso energijos matavimą. Kadangi bangų formos nuolat kinta per tam tikrą laiką, negalima tiesiog išmatuoti įtampos vienu metu. „RMS“ išsprendžia šią problemą, apskaičiuodamas visų bangų formos verčių vidurkį per nustatytą laikotarpį. Ši analizė atliekama dar prieš vartotojui pradedant kalbėti, todėl pats vartotojo balsas negali klaidingai padidinti triukšmo rodmens. Jei foninis triukšmas viršija nustatytą ribą, balso autentifikavimo metodas automatiškai išjungiamas ir sistema parenka kitą autentifikacijos kelią.

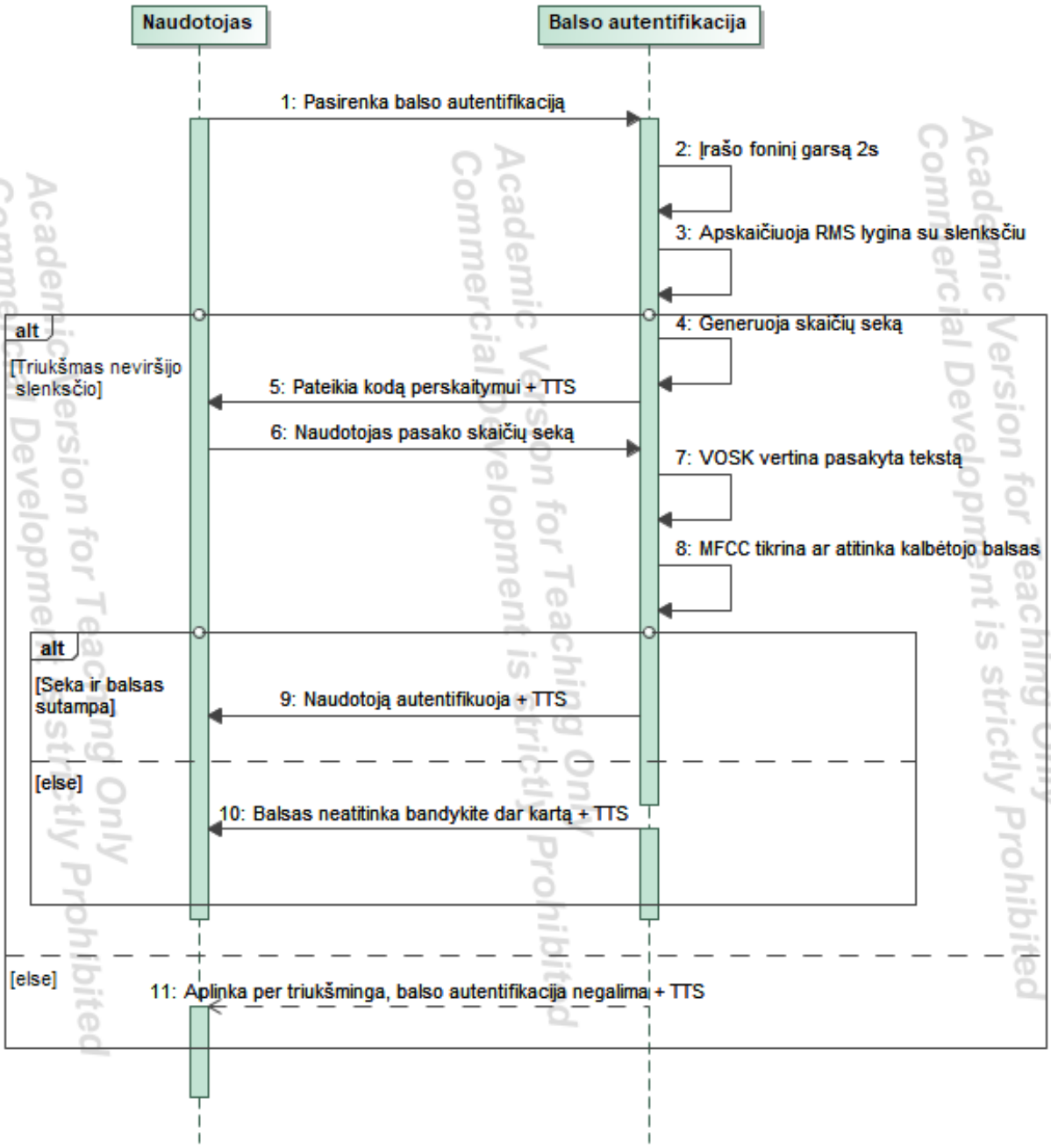
Kai aplinkos sąlygos leidžia naudoti balsu paremta autentifikacija. Autentifikacijos frazės atpažinimui naudojama „Vosk“ biblioteka**,** veikianti lokaliai įrenginyje ir nereikalaujanti interneto ryšio. Autentifikacijos metu vartotojui pateikiama dinamiškai sugeneruota skaitmenų seka (*pvz., „du keturi šeši aštuoni“*), kurią jis turi pakartoti balsu. „Vosk“ modelis atpažįsta ištartą tekstą ir patikrina, ar jis sutampa su sistemos pateiktu iššūkiu.

Tuo pačiu metu balso signalas perduodamas į kalbėtojo atpažinimo modulį, paremtą apmokytu mašininio mokymo modeliu. Naudojamas „TensorFlow Lite“ pagrindu integruotas kalbėtojo kodavimo modelis, kuris įrašytą garsą paverčia skaitmeniniu požymių vektoriumi (*angl. voice embedding*), atspindinčiu individualias kalbėtojo balso savybes. Registracijos metu suformuotas kalbėtojo šablonas saugomas įrenginyje užšifruotu pavidalu.

Autentifikacijos metu naujai sugeneruotas balso požymių vektorius lyginamas su išsaugotu šablonu, apskaičiuojant kosinusinį panašumą tarp jų. Jei ši reikšmė viršija nustatytą slenkstį ir „Vosk“ atpažintas tekstas sutampa su sistemos sugeneruota seka, vartotojo tapatybė patvirtinama sėkmingai.

Tokiu būdu balso autentifikavimas veikia kaip „du viename“ mechanizmas: turinio patikra užtikrina, kad ištarta teisinga frazė, o balso šablono palyginimas patvirtina, kad frazę ištarė

originalus kalbėtojas detalesnis autentifikavimo proceso veikimas pavaizduotas sekų diagramoje (žr. **8 pav.** Autentifikavimasis balsu sekos diagrama).



8 pav. Autentifikavimasis balsu sekos diagrama

Kadangi visi skaičiavimai kalbos atpažinimas, balso požymių vektoriaus generavimas ir šablonų palyginimas vykdomi lokaliai įrenginyje, o balso šablonai saugomi užšifruotu pavidalu, užtikrinamas naudotojo duomenų privatumas ir atitiktis ankstesniuose skyriuose aptartiems duomenų apsaugos reikalavimams.

3.3.2. Vienkartinio slaptažodžio (*OTP*) realizacija

Vienkartinio slaptažodžio (*OTP*) autentifikavimas sistemoje realizuotas kaip paprastas, lokaliai įrenginyje veikiantis mechanizmas, užtikrinantis alternatyvų tapatybės patvirtinimo būdą. Aplikacija lokaliai sugeneruoja atsitiktinį šešių skaitmenų kodą (*pvz., 000000–*

999999) naudodama atsitiktinių skaičių generatorių. Kiekvienam sugeneruotam kodui priskiriamas galiojimo laikas, 120 sekundžių. Tai užtikrina, kad tas pats kodas negalėtų būti panaudotas pakartotinai, o laikinumas padidina bendrą sistemos saugumą.

Taip pat pridedamas „OTP“ metodo supaprastintas pseudokodas, norint pabrėžti esminę logiką (žr. **9 pav.** OTP pseudo kodas).

```
function generateOtp():
    code = randomInt(000000, 999999)        // 6 skaitmenų kodas
    ttl  = currentTime() + 120 seconds      // galioja 120 s

    storeHashedCode(hash(code))            // saugome tik hešuotą kodą
    storeExpiry(ttl)

    showCodeOnScreen(code)                 // parodyti ekrane
    speakCodeWithTts(code)                 // perskaityti balsu (TTS)
    vibrateShort()            // haptinis signalas, kad kodas sukurtas


// Naudotojo įvesties surinkimas (UI logika)
function onUserSubmit(inputCode):
    result = verifyOtp(inputCode)
    if result == "success":
        grantAccess()
    else if result == "expired":
        showMessage("Kodo galiojimo laikas pasibaigė")
    else:
        showMessage("Neteisingas kodas")


// Patikrinti įvestą kodą
function verifyOtp(inputCode):
    storedHash = loadHashedCode()
    ttl = loadExpiry()

    if currentTime() > ttl:
        return "expired"

    if hash(inputCode) == storedHash:
        return "success"
    else:
        return "invalid"
```

9 pav. OTP pseudo kodas

Siekiant užtikrinti universalią prieigą, „OTP“ autentifikavimo sąsaja pritaikyta kelioms negalių grupėms:

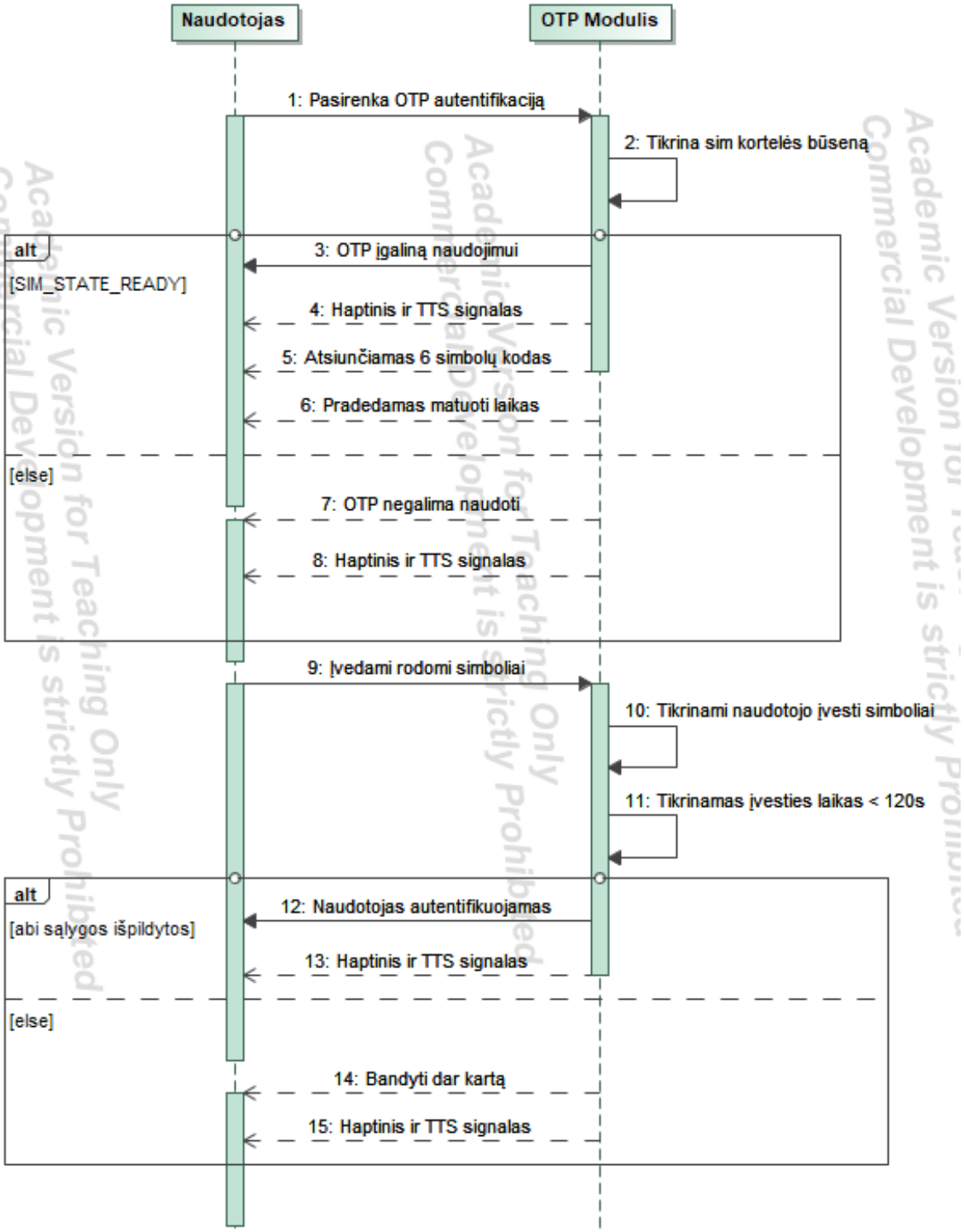
- TTS perskaitymas – kodas automatiškai perskaitomas balsu, kad nereikėtų skaityti ekrane.
- Didelio kontrasto elementai – padeda disleksiją turintiems naudotojams aiškiai suvokti skaitmenis.
- Haptinis signalas – trumpas vibracijos impulsas praneša apie naujo kodo generavimą vartotojams, turintiems regos ar motorikos sutrikimų.

Kadangi prototipe nėra įdiegtas išorinis „SMS“ kanalas, sukurta simuliacija, kuri imituoja realią „SMS“ autofill elgseną siekiant mažinti vartotojo kognityvinę ir motorinę apkrovą. Po kodo sugeneravimo aplikacija automatiškai užpildo patvirtinimo laukelį (*prefill*) ir informuoja naudotoją balso pranešimu (*TTS*) bei trumpu haptiniu impulsu. Tokia elgsena leidžia vartotojams su regos ar motorikos sutrikimais išvengti papildomų klaviatūros įvedimų. Tai yra prototipo sprendimas: produkcinėje aplinkoje autofill būtų realizuotas per „Android SMS autofill“ ar „SmsRetriever API“, kuris priima tik realiai gautus operatoriaus pranešimus. Prototipe vartotojui paliekama galimybė išjungti automatinį užpildymą ir rankiniu būdu įvesti pateiktą kodą.

Autentifikacija per lokalų „OTP“ laikoma sėkminga, jei:

- vartotojo įvestas kodas atitinka sugeneruotą reikšmę.
- kodo galiojimo laikas nepasibaigęs.

Prototipui šio darbo metu įgyvendintas lokalus vienkartinio slaptažodžio (*OTP*) mechanizmas, kuriame kodas generuojamas tiesiogiai matomas (žr. **10 pav.** OTP sekos diagrama). Nors šis sprendimas nėra skirtas realaus saugumo užtikrinimui, jis pilnai atlieka mokslinę funkciją – demonstruoja, kaip „OTP“ metodas gali būti įtrauktas į adaptyvios autentifikacijos ekosistemą kartu su kitais metodais.



10 pav. OTP sekos diagrama

3.3.3. Gestais pagrįsto lytėjimo autentifikavimo realizacija

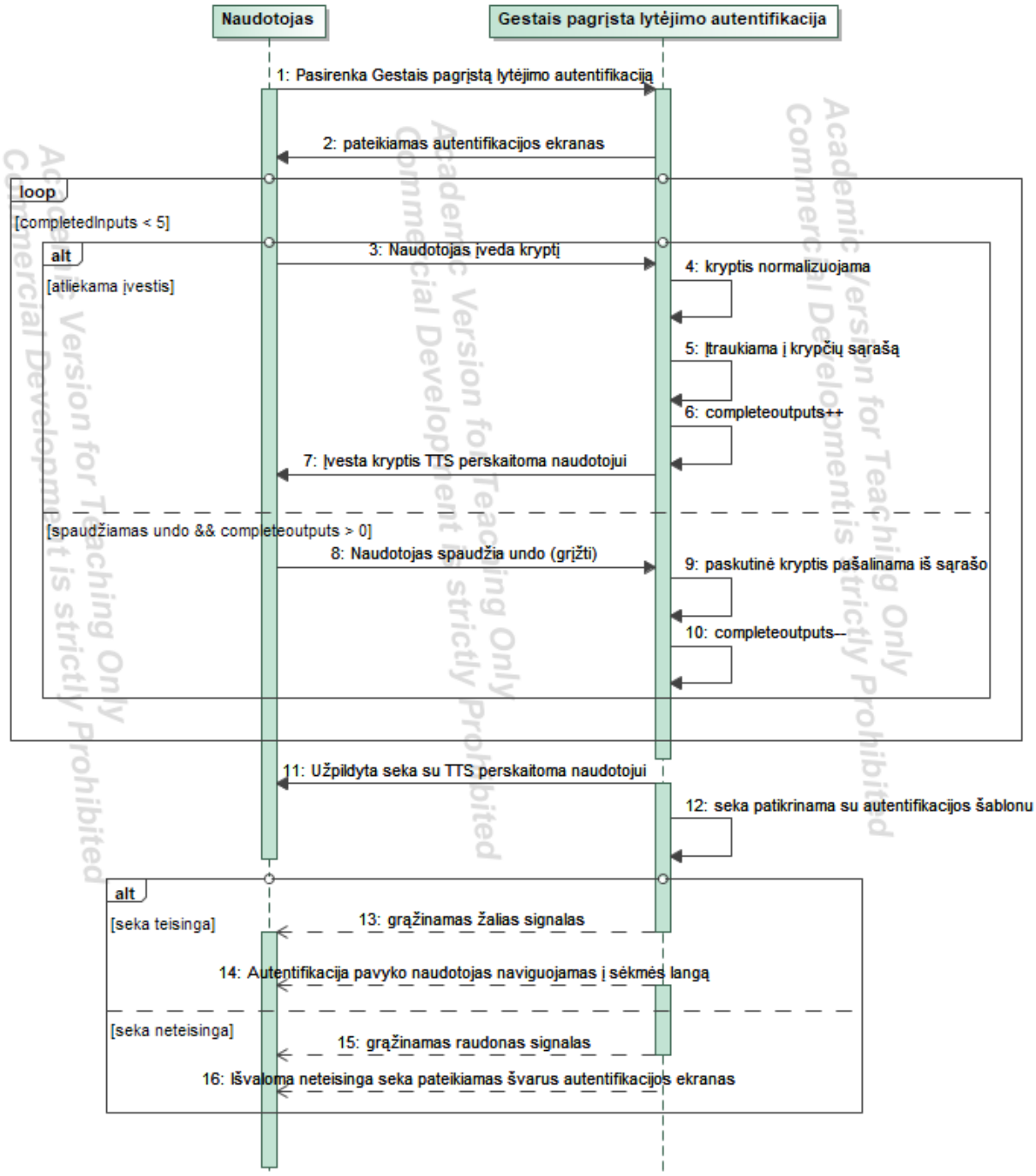
Gestais pagrįstas lytėjimo autentifikavimas prototipe realizuojamas kaip kryptinių braukimų seka. Šis metodas pasirinktas kaip alternatyvus autentifikavimo kanalas, nereikalaujantis išorinių jutiklių (*pvz., piršto atspaudo skaitytuvo*) ir nepriklausantis nuo interneto ryšio. Tokiu būdu jis išlieka prieinamas net tais atvejais, kai biometriniai sprendimai nėra pasiekiami, o balso autentifikavimas negali būti taikomas dėl triukšmingos aplinkos.

Naudotojo idetifikavimo šablonas apibrėžiamas kaip 5 braukimų seka. Kiekvienas braukimas priskiriamas vienai iš keturių galimų krypčių: į viršų, į apačią, į kairę arba į dešinę. Įvedimo metu vartotojo braukimas gali būti netikslus, įstrižas arba banguotas. Todėl prototipe taikomas normalizavimo principas: braukimo vektorius suapvalinamas iki artimiausios iš keturių pagrindinių krypčių. Toks sprendimas sumažina klaidų tikimybę ir padidina metodo toleranciją motoriniams netikslumams. Įvestis renkama žingsnis po žingsnio (*vienas braukimas = vienas simbolis*). Jei įvedimo metu padaroma klaida, naudotojas gali koreguoti paskutinį žingsnį paspausdamas „Undo / Grįžti“ mygtuką. Tai pagerina naudojimo patirtį, nes vartotojui nereikia iš naujo atlikti visos identifikavimo sekos vien dėl vienos neteisingos krypties.

Baigus suvesti visą 5 braukimų kombinaciją, sistema pateikia aiškų grįžtamąjį ryšį. Įvesta seka yra perskaitoma garsiai (*TTS*), kad vartotojas galėtų patvirtinti, jog sistema užfiksavo būtent tai, ką jis atliko. Papildomai pateikiamas vizualinis statuso indikatorius:

- žalias signalas nurodo, kad įvesta seka sutapo su išsaugotu šablonu.
- raudonas signalas informuoja apie neatitikimą ir leidžia vartotojui bandyti dar kartą.

Tokiu būdu gestų autentifikavimas įgyvendinamas kaip procesas, kuriame vartotojas gauna tiek vizualinį, tiek garsinį patvirtinimą. Šis sprendimas yra svarbus prieinamumo kontekste: vartotojai su regos sunkumais gali remtis garsiniu patvirtinimu, o vartotojai, kuriems reikalingas aiškus vizualinis indikatorius (pvz., disleksijos atveju), gauna paprastą spalvinį signalą be perteklinio teksto. Taip pat svarbu paminėti, kad šis autentifikavimo būdas nėra apribotas laiko limitu, todėl yra tinkamas naudotojams, turintiems motorikos sutrikimų. Šio metodo veikimas pavaizduotas sekų diagramoje (žr. **11 pav.** Gestais pagrįsto lytėjimo autentifikavimo sekos diagrama). Vertinant rezultatus, autentifikacija laikoma sėkminga, jei naudotojas įveda pilną 5 krypčių seką ir normalizuota įvesta seka sutampa su sistemoje išsaugotu šablonu. Sėkmingu atveju vartotojui užskaitoma autentifikacija ir sistema pereina prie prieigos suteikimo žingsnio. Nesėkmės atveju pateikiamas klaidos indikatorius ir leidžiama bandyti dar kartą.



11 pav. Gestais pagrįsto lytėjimo autentifikavimo sekos diagrama

Gestais pagrįsto lytėjimo autentifikavimo metu naudotojo braukimo seka nėra saugoma kaip tiesioginiai jutiklių duomenys ar vizualinė trajektorija. Kiekvienas braukimas normalizuojamas į vieną iš keturių galimų krypčių (*aukštyn, žemyn, kairėn, dešinėn*), kurios vidinėje sistemos logikoje koduojamos simboline seka. Šis koduotas šablonas saugomas lokaliai įrenginyje, naudojant užšifruotą duomenų saugojimo mechanizmą (*Encrypted DataStore*), paremtą „Android Keystore“ sugeneruotu kriptografiniu raktu. Toks sprendimas priimtas tam, kad net gavus prieigą prie įrenginio failų sistemos, autentifikavimo seka negalėtų būti atkurta ar interpretuota be konkretaus įrenginio kriptografinio rakto. Visi gestų autentifikavimo duomenys lieka tik naudotojo įrenginyje ir nėra perduodami į išorines sistemas, taip užtikrinant privatumo apsaugą ir atitiktį ankstesniuose skyriuose aptartiems duomenų saugumo reikalavimams.

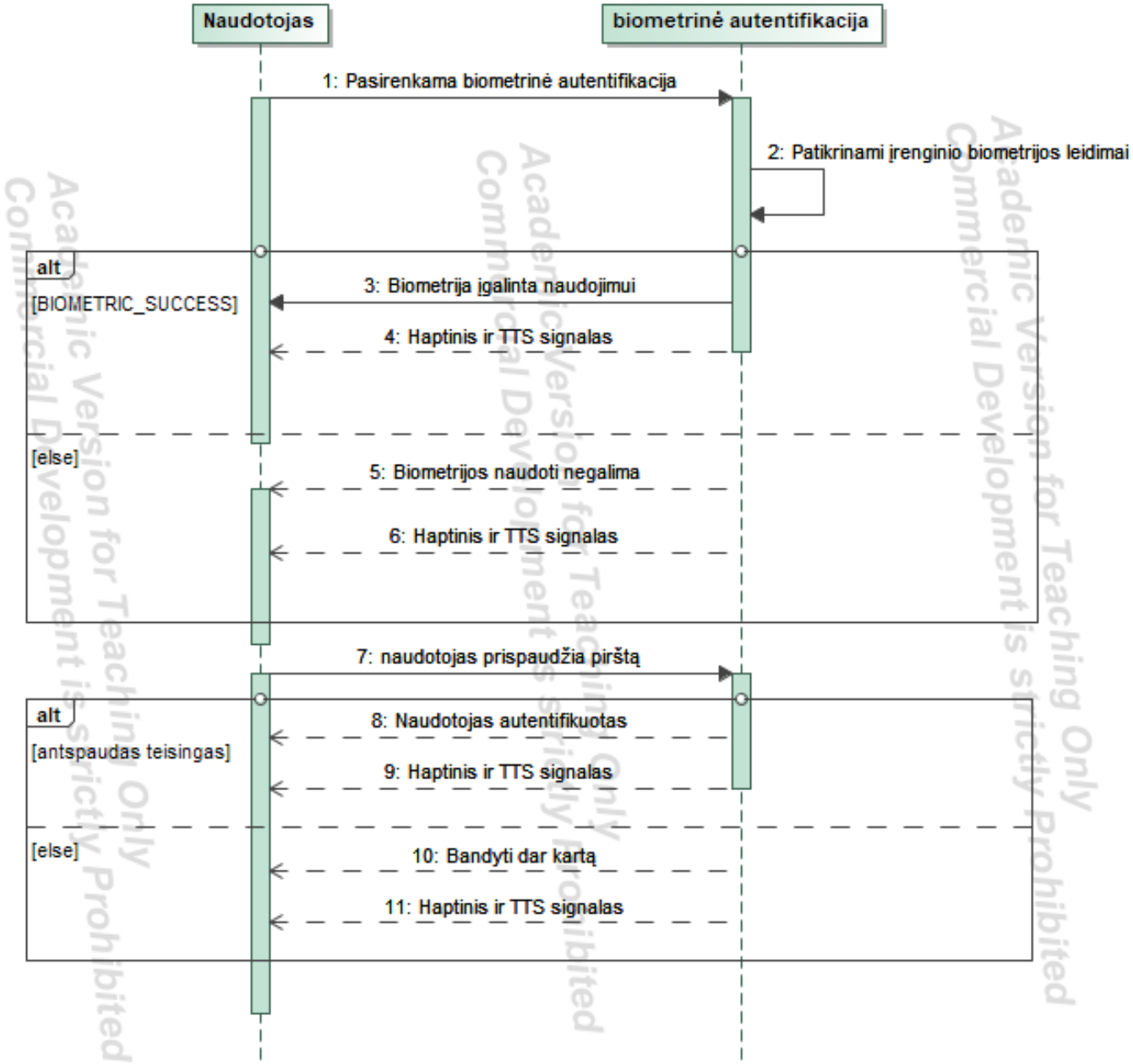
3.3.4. Biometrinės autentifikacijos realizacija

Biometrinė autentifikacija prototipe realizuota pasitelkiant „Android“ operacinės sistemos teikiamą „BiometricPrompt API“, kuri leidžia naudoti įrenginyje integruotus biometrinius jutiklius, tokius kaip piršto atspaudo ar veido atpažinimo moduliai. Šis metodas pasirinktas kaip vienas iš autentifikavimo būdų dėl aukšto saugumo lygio ir ypač geros prieigos naudotojams, turintiems motorikos ar regos sutrikimų, kadangi autentifikacijai pakanka vieno prisilietimo. Sukurta autentifikacijos aplikacija neturi tiesioginės prieigos prie naudotojo biometrinių duomenų. Visa biometrinių požymių analizė ir palyginimas atliekami operacinės sistemos lygmenyje, o aplikacija gauna tik autentifikacijos rezultatą, sėkmė arba nesėkmė. Tokiu būdu užtikrinamas sistemos vientisumas ir tai, kad jautrūs biometriniai duomenys niekada nepaliktų saugios sistemos aplinkos.

Prototipe naudojamas griežtas „BIOMETRIC_STRONG“ autentifikacijos reikalavimas, kuris leidžia priimti tik tuos biometrinius metodus, kurie atitinka aukštus saugumo kriterijus pagal klaidingo priėmimo (*FAR – False Acceptance Rate*) ir klaidingo atmetimo (*FRR – False Rejection Rate*) rodiklius. Tai reiškia, kad silpnesni ar mažiau patikimi biometriniai metodai automatiškai atmetami, o sistema remiasi tik sertifikuotais ir saugiais jutikliais.

Biometrinės autentifikacijos procesas vykdomas izoliuotoje aparatinėje aplinkoje, vadinamoje patikima vykdymo aplinka (*angl. Trusted Execution Environment, TEE*). Ši architektūra užtikrina, kad biometriniai raktai ir autentifikacijos logika būtų apsaugoti net ir tuo atveju, jei pati operacinė sistema būtų pažeista. Tokiu būdu biometrinė autentifikacija tampa vienu saugiausių kuriamo prototipo autentifikavimo metodų.

Naudotojo patirties požiūriu, biometrinė autentifikacija integruota su aiškiu grįžtamuoju ryšiu apie nesėkmingus bandymus (*pvz., neatpažintas pirštas ar laikinai nepasiekiamas jutiklis*). Tai leidžia naudotojui suprasti autentifikacijos būseną be sudėtingų tekstinių paaiškinimų, kas ypač svarbu kuriamo modelio prieinamumo atžvilgiu. Šio metodo veikimas pavaizduotas sekų diagramoje (žr. **12 pav.** Biometrija pagrįsta autentifikavimo sekos diagrama).



12 pav. Biometrija pagrįsta autentifikavimo sekos diagrama

Biometrinė autentifikacija prototipe realizuota kaip saugus, greitas ir prieinamas autentifikavimo būdas, kuris išnaudoja operacinės sistemos teikiamas saugumo garantijas ir natūraliai įsilieja į kuriamą adaptyvų autentifikacijos modelį.

3.4. Aktyvusis adaptyvumas

Aktyvusis adaptyvumas sistemoje užtikrina, kad autentifikavimo procesas prisitaikytų prie kintančių vartotojo aplinkos sąlygų realiuoju laiku. Šio principo esmė – dinamiškai parinkti tinkamiausią autentifikacijos metodą atsižvelgiant į kontekstinius signalus, tokius kaip triukšmo lygis, tinklo prieinamumas, įrenginio būsena ar jutiklių prieiga. Tokiu būdu išvengiama situacijų, kai naudotojui pateikiamas neveikiantis ar sunkiai naudojamas autentifikacijos būdas.

Kontekstinių duomenų surinkimo modulis kiekvieno autentifikacijos kvietimo metu stebi kelis realaus laiko kintančius parametrus:

- Aplinkos triukšmo lygį, nustatomą per mikrofono įvestį, pasitelkus „AudioRecord API“, įrašant trumpą (2s) garso atkarpą dar prieš vartotojui pradedant tarti autentifikavimo frazę. Signalo stiprumui nustatyti taikomas „RMS“ (*root-mean-square*) skaičiavimas nustato vidutinį energijos kiekį per tam tikrą laiką nuolat kintančio signalo atveju. Kadangi bangų formos nuolat kinta per tam tikrą laiką, negalima tiesiog išmatuoti įtampos vienu metu. „RMS“ išsprendžia šią problemą, apskaičiuodamas visų bangų formos verčių vidurkį per nustatytą laikotarpį. „RMS“ metodas leidžia tiksliai atskirti foninį triukšmą nuo žmogaus kalbos, nes pastaroji pasižymi dideliais energijos svyravimais ir pauzėmis. Jei užfiksuotos garso atkarpos „RMS“ reikšmė, atitinkanti aukštą triukšmo lygį parinktas slenkstis, atitinkantis ~67 dB aplinkos triukšmą, balso autentifikavimo metodas automatiškai išjungiamas, nes aplinkoje yra per daug triukšmo autentifikacijai. Kadangi triukšmas matuojamas prieš naudotojo kalbėjimą, vartotojo balsas negali klaidingai padidinti triukšmo rodmens.
- Tinklo prieinamumą ir „SIM“ būseną. Šiam tikslui naudojama pagalbinė klasė „NetworkUtils“, kuri, pasitelkdama „TelephonyManager API“ ir sistemos nustatymus, nustato, ar „OTP“ metodas apskritai gali veikti. Pirmiausia tikrinama „SIM“ kortelės būsena (*simState*): jei ji nėra *SIM_STATE_READY* pavyzdžiui (SIM neįdėta, užrakinta ar neveikia), laikoma, kad mobilusis ryšys nepasiekiamas. Papildomai tikrinamas lėktuvo režimas, skaitant *Settings.Global.AIRPLANE_MODE_ON* reikšmę jei jis įjungtas, „OTP“ metodas taip pat laikinai išjungiamas. Šiais atvejais vartotojo sąsajoje „OTP“ autentifikavimo parinktis nerodoma arba pateikiama kaip nepasiekiama, o autentifikacijos valdymo modulis parenka kitą galimą metodą.
- Biometrinio jutiklio prieinamumą. Modelis naudoja „BiometricManager“, kurį naudojant galima nustatyti ar įrenginys šiuo metu gali atlikti biometrinę autentifikaciją. Kiekvieno autentifikacijos kvietimo metu sistema iškviečia *BiometricManager.canAuthenticate()*, kuris grąžina būsenos kodą:
  BIOMETRIC_SUCCESS,
  BIOMETRIC_ERROR_NO_HARDWARE,
  BIOMETRIC_ERROR_HW_UNAVAILABLE).
  Jei grąžinama *BIOMETRIC_ERROR_HW_UNAVAILABLE*, laikoma, kad pirštų atspaudų jutiklis laikinai nepasiekiamas (pvz., jutiklis uždengtas, užimtas kitų procesų arba įrenginys šiuo metu negali atlikti biometrinio skenavimo). Jei grąžinama *BIOMETRIC_ERROR_NO_HARDWARE*, biometrinis metodas apskritai nerodomas naudotojo sąsajoje. Aptikus šias būsenas, autentifikavimo valdymo modulis automatiškai išjungia biometrinį metodą ir parenka alternatyvų kelią.

Siekiant sumažinti sistemos apkrovą ir užtikrinti efektyvų energijos naudojimą, kontekstinių signalų stebėjimas realizuotas ne nuolatiniu, o mišriu principu. Lengvai įvertinami kontekstiniai parametrai (*pvz., tinklo prieinamumas, „SIM“ būsena ar biometrinio jutiklio parengtis*) tikrinami periodiškai nes nereikalauja didelių skaičiavimo resursų. Tuo tarpu didesnę apkrovą sukeliantys signalai, tokie kaip aplinkos garso analizė per mikrofono

įvestį, nėra stebimi nuolat. Garso skenavimas aktyvuojamas tik naudotojui pasirinkus balso autentifikavimo metodą. Toks sprendimas leidžia išvengti nuolatinio mikrofono naudojimo fone, sumažina baterijos sąnaudas ir atitinka privatumo pagal dizainą (*Privacy-by-Design*) principą, nes aplinkos garsas analizuojamas aiškiai inicijuoto autentifikavimo veiksmo metu. Be to, triukšmo patikra veikia kaip prevencinis filtras – modeliui dar prieš pradedant balso verifikaciją nustato, ar aplinkos sąlygos leidžia patikimai naudoti šį metodą.

Surinkti signalai perduodami autentifikacijos valdymo moduliui, kuris nustato, kurie autentifikavimo metodai įvertinus esamas sąlygas gali būti taikomi. Atsižvelgdama į naudotojo nustatytą prioritetų eilę ir esamą kontekstą, sistema parenka tinkamiausią autentifikavimo būdą arba pasiūlo kitą galimą alternatyvą.

Tokiu būdu autentifikacija tampa konteksto atžvilgiu adaptyvi – naudotojui nėra siūlomas metodas, kuris tuo metu neveikia arba yra sunkiai panaudojamas. Aktyvusis adaptyvumas padeda pašalinti situacijas, kai autentifikacija tampa sudėtinga ar neįmanoma dėl techninių ar aplinkos kliūčių. Tai ypač svarbu naudotojams su regos ar motorikos sutrikimais, nes sistema gali automatiškai prisitaikyti prie pakitusių sąlygų ir išlaikyti prieinamą autentifikavimo eigą.

3.5. Pasyvusis adaptyvumas

Pasyvusis adaptyvumas sistemoje užtikrina ilgalaikį prisitaikymą prie individualaus naudotojo elgsenos modelio. Skirtingai nuo aktyviojo adaptyvumo, kuris reaguoja į momentinius aplinkos pokyčius, pasyvusis orientuotas į duomenų kaupimą ir analizę laikui bėgant. Jo tikslas – nustatyti, kiek esamas prisijungimo kontekstas atitinka anksčiau susiformavusį naudotojo profilį ir pagal tai apskaičiuoti pasitikėjimo lygį, kuris vėliau naudojamas autentifikacijos griežtumui parinkti.

Naudotojo profilis sistemoje saugomas ne kaip pilnas atskirų įvykių sąrašas, bet kaip agreguotų statistinių svorių rinkinys. Tokiu būdu sumažinama duomenų apimtis ir išlaikomas didesnis skaičiavimo efektyvumas. Profilyje kaupiamas bendras sėkmingų prisijungimų svoris, atskirų tinklo identifikatorių („*SSID*“) svoriai, paros laiko blokų svoriai bei kombinuoti tinklo ir laiko signalų svoriai. Papildomai saugoma prisijungimų istorija, naudojama profilio raidai stebėti. Visi duomenys saugomi lokaliai įrenginyje.

Prisijungimo kontekstas formuojamas iš dviejų pagrindinių pasyvių signalų: tinklo identifikatoriaus ir laiko. Aplikacija prisijungimo metu nustato belaidžio tinklo „SSID“ ir prieš įrašymą jį paverčia maišos reikšme. Tokiu būdu sistemoje nėra saugomas tikrasis tinklo pavadinimas, o tai sumažina privatumo riziką. Laiko kontekstas modelyje apibrėžiamas 12 paros blokų po 2 valandas. Papildomai vertinamas jungtinis „SSID“ ir laiko signalas, kuris leidžia tiksliau nustatyti naudotojui būdingą prisijungimo kontekstą.

Kiekvieno naujo prisijungimo metu pasyviojo adaptyvumo modulis nustato esamą prisijungimo kontekstą ir palygina jį su anksčiau sukauptu naudotojo profiliu. Pasitikėjimo balas apskaičiuojamas taikant Laplaso išlyginimu pagrįstą tikimybinį vertinimą:

$$T(X) = \frac{count(X) + \alpha}{totalWeight + \alpha(N + 1)}$$

X žymi konkretų vertinamą kontekstinį signalą, pavyzdžiui, esamą tinklo identifikatorių, laiko bloką arba jų junginį. Koeficiantas α = 1 yra Laplaso išlyginimo koeficientas. Jis užtikrina, kad net ir anksčiau nestebėtas kontekstas, pavyzdžiui, naujas tinklas ar naujas laiko derinys, gautų ne nulinę, o mažą teigiamą tikimybę. Tokiu būdu sistema gali vertinti ir naujas situacijas, nepadarydama jų automatiškai maksimalios rizikos atvejais vien dėl to, kad jos dar nebuvo matytos profilyje.

Galutinis pasitikėjimo balas sudaromas kaip trijų verčių svorinė kombinacija. Didžiausias svoris tenka kombinuotam tinklo ir laiko signalui, nes jis geriausiai apibūdina įprastą naudotojo prisijungimo situaciją. Atskirai vertinami tinklo identifikatorius ir laiko blokas turi mažesnę įtaką, nes kiekvienas iš jų atskirai pateikia mažiau specifinę informaciją. Tokiu būdu sistema pirmenybę teikia tikslesniam kontekstui, bet nepraranda lankstumo pasikeitus vienam iš signalų.

Pradiniame etape pasyvusis adaptyvumas veikia mokymosi režimu. Kol sėkmingų prisijungimų skaičius nepasiekia 30, sukaupta informacija laikoma nepakankama patikimam naudotojo profiliui formuoti, todėl sistema dar nemažina autentifikacijos reikalavimų ir grąžina „LEARNING“ būseną. Kai profilisis susiformuoja, modelis pradeda aktyviai taikyti pasitikėjimo balo vertinimą ir pagal jį priskiria vieną iš rizikos lygių: LOW, MEDIUM arba HIGH.

Siekiant išlaikyti sistemos jautrumą naudotojo elgsenos pokyčiams, profiliui taikomas laipsniškas silpnėjimas. Jei naudotojas ilgesnį laiką nesinaudoja sistema, anksčiau sukauptų signalų svoriai palaipsniui mažėja. Taip užtikrinama, kad seni ir nebepasikartojantys kontekstai ilgainiui prarastų įtaką, o sistema geriau prisitaikytų prie naujų naudotojo įpročių. Silpnėjimas taikomas tiek bendram profilio svoriui, tiek atskiriems tinklo, laiko ir jungtinio signalo svoriams.

Po kiekvieno sėkmingo prisijungimo naudotojo profilis papildomas nauja informacija: atnaujinami tinklo, laiko ir jų kombinacijos svoriai, perskaičiuojamas bendras profilio svoris ir išsaugomas istorijos įrašas. Taip sistema palaipsniui mokosi iš realių naudotojo prisijungimo duomenų. Dėl to didėja jos gebėjimas tiksliau įvertinti, ar konkretus prisijungimo kontekstas yra įprastas, ar nukrypstantis nuo susiformavusio profilio.

3.6. Išvados

1. Sukurtas adaptyvios autentifikacijos prototipo modelis parodė, kad išmaniojo įrenginio funkcionalumas (*mikrofonas, biometriniai jutikliai, haptika, TTS*) leidžia praktiškai įgyvendinti daugialypę autentifikaciją be papildomos įrangos, išlaikant prieinamumą skirtingų negalių turintiems naudotojams.
2. Įgyvendintas aktyvusis adaptyvumas patvirtino, kad kontekstiniai signalai gali būti sėkmingai naudojami autentifikavimo metodų pasirinkimų valdymui realiuoju laiku. Triukšmo analizė, „SIM“ būsenos nustatymas per „TelephonyManager“ ir biometrinio jutiklio prieinamumas per „BiometricManager“ leidžia automatiškai išjungti esamame naudojimo kontekste netinkamus metodus ir užtikrinti adaptyvią autentifikaciją.
3. Aktyvaus ir pasyvaus adaptyvumo derinimas parodė, kad šie mechanizmai papildo vienas kitą, nes aktyvusis adaptyvumas sprendžia momentinius aplinkos apribojimus, o pasyvusis – ilgalaikius elgsenos pokyčius. Tokia architektūra leidžia sistemai prisitaikyti tiek trumpalaikėje, tiek ilgalaikėje perspektyvoje.
4. Svoriniu rizikos vertinimu pagrįstas sprendimų modelis leido efektyviai subalansuoti saugumo ir patogumo reikalavimus, nes įprastose, naudotojui pažįstamose sąlygose autentifikavimo žingsnių skaičius buvo sumažinamas, o aptikus anomalijas – automatiškai didinamas. Tai sumažino perteklinę autentifikavimo naštą saugiose situacijose.
5. Prototipo architektūros moduliškumas parodė, kad adaptyvios autentifikacijos sistema gali būti plečiama ir modifikuojama nekeičiant pagrindinės logikos. Tai sudaro prielaidas ateityje integruoti papildomus kontekstinius signalus ar autentifikavimo metodus, padėsiančius pagerinti modelio naudojimo patirtį.

4. Eksperimentinis siūlomo modelio vertinimas

Išanalizavus autentifikavimo sprendimų prieinamumo problemas, suformavus siūlomo modelio koncepciją ir įgyvendinus jo prototipą, toliau svarbu įvertinti, kaip šis sprendimas atrodo kitų autentifikavimo krypčių kontekste ir kaip jis veikia praktikoje. Ankstesniuose skyriuose buvo nustatyta, kad prieinamas autentifikavimas negali būti grindžiamas vienu universaliu metodu, nes skirtingi naudotojai susiduria su nevienodomis kliūtimis, o autentifikavimo tinkamumas priklauso ne tik nuo saugumo savybių, bet ir nuo naudojimo konteksto, atsarginių būdų prieinamumo bei sprendimo lankstumo. Dėl šios priežasties šiame skyriuje pirmiausia atliekamas siūlomo modelio kokybinis palyginimas su analizės dalyje aptartomis autentifikavimo sprendimų kryptimis, o vėliau pateikiamas eksperimentinis prototipo vertinimas. Toks vertinimas leidžia nustatyti, kokiais aspektais siūlomas modelis išsiskiria prieinamumo, adaptyvumo, privatumo ir atsarginių autentifikavimo būdų požiūriu, bei praktiškai patikrinti, kaip prototipas veikia skirtingomis naudojimo sąlygomis.

4.1. Kokybinis siūlomo modelio palyginimas

4.1.1. Palyginimo kriterijai

Kokybinis palyginimas šiame darbe grindžiamas kriterijais, išvestais iš analizės dalyje aptartų prieinamumo ir autentifikavimo reikalavimų. Vertinant autentifikavimo sprendimus atsižvelgiama į jų prieinamumą tikslinėms naudotojų grupėms, priklausomybę nuo teksto suvokimo, regimosios informacijos apdorojimo ir tikslios motorinės kontrolės, jautrumą aplinkos sąlygoms, galimybę taikyti atsarginius autentifikavimo būdus, prisitaikymą prie naudojimo konteksto, privatumo užtikrinimą, duomenų kiekio optimalaus rinkimo ir sprendimo veikimo aiškumą. Šie kriterijai leidžia nuosekliai palyginti analizuotas autentifikavimo sprendimų kryptis su šiame darbe siūlomu adaptyvaus autentifikavimo modeliu.

4.1.2. Siūlomo modelio palyginimas su analizuotomis autentifikavimo sprendimų kryptimis

Siekiant nuosekliai įvertinti siūlomo modelio vietą tarp analizėje aptartų autentifikavimo sprendimų krypčių, toliau pateikiamas kokybinis palyginimas pagal anksčiau išskirtus kriterijus. Lentelėje pateiktas vertinimas yra kokybinis, todėl jis remiasi analizės dalyje aptartomis sprendimų savybėmis, o ne tiesiogiai palyginamais eksperimentiniais matavimais (žr. **1 lentelė.** Kokybinis metodų palyginimas). Vertinimai pateikiami siekiant apimti skirtingų autentifikavimo krypčių bendras tendencijas prieinamumo, lankstumo, privatumo ir praktinio taikymo požiūriu.

1 lentelė. Kokybinis metodų palyginimas

Vertinimo kriterijus	**Vieno metodo prieinamumo sprendimai**	**Biometriniai ir slaptažodžių nenaudojantys sprendimai**	**Adaptyvūs, kontekstą vertinantys sprendimai**	**Daugiametodžiai autentifikavimo sprendimai**	**Siūlomas modelis**
Prieinamumas tikslinėms naudotojų	Vidutinis	Vidutinis	Vidutinis	Stiprus	Stiprus

grupėms					
Priklausomybė nuo teksto	Ribota	Ribota	Vidutinė	Vidutinė	Ribota
Priklausomybė nuo regimosios informacijos	Vidutinė	Ribota	Vidutinė	Vidutinė	Ribota
Priklausomybė nuo tikslios motorinės kontrolės	Vidutinė	Ribota	Vidutinė	Vidutinė	Ribota
Jautrumas aplinkos sąlygoms	Stiprus	Ribotas	Vidutinis	Vidutinis	Vidutinis
Atsarginių autentifikavimo būdų prieinamumas	Ribotas	Ribotas	Vidutinis	Stiprus	Stiprus
Prisitaikymas prie naudojimo konteksto	Ribotas	Ribotas	Stiprus	Vidutinis	Stiprus
Privatumo ir duomenų kiekio optimizavimo užtikrinimas	Vidutinis	Vidutinis	Vidutinis	Vidutinis	Stiprus
Sprendimo logikos aiškumas	Vidutinis	Vidutinis	Vidutinis	Vidutinis	Stiprus

Lentelėje pateiktas palyginimas rodo, kad vieno metodo prieinamumo sprendimai dažniausiai yra stipriai orientuoti į konkrečią naudotojų grupę ar aiškiai apibrėžtą kliūtį, todėl gali būti veiksmingi sprendžiant vieną specifinę prieinamumo problemą. Tačiau jų pritaikomumas platesniame autentifikavimo kontekste paprastai išlieka ribotas, nes tokie sprendimai dažniausiai remiasi viena dominuojančia autentifikacijos forma ir turi mažiau alternatyvių autentifikacijos kelių. Dėl šios priežasties jų jautrumas aplinkos sąlygoms ar individualiems naudotojo skirtumams dažnai yra didesnis, o lankstumas kasdienėse skirtingose situacijose, mažesnis nei siūlomame modelyje. Biometriniai ir slaptažodžių nenaudojantys autentifikavimo sprendimai pasižymi stipria technologine baze ir sumažina priklausomybę nuo tradicinių tekstinių slaptažodžių, todėl gali būti patogesni daliai naudotojų, kuriems tekstinė įvestis yra sudėtinga ir nepatogi. Vis dėlto jų praktinis prieinamumas dažnai priklauso nuo konkretaus įrenginio techninių galimybių, operacinės sistemos palaikymo ir kaip toks sprendimas yra įgyvendintas konkrečioje platformoje. Dėl to jie ne visada numato pakankamai lankstų atsarginių būdų taikymą ar prisitaikymą prie naudotojo su specifine negalia situacijos. Siūlomas modelis šioje vietoje išsiskiria tuo, kad biometrinį autentifikavimą naudoja kaip vieną iš galimų metodų, o ne kaip vienintelį, dominuojantį autentifikavimo kelią. Adaptyvūs, kontekstą vertinantys sprendimai yra artimiausia kryptis siūlomam modeliui, nes jų esmė taip pat grindžiama autentifikavimo reikalavimų keitimu priklausomai nuo kasdienio naudojimo konteksto ir įvertintos rizikos. Tokie sprendimai leidžia sumažinti autentifikavimo naštą įprastose situacijose ir sugriežtinti autentifikavimą tada, kai prisijungimo aplinkybės tampa neįprastos. Tačiau šios krypties sprendimai ne visada pakankamai akcentuoja atsarginių autentifikavimo būdų prieinamumą ir aiškiai apibūdina naudojamą sprendimo logiką. Siūlomas modelis skiriasi

tuo, kad adaptyvumas jame derinamas su kelių autentifikavimo metodų naudojimu, lokaliu duomenų saugojimu ir sistema pasitikėjimo lygį apskaičiuoja pagal aiškiai apibrėžtas taisykles, o ne pagal nepaaiškinamą mašininio modelio veikimą ar „juodosios dėžės“ modelį, kai vyrauja paslėpta platformos logika, kurios negalima detaliai paaiškinti. Daugiametodžiai autentifikavimo sprendimai pagal savo logiką yra artimiausi siūlomam modeliui prieinamumo požiūriu, nes kelių metodų buvimas iš karto mažina riziką, kad naudotojas liks be galimybės autentifikuotis. Vis dėlto vien kelių metodų integravimas dar nereiškia, kad sistema iš tiesų geba lanksčiai reaguoti į pakitusį kontekstą, aplinkos apribojimus ar laikinas konkretaus metodo neprieinamumo situacijas. Siūlomo modelio pranašumas šioje vietoje yra tas, kad keli autentifikavimo metodai jame nėra tik alternatyvų rinkinys, bet yra susieti su aktyvaus ir pasyvaus adaptyvumo logika. Tai suteikia galimybę ne tik naudoti kelis autentifikavimo būdus, bet ir lanksčiai parinkti tinkamiausią iš jų pagal esamą kontekstą, kartu išlaikant atsarginį autentifikavimo variantą ir vengiant situacijų, kai naudotojas nebegali atlikti autentifikavimo proceso.

4.1.3. Kokybinio palyginimo apibendrinimas

Atliktas kokybinis palyginimas parodė, kad siūlomas adaptyvus autentifikavimo modelis išsiskiria kelių autentifikavimo metodų derinimu, prisitaikymu prie naudojimo konteksto, atsarginių autentifikavimo kelių numatymu ir privatumo principais grindžiamu veikimu. Palyginimas taip pat parodė, kad siūlomo modelio stiprioji pusė atsiskleidžia ne vien atskiro autentifikavimo metodo pasirinkime, bet jų tarpusavio derinime ir gebėjime lanksčiai reaguoti į skirtingas naudojimo situacijas. Dėl to siūlomas modelis gali būti vertinamas kaip lankstesnis sprendimas prieinamumo ir adaptyvumo požiūriu, analizės identifikuotoms naudotojų grupėms nei siauresnio pritaikomumo vieno metodo autentifikavimo kryptys. Atsižvelgiant į tai, tolesniame poskyryje siekiama eksperimentiškai įvertinti, kaip siūlomo modelio savybės pasireiškia praktikoje ir kaip prototipas funkcionuoja esant skirtingoms naudojimo sąlygoms.

4.2. Eksperimentinio vertinimo tikslas ir metodika

4.2.1. Eksperimentinio vertinimo tikslas

Šiame darbe atliekamo eksperimentinio vertinimo tikslas yra praktiškai įvertinti, kaip siūlomo adaptyvaus autentifikavimo modelio savybės pasireiškia įgyvendintame prototipe skirtingomis naudojimo sąlygomis. Vertinimu siekiama nustatyti, ar sistema geba prisitaikyti prie konteksto, formuoti naudotojo pasitikėjimo profilį, mažinti autentifikavimo apkrovą įprastose situacijose ir taikyti griežtesnį autentifikavimą tada, kai prisijungimo aplinkybės tampa neįprastos. Taip pat vertinama, kaip praktikoje veikia aktyviojo adaptyvumo logika, kai autentifikavimo metodų prieinamumas kinta dėl aplinkos triukšmo, tinklo būsenos ar biometrinių jutiklių prieinamumo. Šiame darbe eksperimentinis vertinimas nėra skirtas pačių operacinės sistemos ar platformos lygmens autentifikavimo technologijų tikslumui tirti. Pagrindinis dėmesys skiriamas tam, kaip siūlomame modelyje derinami keli autentifikavimo metodai, kaip sistema prisitaiko prie kontekstinių signalų ir kaip šios savybės pasireiškia praktiniame prototipo veikime.

4.2.2. Eksperimentų organizavimas

Eksperimentai šiame darbe organizuojami taip, kad būtų galima atskirai įvertinti pasyviojo ir aktyviojo adaptyvumo veikimą. Pasyviojo adaptyvumo eksperimentuose taikomos pasikartojančių autentifikacijos sesijų sekos, kurių metu kontroliuojamai keičiami prisijungimo kontekstiniai signalai, tokie kaip tinklas ar paros laiko intervalas. Tai leidžia stebėti, kaip sistema formuoja pasitikėjimo profilį, kaip jis stabilizuojasi ir kaip kinta pasikeitus įprastoms prisijungimo sąlygoms. Aktyviojo adaptyvumo eksperimentuose keičiamos aplinkos sąlygos, turinčios tiesioginę įtaką autentifikavimo metodų prieinamumui, pavyzdžiui, triukšmo lygis, tinklo būsena ar biometrinių jutiklių prieinamumas. Visi eksperimentai atliekami pagal iš anksto apibrėžtus scenarijus, kuriuose keičiami tik su konkrečiu vertinimo tikslu susije veiksniai.

4.2.3. Renkami duomenys ir vertinimo rodikliai

Siekiant nuosekliai įvertinti siūlomo adaptyvaus autentifikavimo modelio veikimą, eksperimentų metu renkami tiek kontekstiniai duomenys, tiek paties modelio apskaičiuojami vidiniai rodikliai. Kadangi šiame darbe vertinamas ne vien atskirų autentifikavimo metodų techninis veikimas, bet ir bendras modelio prisitaikymas prie naudotojo elgsenos bei aplinkos sąlygų, duomenų rinkimas orientuojamas į tuos požymius, kurie leidžia stebėti sistemos sprendimų logiką ir jos pokyčius laike. Pasyviojo adaptyvumo eksperimentuose pagrindiniai renkami duomenys apima prisijungimo kontekstą ir pasitikėjimo profilio būseną. Kiekvienos autentifikacijos sesijos metu fiksuojamas naudojamas tinklo identifikatorius, paros laiko intervalas, bendras sėkmingų prisijungimų skaičius, bendras profilio svoris, apskaičiuotas pasitikėjimo lygis ir jam priskirtas rizikos lygis. Tais atvejais, kai vertinamas profilio silpnėjimas po neveiklumo, papildomai registruojamas pritaikytas laiko silpnėjimo koeficientas ir jo įtaka pasitikėjimo lygiui. Šie duomenys leidžia stebėti, kaip sistema formuoja naudotojo profilį, kaip jis stabilizuojasi, kaip reaguoja į naują aplinką ir kaip kinta ilgesnį laiką nesinaudojant sistema. Aktyviojo adaptyvumo eksperimentuose pagrindinis dėmesys skiriamas autentifikavimo metodų prieinamumo pokyčiams realiuoju laiku. Šiuo atveju registruojami tokie duomenys kaip aplinkos triukšmo lygis, balso autentifikavimo metodo būsenos pokytis, tinklo prieinamumas, SIM būklė, biometrinio jutiklio prieinamumas. Šie duomenys leidžia įvertinti, kaip aktyviojo adaptyvumo logika reaguoja į aplinkos apribojimus ir ar sistema geba išlaikyti prieinamą autentifikavimo kelią net ir tada, kai dalis metodų tampa laikinai neprieinami naudojimui. Profilio brandos reikšmė apskaičiuojama pagal sėkmingų prisijungimų skaičių S, dalijamą iš mokymosi fazei reikalingų 30 prisijungimų:

$$M = \frac{S}{30}$$

M – profilio formavimos reikšmė, o S – sėkmingų prisijungimų skaičius. Kai S ≥ 30, laikoma, kad profilis yra pilnai susiformavęs.

Vertinant pasyviojo adaptyvumo logiką, pasitikėjimo lygis apskaičiuojamas pagal kelių kontekstinių tikimybių kombinaciją, kurioje kiekvienas signalas turi skirtingą įtaką galutiniam pasitikėjimo lygiui:

$$T = 0.55 * P_{ssidHour} + 0.30 * P_{ssid} + 0.15 * P_{hour}$$

T – bendras pasitikėjimo lygis, $P_{ssidHour}$ – jungtinio tinklo ir laiko konteksto įvertis, P_{ssid} – tinklo konteksto įvertis, P_{hour} – laiko konteksto įvertis. Ši formulė leidžia kiekybiškai įvertinti, kiek esamas prisijungimo kontekstas atitinka anksčiau suformuotą naudotojo profilį.

Kai vertinamas profilio silpnėjimas dėl neveiklumo, naudojamas laiko silpnėjimo koeficientas:

$$d = 0{,}1\frac{\min(\Delta t, 30)}{30}$$

d – silpnėjimo koeficientas, Δt – dienų skaičius nuo paskutinio profilio atnaujinimo. Tokiu būdu naujesni prisijungimo duomenys turi didesnį svorį nei senesni, o po ilgesnio neveiksnumo laikotarpio pasitikėjimo profilis natūraliai susilpnėja.

Pagal apskaičiuotą pasitikėjimo lygį sistemai priskiriamas rizikos lygis:

$$R = \begin{cases} LEARNING & if\ S < 30 \\ LOW & if\ T \geq 0.15 \\ MEDIUM & if\ 0.06 \leq T < 0.15 \\ HIGH & if\ T < 0.06 \end{cases}$$

R – rizikos lygis, S – sėkmingų prisijungimų skaičius, o T– apskaičiuotas pasitikėjimo lygis. Šis rodiklis naudojamas vertinant, kaip sistema keičia autentifikavimo griežtumą priklausomai nuo naudotojo konteksto ir profilio susiformavimo būklės. Tokiu būdu surinkti duomenys ir apibrėžti vertinimo rodikliai sudaro pagrindą tolesniuose poskyriuose pateikiamam atskirų eksperimentų vertinimui.

4.3. Tapatybės profilio formavimosi ir mokymosi fazės vertinimas

4.3.1. Eksperimento tikslas

Šio eksperimento tikslas yra įvertinti, kaip siūlomame modelyje per pirmąsias sėkmingas autentifikacijos sesijas formuojamas pasyvusis naudotojo profilis ir kaip veikia mokymosi fazė. Eksperimentu siekiama patikrinti ar sistema iki nustatytos 30 sėkmingų prisijungimų ribos išlaiko mokymosi būseną, neperkelia naudotojo į žemesnės rizikos lygį per anksti ir nuosekliai kaupia kontekstinę informaciją apie naudotojo prisijungimo aplinką. Taip pat siekiama stebėti, kaip šios fazės metu kinta profilio brandos reikšmė, pasitikėjimo lygis ir atskiri kontekstiniai įverčiai, naudojami galutiniam pasitikėjimo lygiui apskaičiuoti. Tokiu būdu eksperimentas leidžia įvertinti ar pradinė mokymosi fazė iš tiesų veikia kaip apsauginis mechanizmas nuo situacijų, kai nepakankamai sukauptas kontekstas mokymosi metu būtų vertinamas kaip patikimas.

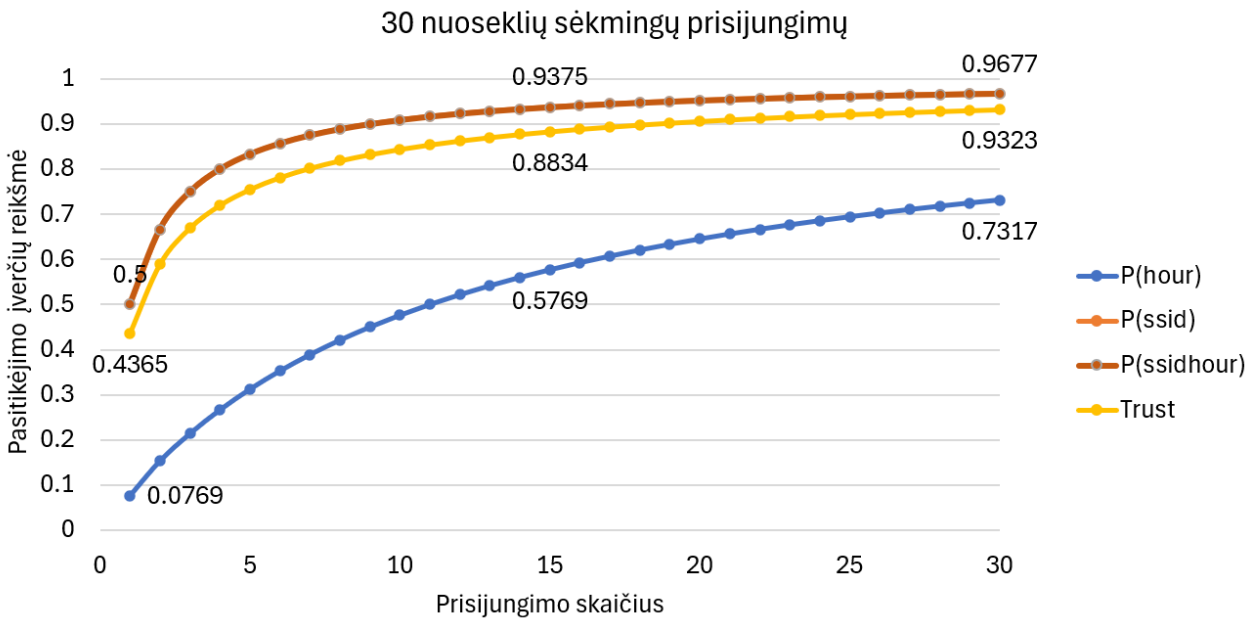
4.3.2. Eksperimento eiga

Eksperimentas buvo atliekamas kontroliuojamomis sąlygomis, palaikant nekintantį prisijungimo kontekstą. Visos autentifikacijos sesijos buvo vykdomos naudojant tą patį tinklo identifikatorių ir tą patį paros laiko intervalą, todėl eksperimento metu nekito nei

tinklo, nei laiko kontekstas. Tokiomis sąlygomis buvo atlikta 30 nuoseklių sėkmingų prisijungimų, kurie yra reikiami norint pereiti iš mokymosi fazės į suformuotą profilį. Kiekvienos sesijos metu buvo registruojamas prisijungimo skaičius, pasitikėjimo lygis, kontekstiniai įverčiai $P_{ssidHour}$, P_{ssid}, P_{hour}. Tokia eksperimento organizavimo schema leido stebėti, kaip sistema nuosekliai kaupia kontekstinę informaciją stabilioje aplinkoje ir kaip, didėjant sėkmingų prisijungimų skaičiui, formuojasi pradinis naudotojo pasitikėjimo profilis (žr. **2 lentelė.** 30 nuoseklių sėkmingų prisijungimų duomenys).

2 lentelė. 30 nuoseklių sėkmingų prisijungimų duomenys

Prisijungimo Nr.	P_{hour}	P_{ssid}	$P_{ssidHour}$	Pasitikėjimo lygis T
1.	0,0769	0,5000	0,5000	0,4365
2.	0,1538	0,6667	0,6667	0,5897
3.	0,2143	0,7500	0,7500	0,6696
4.	0,2667	0,8000	0,8000	0,7200
5.	0,3125	0,8333	0,8333	0,7552
6.	0,3529	0,8571	0,8571	0,7815
7.	0,3889	0,8750	0,8750	0,8021
8.	0,4211	0,8889	0,8889	0,8187
9.	0,4500	0,9000	0,9000	0,8325
10.	0,4762	0,9091	0,9091	0,8442
11.	0,5000	0,9167	0,9167	0,8542
12.	0,5217	0,9231	0,9231	0,8629
13.	0,5417	0,9286	0,9286	0,8705
14.	0,5600	0,9333	0,9333	0,8773
15.	0,5769	0,9375	0,9375	0,8834
16.	0,5926	0,9412	0,9412	0,8889
17.	0,6071	0,9444	0,9444	0,8938
18.	0,6207	0,9474	0,9474	0,8984
19.	0,6333	0,9500	0,9500	0,9025
20.	0,6452	0,9524	0,9524	0,9063
21.	0,6563	0,9545	0,9545	0,9098
22.	0,6667	0,9565	0,9565	0,9130
23.	0,6765	0,9583	0,9583	0,9161
24.	0,6857	0,9600	0,9600	0,9189
25.	0,6944	0,9615	0,9615	0,9215
26.	0,7027	0,9630	0,9630	0,9239
27.	0,7105	0,9643	0,9643	0,9262
28.	0,7179	0,9655	0,9655	0,9284
29.	0,7250	0,9667	0,9667	0,9304
30.	0,7317	0,9677	0,9677	0,9323



13 pav. Kontekstinių įverčių kitimas per 30 nuoseklių sėkmingų prisijungimų

Atliekant eksperimenta matyti (žr. **13 pav.** Kontekstinių įverčių kitimas per 30 nuoseklių sėkmingų prisijungimų), kad didėjant sėkmingų prisijungimų skaičiui visi pagrindiniai įverčiai ir bendras pasitikėjimo lygis nuosekliai auga. $P_{ssidHour}$, P_{ssid} reikšmės šiame eksperimente beveik sutampa, nes visi prisijungimai buvo atliekami tame pačiame tinklo ir laiko kontekste, todėl jungtinio tinklo ir laiko signalo kaupimas vyko beveik identiškai kaip vien „Wi-Fi“ tinklo konteksto kaupimas. Tup pat metu P_{hour} augo lėčiau, nes laiko signalas modelyje vertinamas platesniame galimų intervalų rinkinyje.

4.3.3. Rezultatų analizė

Eksperimento rezultatai parodė, kad nekintančiame prisijungimo kontekste pasyvusis naudotojo profilis formuojasi nuosekliai, o visi pagrindiniai kontekstiniai įverčiai didėja kartu su sėkmingų prisijungimų skaičiumi. Kadangi autentifikacijos sesijos buvo atliekamos naudojant tą patį tinklo identifikatorių ir laiko intervalą, tiek tinklo konteksto įvertis P_{ssid}, tiek jungtinis tinklo ir laiko konteksto įvertis $P_{ssidHour}$ augo sparčiai ir beveik sutapo tarpusavyje. Laiko konteksto įvertis P_{hour}taip pat nuosekliai didėjo, tačiau augo lėčiau nei kiti kontekstiniai įverčiai. Taip yra todėl, kad laiko signalas modelyje vertinamas tarp 12 galimų dviejų valandų intervalų, todėl pradinėje fazėje jo reikšmė didėja lėčiau nei pastoviame tinkle kaupiamas SSID kontekstas. Dėl šios priežasties bendras pasitikėjimo lygis kilo tolygiai nuo 0,4365 pirmojo prisijungimo metu iki 0,9323 trisdešimtojo prisijungimo metu. Šie rezultatai rodo, kad modelis stabilioje aplinkoje sėkmingai kaupia pasikartojantį kontekstą ir formuoja aiškų naudotojo profilį. Eksperimento metu nustatyta, kad pasitikėjimo lygis nekintančiame kontekste didėja labai sparčiai, todėl šis eksperimentas patvirtina mokymosi fazės ir profilio formavimosi logiką, tačiau nesudaro pakankamo pagrindo galutinai vertinti pasirinktų rizikos slenksčių tinkamumo skirtingose profilio formavimosi situacijose. Gauti rezultatai rodo, kad modelis nuosekliai kaupia kontekstinę informaciją ir išlaiko mokymosi būsena viso profilio formavimosi metu, tai

veikia kaip atskiras apsauginis mechanizmas, kuris neleidžia autentifikavimo griežtumo sumažinti per anksti vien dėl greitai besiformuojančio stabilaus konteksto.

4.4. Pasitikėjimo lygio stabilumo vertinimas

4.4.1. Eksperimento tikslas

Šio eksperimento tikslas yra įvertinti, kaip siūlomame modelyje keičiasi pasitikėjimo lygis po to, kai naudotojo profilis jau yra susiformavęs ir sistema pereina iš mokymosi fazės į įprastą veikimo režimą. Eksperimentu siekiama nustatyti, ar pasitikėjimo lygis, toliau kartojantis tam pačiam prisijungimo kontekstui, toliau auga, tačiau jo augimas palaipsniui lėtėja, ar augimas išlieka nekontroliuojamai spartus. Taip pat siekiama stebėti, kaip po profilio susiformavimo kinta atskiri kontekstiniai įverčiai ir kaip jų reikšmės artėja prie aukšto pasitikėjimo reikšmių srities. Tokiu būdu eksperimentas leidžia įvertinti, ar nekintančiame kontekste modelio pasitikėjimo lygis praktiškai stabilizuojasi.

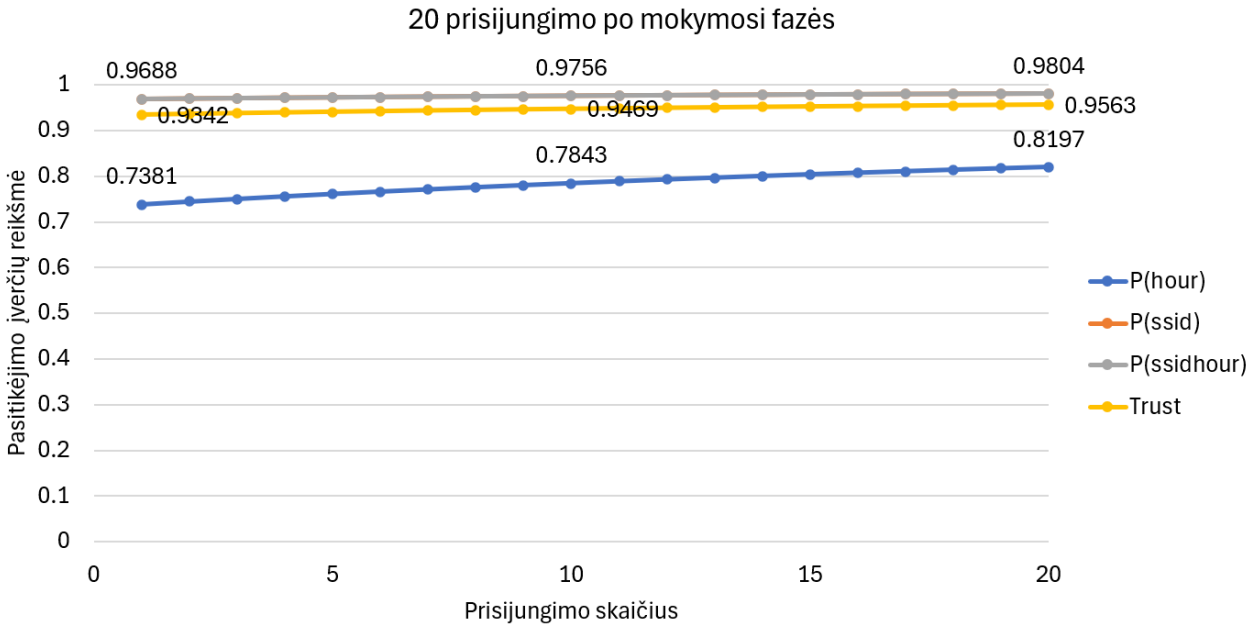
4.4.2. Eksperimento eiga

Eksperimentas buvo atliekamas kontroliuojamomis sąlygomis, išlaikant tą patį prisijungimo kontekstą. Po mokymosi fazės pabaigos buvo tęsiama sėkmingų autentifikacijos sesijų seka, siekiant stebėti tolesnį pasitikėjimo lygio kitimą. Kadangi įprastame veikimo režime, pasiekus pakankamai aukštą pasitikėjimo lygį, sistema gali sumažinti autentifikavimo griežtumą, šis eksperimentas buvo vykdomas kontroliuojamu testavimo režimu, siekiant toliau registruoti sėkmingas prisijungimo sesijas ir stebėti pasitikėjimo lygio kitimą nekintančiame kontekste. Tokiu būdu buvo sudarytos sąlygos vertinti ne tik mokymosi fazės pabaigą, bet ir tolesnį pasitikėjimo lygio formavimos elgesį jau susiformavus profiliui. Vertinimo metu po pirmųjų 30 sėkmingų prisijungimų toje pačioje aplinkoje buvo atlikta papildomai dar 20 sėkmingų prisijungimų. Visos sesijos buvo vykdomos naudojant tą patį tinklo identifikatorių ir tą patį paros laiko intervalą, todėl eksperimento metu nekito nei tinklo, nei laiko kontekstas. Kiekvienos sesijos metu buvo registruojamas prisijungimo skaičius, pasitikėjimo lygis, atskiri kontekstiniai įverčiai $P_{ssidHour}$, P_{ssid}, P_{hour}. Pagrindinis dėmesys šiame eksperimente buvo skiriamas pasitikėjimo lygio pokyčiui tarp gretimų prisijungimų (žr. **3 lentelė.** 20 prisijungimo po mokymosi fazės duomenys). Tokia eksperimento eiga leido įvertinti, ar po profilio susiformavimo pasitikėjimo lygio augimas išlieka spartus, ar palaipsniui lėtėja ir artėja prie stabilesnės reikšmių srities.

3 lentelė. 20 prisijungimo po mokymosi fazės duomenys

Prisijungimo Nr.	P_{hour}	P_{ssid}	$P_{ssidHour}$	Pasitikėjimo lygis T
31.	0,7381	0,9688	0,9688	0,9342
32.	0,7442	0,9697	0,9697	0,9359
33.	0,7500	0,9706	0,9706	0,9375
34.	0,7556	0,9714	0,9714	0,9390
35.	0,7609	0,9722	0,9722	0,9405
36.	0,7660	0,9730	0,9730	0,9419
37.	0,7708	0,9737	0,9737	0,9433
38.	0,7755	0,9744	0,9744	0,9445
39.	0,7800	0,9750	0,9750	0,9458
40.	0,7843	0,9756	0,9756	0,9469
41.	0,7885	0,9762	0,9762	0,9480

42.	0,7925	0,9767	0,9767	0,9491
43.	0,7963	0,9773	0,9773	0,9501
44.	0,8000	0,9778	0,9778	0,9511
45.	0,8036	0,9783	0,9783	0,9521
46.	0,8070	0,9787	0,9787	0,9530
47.	0,8103	0,9792	0,9792	0,9538
48.	0,8136	0,9796	0,9796	0,9547
49.	0,8167	0,9800	0,9800	0,9555
50.	0,8197	0,9804	0,9804	0,9563



14 pav. Kontekstinių įverčių kitimas per 20 sėkmingų prisijungimų po mokymosi fazės

Stebint tolimesnį modelio naudojimą po mokymosi fazės galima pastebėti (žr. **14 pav.** Kontekstinių įverčių kitimas per 20 sėkmingų prisijungimų po mokymosi fazės), jog pasitikėjimo lygio augimas po profilio susiformavimo praktiškai stabilizuojasi, o kiekvienas papildomas prisijungimas daro vis mažesnę įtaką bendram pasitikėjimo lygiui. Tokia tendencija atitinka modelio suprojektuotą logiką, nes pasitikėjimo lygis nėra skirtas neribotam augimui kai kartojasi tas pats prisijungimo kontekstas. Artėjant prie aukštų reikšmių, papildomų prisijungimų poveikis tampa vis mažesnis, todėl bendras pasitikėjimo lygis pradeda stabilizuotis.

4.4.3. Rezultatų analizė

Eksperimento rezultatai parodė, kad po profilio susiformavimo pasitikėjimo lygis autentifikuojantis nekintančiame kontekste ir toliau didėja, tačiau jo augimas palaipsniui lėtėja. Lentelėje pateikti duomenys rodo, kad nuo 31 iki 50 prisijungimo pasitikėjimo lygis padidėjo nuo 0,9342 iki 0,9563, tačiau pokytis tarp gretimų prisijungimų šiame etape jau buvo gerokai mažesnis nei pradinėje mokymosi fazėje. Tai reiškia, kad modelio išvestis po profilio susiformavimo nebedidėja tokiu pačiu tempu kaip pradžioje, o artėja prie praktiškai stabilesnės aukštų pasitikėjimo reikšmių srities. Atskiri kontekstiniai įverčiai $P_{ssidHour}$, P_{ssid}, P_{hour} taip pat toliau didėjo, tačiau jų reikšmių pokyčiai tarp prisijungimų tapo vis mažesni. Tai rodo, kad modelis, toliau kartojantis tam pačiam prisijungimo kontekstui, į papildomus

to paties konteksto prisijungimus reaguoja vis silpniau ir palaipsniui artėja prie nusistovėjusio konteksto įverčio. Tokia elgsena leidžia teigti, kad pasitikėjimo lygio augimas šiame etape tampa vis mažiau jautrus kiekvienam papildomam to paties konteksto prisijungimui. Tai rodo, kad modeliui toliau vertinant tą patį prisijungimo kontekstą, kiekvieno papildomo prisijungimo įtaka kontekstiniams įverčiams palaipsniui mažėja, o jų reikšmės artėja prie nusistovėjusios būsenos. Toks modelio elgesys parodo, kad šiame etape pasitikėjimo lygio augimas tampa vis mažiau jautrus kiekvienam papildomam to paties konteksto prisijungimui.

4.5. Konteksto jautrumo ir rizikos priskyrimo vertinimas

4.5.1. Eksperimento tikslas

Šio eksperimento tikslas yra įvertinti, kaip siūlomame modelyje pasitikėjimo lygis ir rizikos priskyrimas kinta pasikeitus prisijungimo kontekstui. Eksperimentu siekiama nustatyti, kaip keičiant tinklo bei laiko kontekstą modelis reaguoja į dalinai pažįstamas ir nepažįstamas prisijungimo aplinkybes. Taip pat siekiama stebėti, kaip tokiose situacijose kinta atskiri kontekstiniai įverčiai $P_{ssidHour}$, P_{ssid}, P_{hour}, bei kaip jų pokyčiai atsispindi galutinio pasitikėjimo lygio kitime. Tokiu būdu eksperimentas leidžia įvertinti, ar modelis jautriai ir nuosekliai reaguoja į skirtingo konteksto prisijungimo scenarijus.

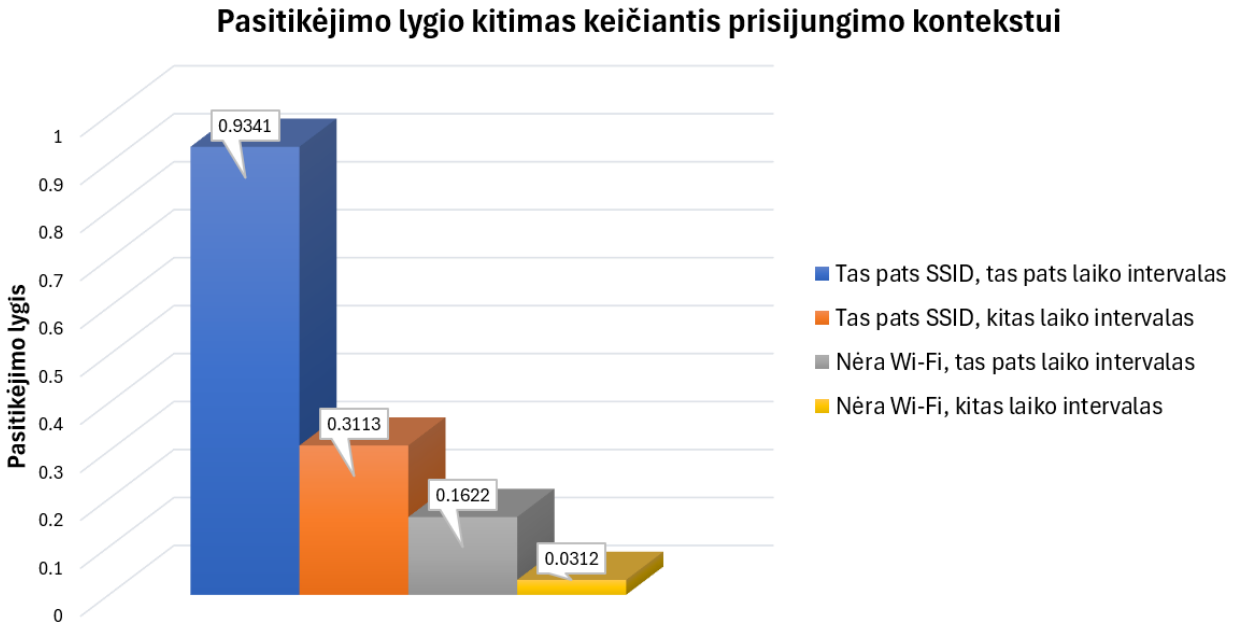
4.5.2. Eksperimento eiga

Eksperimentas buvo atliekamas naudojant jau susiformavusį naudotojo profilį, kuris prieš tai buvo sukurtas kartojant sėkmingas autentifikacijos sesijas nekintančiame prisijungimo kontekste. Vertinimo metu buvo pasirinkti keli kontroliuojami scenarijai, kuriuose keičiamas laiko kontekstas, tinklo kontekstas arba abu kartu. Tokiu būdu buvo siekiama praktiškai patikrinti, kaip modelis reaguoja į dalinai pažįstamas ir mažiau pažįstamas prisijungimo aplinkybes. Kiekvieno scenarijaus metu buvo registruojami atskiri kontekstiniai įverčiai $P_{ssidHour}$, P_{ssid}, P_{hour} ir galutinis pasitikėjimo lygis T. Eksperimento metu buvo vertinami trys scenarijai: prisijungimas naudojant tą patį SSID, bet kitą laiko intervalą, prisijungimas be Wi-Fi tame pačiame laiko intervale ir prisijungimas be Wi-Fi kitame laiko intervale (žr. **4 lentelė.** Kintantčio konteksto prisijungimų duomenys).

4 lentelė. Kintantčio konteksto prisijungimų duomenys

Scenarijus	P_{hour}	P_{ssid}	$P_{ssidHour}$	Pasitikėjimo lygis T
Tas pats SSID, tas pats laiko intervalas	0.7380	0.9687	0.9687	0.9341
Tas pats SSID, kitas laiko intervalas	0.0238	0.9687	0.0312	0.3113
Tas pats SSID, kitas laiko intervalas	0.0465	0.9696	0.0588	0.3302
Tas pats SSID, kitas laiko intervalas	0.0681	0.9705	0.0857	0.3485
Nėra Wi-Fi, tas pats laiko	0.7380	0.0606	0.0606	0.1622

intervalas				
Nėra Wi-Fi, tas pats laiko intervalas	0.7441	0.0882	0.0882	0.1866
Nėra Wi-Fi, tas pats laiko intervalas	0.75	0.1142	0.1142	0.2096
Nėra Wi-Fi, kitas laiko intervalas	0.1143	0.0167	0.0164	0.0312
Nėra Wi-Fi, kitas laiko intervalas	0.1268	0.0323	0.0317	0.0462
Nėra Wi-Fi, kitas laiko intervalas	0.1389	0.0476	0.0469	0.0609



15 pav. Pasitikėjimo lygio kitimas keičiantis prisijungimo kontekstui

Pateikti duomenys parodo (žr. **15 pav.** Pasitikėjimo lygio kitimas keičiantis prisijungimo kontekstui), kad pasitikėjimo lygis mažėja didėjant konteksto prisijungimo duomenų nuokrypiui nuo anksčiau suformuoto profilio. Tai rodo, kad modelis skirtingai vertina visiškai pažįstamus, dalinai pažįstamus ir nepažįstamus prisijungimo scenarijus.

4.5.3. Rezultatų analizė

Eksperimento rezultatai parodė, kad susiformavus naudotojo profiliui pasitikėjimo lygis jautriai reaguoja į prisijungimo konteksto pokyčius. Baziniame scenarijuje, kai išlaikomas tas pats SSID ir tas pats laiko intervalas, pasitikėjimo lygis išlieka aukštas ir siekia 0,9341. Pakeitus tik laiko intervalą, tačiau išlaikant tą patį SSID, pasitikėjimo lygis sumažėja iki 0,3113 - 0,3485. Tai rodo, kad modelis pažįstamą tinklą vertina kaip stiprų atpažinimo signalą, tačiau naujas laiko intervalas sumažina bendrą konteksto įvertį $P_{ssidHour}$, todėl mažėja ir bendras pasitikėjimo lygis. Išjungus Wi-Fi ir išlaikant tą patį laiko intervalą, pasitikėjimo lygis sumažėja dar labiau ir siekia 0.1622 - 0.2096. Šiuo atveju matyti, kad laiko kontekstas išlieka tas pats, tačiau tinklo konteksto įverčiai P_{ssid}, $P_{ssidHour}$ smarkiai sumažėja, nes sistema neberanda anksčiau sukaupto profiliui pažįstamo tinklo požymio.

Tai leidžia teigti, kad modelis skiria reikšmingą svarbą tinklo kontekstui, o vien įprasto laiko intervalo nepakanka išlaikyti aukštam pasitikėjimo lygiui. Didžiausias pasitikėjimo lygio sumažėjimas stebimas scenarijuje, kai tuo pačiu metu nėra Wi-Fi ir pasikeičia laiko intervalas. Tokiu atveju pasitikėjimo lygis sumažėja iki 0,0312 - 0,0609, o tai rodo, kad modelis tokį prisijungimo scenarijų vertina kaip labai nepatikimą. Šie rezultatai leidžia daryti išvadą, kad siūlomas modelis nuosekliai atspindi skirtingą prisijungimo scenarijų pažįstamumo lygį: mažiausias pasitikėjimo lygis nustatomas tada, kai vienu metu abu pagrindiniai kontekstiniai signalai neatitinka standartinio profilio, o dalinis konteksto pokytis lemia tarpinį pasitikėjimo lygio sumažėjimą. Tokiu būdu eksperimentas patvirtina, kad modelis geba nuosekliai reaguoti į konteksto pokyčius.

4.6. Elgsenos pokyčių prisitaikymo vertinimas

4.6.1. Eksperimento tikslas

Šio eksperimento tikslas yra įvertinti, kaip siūlomas modelis prisitaiko prie naudotojo elgsenos pokyčio, kai po pradinio profilio susiformavimo pasikeičia įprastas prisijungimo tinklo kontekstas naudotas formavimosi metu. Eksperimentu siekiama nustatyti, ar modelis, geba palaipsniui mažinti nepažįstamo tinklo riziką, kai pasikeičia pastovus tinklo prisijungimo kontekstas. Taip pat siekiama stebėti, kaip šio proceso metu kinta pasitikėjimo lygis ir atskiri kontekstiniai įverčiai, bei ar anksčiau susiformavęs pažįstamas kontekstas išlieka atpažįstamas grįžus po tam tikro prisijungimų kiekio. Tokiu būdu bandoma įvertinti, ar modelis geba prisitaikyti prie naujos elgsenos neprarasdamas anksčiau sukauptos profilio kontekstinės informacijos.

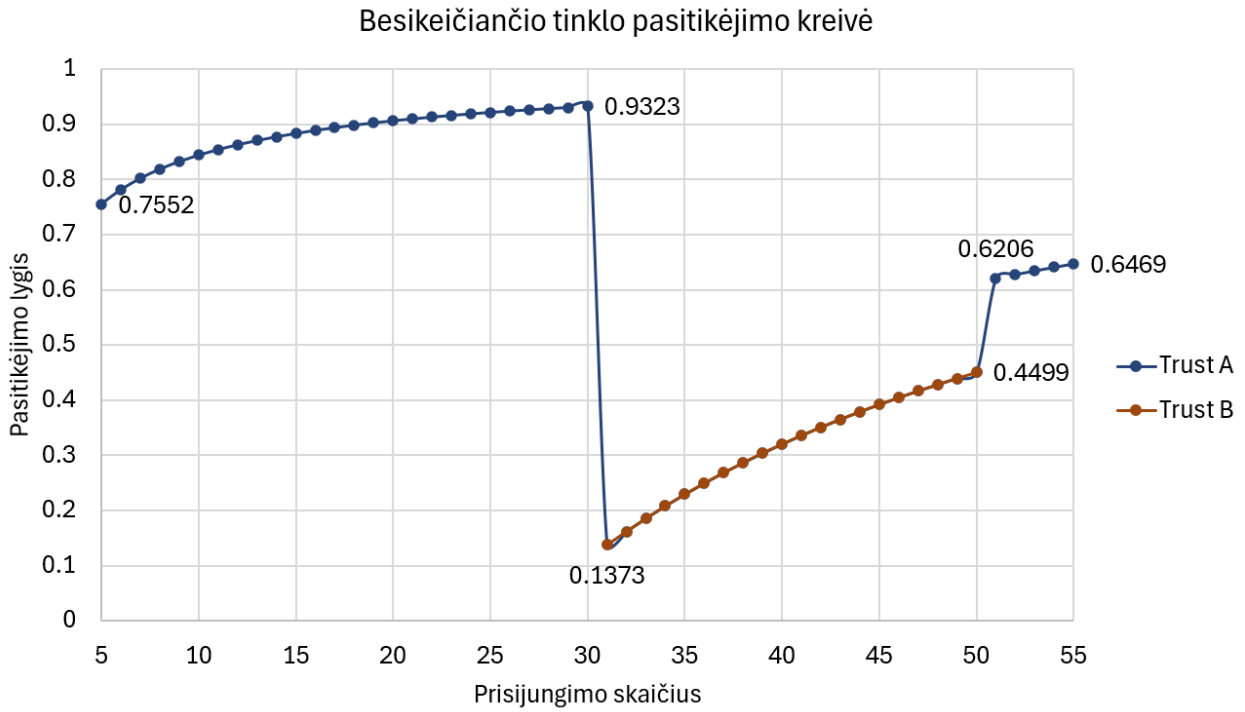
4.6.2. Eksperimento eiga

Eksperimentas buvo atliekamas, siekiant įvertinti modelio prisitaikymą prie pasikeitusio tinklo konteksto. Pirmoje eksperimento fazėje buvo suformuotas pradinis naudotojo profilis, atliekant 30 sėkmingų autentifikacijos prisijungimų išlaikant prisijungimo kontekstą, naudojant tą patį tinklo identifikatorių SSID-A ir tą patį paros laiko intervalą. Antroje fazėje, nekeičiant laiko intervalo, prisijungimo tinklo kontekstas buvo pakeistas į SSID-B ir šiame naujame kontekste atlikta 20 papildomų sėkmingų autentifikacijos prisijungimų. Trečioje fazėje prisijungimo kontekstas buvo vėl grąžintas į SSID-A, tame pačiame laiko intervale atliekant dar 5 sėkmingas autentifikacijas (žr. **5 lentelė.** Besikeičiančio tinklo konteksto duomenys). Tokia eksperimento eiga leido stebėti pasitikėjimo lygio pokytį pereinant į naują tinklo kontekstą, tiek modelio reakciją grįžus prie įprasto prisijungimo tinklo. Kiekvienos sesijos metu buvo registruojamas prisijungimo skaičius, pasitikėjimo lygis ir atskiri kontekstiniai įverčiai $P_{ssidHour}$, P_{ssid} ir P_{hour}. Kadangi šiame eksperimente svarbus nuoseklus perėjimas tarp skirtingų kontekstų, tolesniam vertinimui pateikiama pilna 55 prisijungimų sekos lentelė.

5 lentelė. Besikeičiančio tinklo konteksto duomenys

Prisijungimo Nr.	Tinklas	P_{hour}	P_{ssid}	$P_{ssidHour}$	Pasitikėjimo lygis T
1.	SSID-A	0,0769	0,5000	0,5000	0,4365
2.	SSID-A	0,1538	0,6667	0,6667	0,5897

3.	SSID-A	0,2143	0,7500	0,7500	0,6696
4.	SSID-A	0,2667	0,8000	0,8000	0,7200
5.	SSID-A	0,3125	0,8333	0,8333	0,7552
6.	SSID-A	0,3529	0,8571	0,8571	0,7815
7.	SSID-A	0,3889	0,8750	0,8750	0,8021
8.	SSID-A	0,4211	0,8889	0,8889	0,8187
9.	SSID-A	0,4500	0,9000	0,9000	0,8325
10.	SSID-A	0,4762	0,9091	0,9091	0,8442
11.	SSID-A	0,5000	0,9167	0,9167	0,8542
12.	SSID-A	0,5217	0,9231	0,9231	0,8629
13.	SSID-A	0,5417	0,9286	0,9286	0,8705
14.	SSID-A	0,5600	0,9333	0,9333	0,8773
15.	SSID-A	0,5769	0,9375	0,9375	0,8834
16.	SSID-A	0,5926	0,9412	0,9412	0,8889
17.	SSID-A	0,6071	0,9444	0,9444	0,8938
18.	SSID-A	0,6207	0,9474	0,9474	0,8984
19.	SSID-A	0,6333	0,9500	0,9500	0,9025
20.	SSID-A	0,6452	0,9524	0,9524	0,9063
21.	SSID-A	0,6563	0,9545	0,9545	0,9098
22.	SSID-A	0,6667	0,9565	0,9565	0,9130
23.	SSID-A	0,6765	0,9583	0,9583	0,9161
24.	SSID-A	0,6857	0,9600	0,9600	0,9189
25.	SSID-A	0,6944	0,9615	0,9615	0,9215
26.	SSID-A	0,7027	0,9630	0,9630	0,9239
27.	SSID-A	0,7105	0,9643	0,9643	0,9262
28.	SSID-A	0,7179	0,9655	0,9655	0,9284
29.	SSID-A	0,7250	0,9667	0,9667	0,9304
30.	SSID-A	0,7317	0,9677	0,9677	0,9323
31.	SSID-B	0,7381	0,0313	0,0313	0,1373
32.	SSID-B	0,7442	0,0588	0,0588	0,1616
33.	SSID-B	0,7500	0,0857	0,0857	0,1854
34.	SSID-B	0,7556	0,1111	0,1111	0,2078
35.	SSID-B	0,7609	0,1351	0,1351	0,2290
36.	SSID-B	0,7660	0,1579	0,1579	0,2491
37.	SSID-B	0,7708	0,1795	0,1795	0,2682
38.	SSID-B	0,7755	0,2000	0,2000	0,2863
39.	SSID-B	0,7800	0,2195	0,2195	0,3036
40.	SSID-B	0,7843	0,2381	0,2381	0,3200
41.	SSID-B	0,7885	0,2558	0,2558	0,3357
42.	SSID-B	0,7925	0,2727	0,2727	0,3507
43.	SSID-B	0,7963	0,2889	0,2889	0,3650
44.	SSID-B	0,8000	0,3043	0,3043	0,3787
45.	SSID-B	0,8036	0,3191	0,3191	0,3918
46.	SSID-B	0,8070	0,3333	0,3333	0,4044
47.	SSID-B	0,8103	0,3469	0,3469	0,4164
48.	SSID-B	0,8136	0,3600	0,3600	0,4280
49.	SSID-B	0,8167	0,3725	0,3725	0,4392
50.	SSID-B	0,8197	0,3846	0,3846	0,4499
51.	Grįžimas į SSID-A	0,8226	0,5849	0,5849	0,6206
52.	Grįžimas į SSID-A	0,8254	0,5926	0,5926	0,6275
53.	Grįžimas į SSID-A	0,8281	0,6000	0,6000	0,6342
54.	Grįžimas į SSID-A	0,8308	0,6071	0,6071	0,6407
55.	Grįžimas į SSID-A	0,8333	0,6140	0,6140	0,6469



16 pav. Kintančio tinklo pasitikėjimo variacija

Pasitikėjimo kreivė (žr. **16 pav.** Kintančio tinklo pasitikėjimo variacija), rodo, kad modelis jautriai reaguoja į tinklo konteksto pasikeitimą. Tolesni prisijungimai naujajame kontekste lėmė laipsnišką pasitikėjimo augimą, tačiau grįžus prie anksčiau naudoto SSID-A pasitikėjimo lygis nebepasiekė ankstesnės reikšmės, buvusios prieš konteksto pasikeitimą. Tai rodo, kad modelis, prisitaikydamas prie naujo tinklo konteksto, kartu sumažina anksčiau sukaupto konteksto duomenų svarbą ir perskirsto pasitikėjimą pagal pakitusę naudotojo elgseną.

4.6.3. Rezultatų analizė

Eksperimento metu pastebėta, jog pasikeitus tinklo kontekstui pasitikėjimo lygis iš pradžių reikšmingai sumažėja, tačiau naujam scenarijui kartojantis vėl pradeda nuosekliai augti. Pirmoje fazėje, naudojant SSID-A, pasitikėjimo lygis padidėjo nuo 0,4365 iki 0,9323. Perėjus į SSID-B, jis staigiai sumažėjo iki 0,1373, tačiau toliau kartojant prisijungimus išlaikant nuająjį tinklo kontekstą pakilo iki 0,4499. Tai rodo, kad modelis naują tinklo kontekstą iš pradžių vertina kaip mažiau pažįstamą, bet palaipsniui jį įtraukia į patikimą naudotojo profilį. Grįžus prie SSID-A, pasitikėjimo lygis vėl padidėjo iki 0,6206 ir toliau kilo, todėl galima teigti, kad modelis prisitaiko prie naujo konteksto neprarasdamas visos anksčiau sukauptos informacijos.

4.7. Laikinio silpnėjimo vertinimas

4.7.1. Eksperimento tisklas

Šio eksperimento tikslas yra įvertinti, kaip siūlomame modelyje kinta pasitikėjimo lygis, kai jis naudojamas ne nuolat, bet tik periodiškai po ilgesnių neveiklumo tarpų. Eksperimentu siekiama nustatyti, ar po neveiklumo laikotarpio pasitikėjimo profilis palaipsniui silpnėja ir dėl to sistema tą patį prisijungimo kontekstą pradeda vertinti mažiau patikimai. aip pat

siekiama stebėti, kaip laikui bėgant kinta atskiri kontekstiniai įverčiai, bei gauti rezultatai atitinka modelyje taikomą laikinio silpnėjimo logiką. Tokiu būdu eksperimentas leidžia įvertinti, ar ilgiau nesinaudojant sistema anksčiau sukauptas pasitikėjimo profilis natūraliai silpnėja.

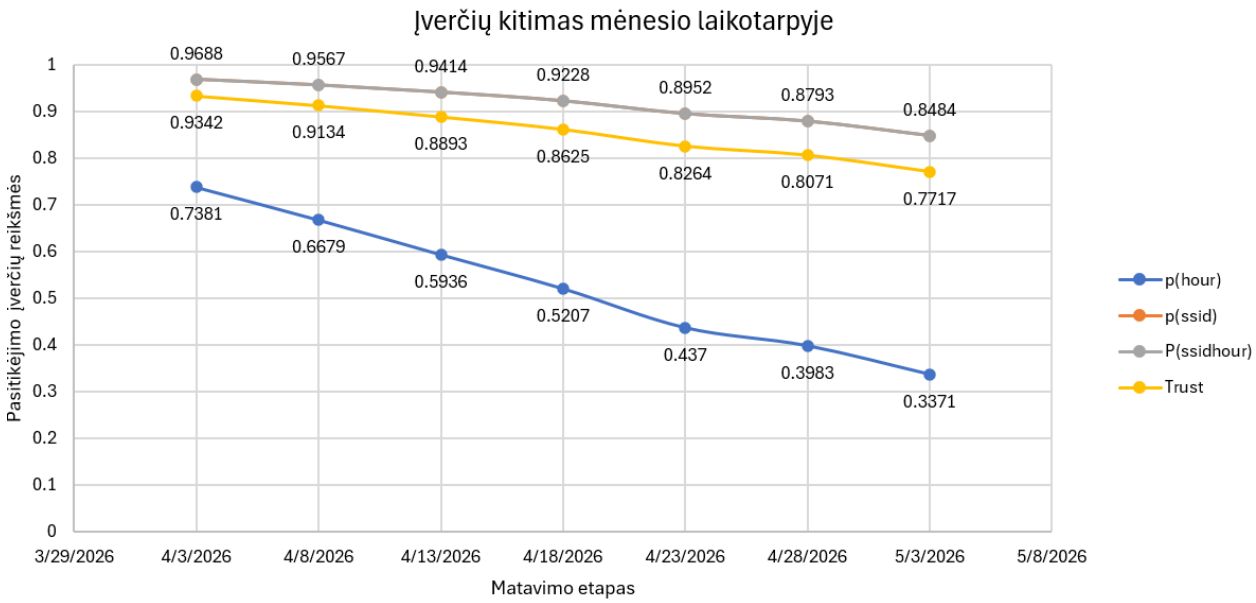
4.7.2. Eksperimento eiga

Eksperimentas buvo atliekamas naudojant jau susiformavusį naudotojo profilį, kuris prieš tai buvo sukurtas stabiliame prisijungimo kontekste, naudojant tą patį tinklo identifikatorių ir tą patį paros laiko intervalą. Skirtingai nuo ankstesnių pasyviojo adaptyvumo eksperimentų, šiame vertinime sistema buvo tikrinama iteracijomis. Prisijungimai buvo atliekami periodiškai kas penkias dienas, išlaikant tą patį prisijungimo kontekstą. Taip buvo siekiama stebėti, kaip laikui bėgant silpnėja anksčiau sukauptas pasitikėjimo profilis. Kadangi eksperimento metu prisijungimo kontekstas nebuvo keičiamas, gauti pasitikėjimo lygio pokyčiai gali būti siejami su laiko poveikiu ir neveiklumo intervalais, o ne su tinklo ar laiko intervalo pokyčiu.

Vertinimo metu buvo registruojami įverčiai, prisijungimo data, $P_{ssidHour}$, P_{ssid}, P_{hour} ir pasitikėjimo lygis T. Pirmasis matavimas buvo atliktas su katik susiformavusiu profiliu, o vėlesni matavimai vykdyti kas penkias dienas. Tokiu būdu buvo siekiama praktiškai patikrinti, ar laikui bėgant pasitikėjimo lygis mažėja nuosekliai, net ir nekeičiant įprasto prisijungimo konteksto.

6 lentelė. Pasitikėjimo lygio kitimo lentelė

Matavimo etapas	Data	P_{hour}	P_{ssid}	$P_{ssidHour}$	Pasitikėjimo lygis T
Pradinis matavimas	2026-04-03	0,7381	0,9688	0,9688	0,9342
1 iteracija	2026-04-08	0,6679	0,9567	0,9567	0,9134
2 iteracija	2026-04-13	0,5936	0,9414	0,9414	0,8893
3 iteracija	2026-04-18	0,5207	0,9228	0,9228	0,8625
4 iteracija	2026-04-23	0,4370	0,8952	0,8952	0,8264
5 iteracija	2026-04-28	0,3983	0,8793	0,8793	0,8071
6 iteracija	2026-05-03	0,3371	0,8484	0,8484	0,7717



17 pav. Kontekstinių duomenų ir pasitikėjimo kitimas mėnesio laikotarpyje

Pateikti duomenys (žr. **17 pav.** Kontekstinių duomenų ir pasitikėjimo kitimas mėnesio laikotarpyje) rodo, kad laikui bėgant nuosekliai mažėja bendras pasitikėjimo lygis ir kiti kontekstiniai įverčiai, tačiau laiko konteksto reikšmė silpnėja greičiau nei tinklo identifikatoriaus reikšmė. Tai susiję ne tik su taikomu laikinio silpnėjimo mechanizmu, bet ir su pačia modelio skaičiavimo logika. Laiko signalas vertinamas platesniame galimų intervalų rinkinyje, todėl mažėjant sukauptam profilio svoriui jo įvertis greičiau artėja prie žemos bazinės reikšmės. Tai reiškia, kad po neveiklumo laikotarpio pasitikėjimas tinklo kontekstu mažėja lėčiau negu pasitikėjimas prisijungimo laiko kontekstu.

4.7.3. Rezultatų analizė

Eksperimento rezultatai parodė, nors prisijungimo kontekstas išlieka nepakitęs, periodiškai tikrinant sistemą po penkių dienų neveiklumo intervalų pasitikėjimo lygis palaipsniui mažėja. Pradiniame matavime pasitikėjimo lygis siekė 0,9342, o paskutinėje iteracijoje sumažėjo iki 0,7717. Tai rodo, kad seniau surinkti kontekstiniai duomenys laikui bėgant turi mažesnį svorį. Eksperimento metu buvo išlaikytas tas pats tinklo identifikatorius ir paros laiko intervalas. Dėl to stebėtas pasitikėjimo lygio mažėjimas gali būti siejamas su modelyje taikomu laiku paremtu silpnėjimo mechanizmu. Tokia logika svarbi saugumo požiūriu, nes sistema ilgainiui silpnina anksčiau sukauptą pasitikėjimą ir neleidžia senam profiliui išlikti nepakitusiam neribotą laiką.

4.8. Balso autentifikavimo veikimo priklausomybės nuo triukšmo vertinimas

4.8.1. Eksperimento tikslas

Šio eksperimento tikslas yra įvertinti, kaip aplinkos triukšmo lygis veikia balso autentifikavimo metodo veikimą siūlomame modelyje. Kadangi balso autentifikavimas priklauso nuo aplinkos sąlygų, būtina nustatyti, kokiame triukšmo lygyje šis metodas dar gali būti taikomas pakankamai patikimai, o nuo kada jo veikimas pradeda tapti nestabilus. Eksperimentu siekiama praktiškai stebėti, kaip didėjantis aplinkos triukšmas įtakoje balso

autentifikavimo rezultatus ir koks triukšmo blokavimo slenkstis yra tinkamas sukurtam modeliui. Tokiu būdu vertinama, ar balso autentifikavimo ribojimas esant didesniam triukšmui gali būti laikomas praktiškai tinkamu sprendimu adaptyvaus autentifikavimo modelyje.

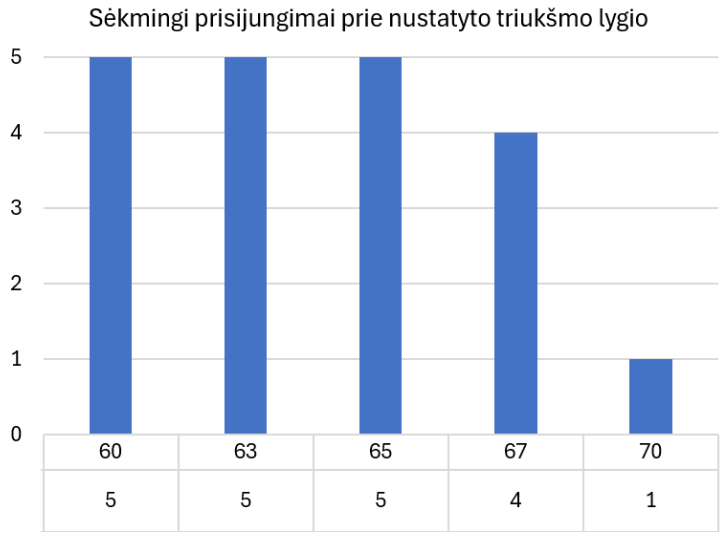
4.8.2. Eksperimento eiga

Eksperimentas buvo atliekamas kontroliuojamomis sąlygomis, siekiant įvertinti, kaip skirtingas aplinkos triukšmo lygis veikia balso autentifikavimo rezultatus. Bandymo metu buvo išlaikoma pastovi naudotojo padėtis įrenginio atžvilgiu, o atstumai tarp eksperimente naudotų objektų buvo fiksuoti. Atstumas tarp naudotojo burnos ir mikrofono siekė 11 cm, atstumas tarp mikrofono ir garso šaltinio – 3 cm, atstumas tarp garso šaltinio ir garso matuoklio – 7 cm, o tarp mikrofono ir garso matuoklio – 5 cm. Tokiu būdu buvo siekiama išlaikyti kuo panašesnes matavimo sąlygas tarp atskirų bandymų.

Kaip pradinė atskaitos reikšmė buvo pasirinktas 60 dB triukšmo lygis, atitinkantis įprasto pokalbio aplinką. Toliau triukšmo lygis buvo didinamas iki ~63 dB, ~65 dB, ~67 dB ir ~70 dB. Kiekviename triukšmo lygyje buvo atlikti 5 balso autentifikavimo bandymai, registruojant, kiek iš jų buvo sėkmingi (žr. **6 lentelė.** Sėkmingi prisijungimai prie nustatyto triukšmo lygio). Šis eksperimentas leido palyginti balso autentifikavimo veikimą esant palaipsniui blogėjančioms aplinkos sąlygoms ir įvertinti, nuo kurio triukšmo lygio metodo patikimumas pradeda pastebimai mažėti.

7 lentelė. Sėkmingi prisijungimai prie nustatyto triukšmo lygio

Triukšmo lygis, dB	Sėkmingų autentifikacijų skaičius
60	5
63	5
65	5
67	4
70	1



18 pav. Sėkmingų prisijungimų prie nustatyto triukšmo lygio palyginimas

Remiantis rezultatais (žr. **18 pav.** Sėkmingų prisijungimų prie nustatyto triukšmo lygio palyginimas) matyti, kad iki 65 dB metodo veikimas išlieka stabilus, tačiau didesnis triukšmo lygis lemia pastebimą sėkmingų autentifikacijų mažėjimą. Tai leidžia pagrįsti pasirinkto triukšmo slenksčio tinkamumą.

4.8.3. Rezultatų analizė

Eksperimento rezultatai parodė, kad balso autentifikavimo metodo patikimumas tiesiogiai priklauso nuo aplinkos triukšmo lygio. Esant maždaug 60 dB, 63 dB ir 65 dB triukšmo lygiui visi 5 iš 5 bandymų buvo sėkmingi, todėl galima teigti, kad šiame intervale balso autentifikavimo metodas veikė stabiliai. Padidinus triukšmo lygį iki maždaug 67 dB, sėkmingų bandymų skaičius sumažėjo iki 4 iš 5, o ties maždaug 70 dB sėkmingas buvo tik 1 iš 5 bandymų. Tai rodo, kad ties maždaug 67 dB balso autentifikavimo patikimumas pradeda mažėti, o ties 70 dB metodo veikimas tampa nestabilus.

Eksperimento rezultatai parodė, kad balso autentifikavimo metodo patikimumas tiesiogiai priklauso nuo aplinkos triukšmo lygio. Esant maždaug 60 dB, 63 dB ir 65 dB triukšmo lygiui visi 5 iš 5 bandymų buvo sėkmingi, todėl galima teigti, kad šiame intervale balso autentifikavimo metodas veikė stabiliai. Padidinus triukšmo lygį iki maždaug 67 dB, sėkmingų bandymų skaičius sumažėjo iki 4 iš 5, o ties maždaug 70 dB sėkmingas buvo tik 1 iš 5 bandymų. Tai rodo, kad ties maždaug 67 dB balso autentifikavimo patikimumas pradeda mažėti, o ties 70 dB metodo veikimas tampa aiškiai nestabilus.

4.9. Išvados

1. Tapatybės profilio formavimosi vertinimas patvirtino, kad pasyvusis naudotojo profilis stabilioje aplinkoje formuojasi nuosekliai, o mokymosi fazė atlieka apsauginę funkciją. Nors pasitikėjimo lygis nekintančiame kontekste augo sparčiai, iki nustatytos ribos sistema išlaikė „LEARNING“ būseną, todėl autentifikavimo griežtumas nebuvo sumažintas per anksti.
2. Pasitikėjimo lygio stabilumo eksperimentas parodė, kad susiformavus profiliui pasitikėjimo lygis nekintančiame kontekste ir toliau didėja, tačiau jo augimas palaipsniui lėtėja. Tai leidžia daryti išvadą, kad modelio išvestis praktiškai stabilizuojasi, o papildomi to paties konteksto prisijungimai daro vis mažesnę įtaką bendram pasitikėjimo lygiui.
3. Konteksto jautrumo ir rizikos priskyrimo eksperimentas patvirtino, kad siūlomas modelis nuosekliai reaguoja į prisijungimo aplinkos pokyčius, o pasitikėjimo lygis mažėja proporcingai tam, kiek naujas scenarijus nutolsta nuo anksčiau suformuoto profilio. Išlaikant tą patį tinklą, bet pakeitus laiko intervalą, pasitikėjimo lygis sumažėjo vidutiniškai, o išjungus Wi-Fi ir kartu pakeitus laiko intervalą – labiausiai. Tai leidžia teigti, kad modelis geba atskirti ir įvertinti dalinai pažįstamas ir nepažįstamas prisijungimo situacijas
4. Konteksto jautrumo ir elgsenos pokyčių vertinimas leido įsitikinti, kad modelis nuosekliai reaguoja į prisijungimo aplinkos pokyčius ir geba prisitaikyti prie naujo tinklo konteksto be profilio permokinimo gržtant į LEARNING būseną. Pasikeitus tinklo ar laiko signalams, pasitikėjimo lygis reikšmingai mažėjo, o kartojantis naujam

scenarijui pradėjo vėl augti, kartu išlaikant dalį anksčiau sukauptos informacijos apie pradinį kontekstą.

5. Laikinio silpnėjimo vertinimas patvirtino, kad net ir nekeičiant prisijungimo konteksto pasitikėjimo lygis laikui bėgant palaipsniui mažėja, jei sistema naudojama tik periodiškai su neveiklumo intervalais. Tai rodo, kad anksčiau sukauptas pasitikėjimo profilis nėra laikomas pastoviu, o anksčiau surinkti kontekstiniai duomenys modelyje laikui bėgant praranda svorį.
6. Balso autentifikavimo priklausomybės nuo triukšmo eksperimentas parodė, kad šio metodo patikimumas tiesiogiai susijęs su aplinkos sąlygomis, todėl jo ribojimas didesnio triukšmo atveju yra praktiškai pagrįstas. Gauti rezultatai leidžia teigti, kad maždaug ties 67 dB balso autentifikavimo stabilumas pradeda mažėti, o ties 70 dB metodo veikimas tampa aiškiai nepatikimas, todėl pasirinktas balso autentifikavimo blokavimo slenkstis apie 67 dB gali būti laikomas praktiškai tinkamu siūlomam modeliui.

Literatūra

1. Wahidin, H., Waycott, J., & Baker, S. (2018). The challenges in adopting assistive technologies in the workplace for people with visual impairments. In Proceedings of the 30th Australian Conference on Computer-Human Interaction (OzCHI ’18). ACM. https://doi.org/10.1145/3292147.3292175

2. Evtimova, P. ir Nicholson, J. (2021). Exploring the acceptability of graphical passwords for people with dyslexia. In Human-Computer Interaction – INTERACT 2021: 18th IFIP TC 13 International Conference, Bari, Italy, August 30 – September 3, 2021, Proceedings, Part I (pp. 213–222). Springer. https://doi.org/10.1007/978-3-030-85623-6_14

3. Lewis, B. ir Venkatasubramanian, K. (2021). “I...Got my Nose-Print. But it Wasn’t Accurate”: How People with Upper Extremity Impairment Authenticate on their Personal Computing Devices. In CHI Conference on Human Factors in Computing Systems (CHI ’21). ACM. https://doi.org/10.1145/3411764.3445070

4. Andrew, S. Watson, S. Oh, T. Tigwell, G.W. A Review of Literature on Accessibility and Authentication Techniques. In The 22nd International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS ’20). ACM. https://doi.org/10.1145/3373625.3418005

5. Vatavu, R.-D. ir Ungurean, O.-C. (2022). Understanding gesture input articulation with upper-body wearables for users with upper-body motor impairments. In CHI Conference on Human Factors in Computing Systems (CHI ’22). ACM. (pp. 1–16). https://doi.org/10.1145/3491102.3501964

6. Briotto Faustino, D. ir Girouard, A. (2018). Understanding authentication method use on mobile devices by people with vision impairment. In The 20th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS ’18). ACM (pp. 217–228). https://dl.acm.org/doi/10.1145/3234695.3236342

7. Bhole, P. V., Li, Z., Bokolia, S., Oh, T., Tigwell, G. W., & Peiris, R. L. (2024). Haptic2FA: Haptics-based accessible two-factor authentication for blind and low vision people. Proceedings of the ACM on Human-Computer Interaction, 8(MHCI), Article 264. https://doi.org/10.1145/3676509

8. Fuglerud, K. S. ir Dale, Ø. (2011). Secure and inclusive authentication with a talking mobile one-time-password client. IEEE Security & Privacy, 27–34. https://doi.org/10.1109/MSP.2010.204

9. Lewis, B., Hebert, J., Venkatasubramanian, K., Provost, M., & Charlebois, K. (2020). A new authentication approach for people with upper extremity impairment. In IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Austin, TX, USA (pp. 1–6). IEEE. https://doi.org/10.1109/PerComWorkshops48775.2020.9156171.

10. Price, A. ir Loizides, F. (2024). Allowing for secure and accessible authentication for individuals with disabilities of dexterity. In Human-Centered Software Engineering: 10th IFIP WG 13.2 International Working Conference, HCSE 2024, Reykjavik, Iceland, July 8–10, 2024, Proceedings (pp. 133–146). Springer. https://doi.org/10.1007/978-3-031-64576-1_7

11. Olaniyi, O. M., Bala, J. A., Ndunagu, J., Abubakar, A., & Is'Haq, A. (2019). V-Authenticate: Voice authentication system for electorates living with disability. In Cyber Secure Nigeria 2019 Conference (pp. 29–38).

12. Toussaint, C., Chateau, B., Gourio-Jewell, P.-G., Bonnefoy, E., & Louveton, N. (2025). Inclusive by design: Developing barrier-free authentication for blind and low vision users through the ALIAS project. In Proceedings of the 36th Annual Conference of the European Association of Cognitive Ergonomics (ECCE '25), Tallinn, Estonia. ACM. https://doi.org/10.1145/3746175.3746210

13. FIDO Alliance. (2022, rugpjūtis). Guidance for making FIDO deployments accessible to users with disabilities. https://fidoalliance.org

14. ten Brink, R. N. ir Scollan, R. I. (2019). Usability of biometric authentication methods for citizens with disabilities (MITRE Technical Report No. MTR190511). The MITRE Corporation.

15. Arias-Cabarcos, P., Krupitzer, C., & Becker, C. (2019). A survey on adaptive authentication. ACM Computing Surveys, 52(4), Article 80. https://doi.org/10.1145/3336117

16. Wiefling, S., Durmuth, M., & Lo Iacono, L. (2021). Verify It's You: How users perceive risk-based authentication. IEEE Security & Privacy. https://doi.org/10.1109/MSEC.2021.3077954

17. Progonov, D., Cherniakova, V., Kolesnichenko, P., & Oliynyk, A. (2022). Behavior-based user authentication on mobile devices in various usage contexts. EURASIP Journal on Information Security, 2022, Article 6. https://doi.org/10.1186/s13635-022-00132-x

18. Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj

19. Charter of Fundamental Rights of the European Union. (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016P/TXT

20. *Lietuvos Respublikos asmens su negalia teisių apsaugos pagrindų įstatymas, Nr. I-2044. (1991). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.2319/asr*