

**RADA NAUKOWA DYSCYPLINY
INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI WARSZAWSKIEJ**

zaprasza
na

PUBLICZNĄ OBRONĘ ROZPRAWY DOKTORSKIEJ
mgr. inż. Pawła ŁĄKI

która odbędzie się w dniu 9 listopada 2021 roku o godzinie 10:00 w trybie

zdalnym na platformie MS Teams*.

Temat rozprawy doktorskiej:

„Wieloskładnikowe i transparentne uwierzytelnianie użytkownika z wykorzystaniem technik uczenia maszynowego”

Promotor: dr hab. inż. Wojciech Mazurczyk- Politechnika Warszawska

Recenzenci: dr hab. inż. Bogdan Księżopolski - Uniwersytet Marii Curie-Skłodowskiej w Lublinie

dr hab. inż. Rafał Kozik – Uniwersytet Technologiczno-Przyrodniczy w Bydgoszczy

* Obrona odbędzie się zdalnie na platformie MS Teams. Osoby zainteresowane uczestnictwem w obronie proszone są o zgłoszenie chęci uczestnictwa w formie elektronicznej na adres sekretarza komisji: Mariusz Rawski – email : mariusz.rawski@pw.edu.pl w dniu 5 listopada 2021 do godz. 18:00

Z rozprawą doktorską i recenzjami można zapoznać się w Czytelnicy Biblioteki Głównej Politechniki Warszawskiej, Warszawa, Plac Politechniki 1.

Streszczenie rozprawy doktorskiej i recenzje są zamieszczone na stronie internetowej:

<https://admin.bip.pw.edu.pl/Postepowania-w-sprawie-nadania-stopnia-naukowego/Doktoraty/Wszczete-do-30-kwietnia-2019-r/Dyscyplina-informatyka-techniczna-i-telekomunikacja-dziedzina-nauk-inzynieryjno-technicznych/mgr-inz.-Pawel-Laka>

Przewodniczący Rady Naukowej Dyscypliny Informatyka Techniczna i Telekomunikacja Politechniki Warszawskiej

dr hab. inż. Jarosław Arabas

Streszczenie

W niniejszej rozprawie dokonano analizy istniejących sposobów potwierdzania tożsamości użytkowników z uwzględnieniem rozwiązań opublikowanych w literaturze oraz używanych komercyjnie. Wykazała ona brak kompleksowego podejścia, uwzględniającego zarówno wygodę użytkowników końcowych jak i bezpieczeństwo samego procesu uwierzytelniania, w związku z czym zaprojektowano oraz wykonano całościowy system uwierzytelniający.

Opracowany przez autora rozprawy system, służący potwierdzaniu tożsamości, wykorzystuje niezależne metody uwierzytelniania z obszarów wiedzy, posiadania, cech oraz zachowania użytkownika końcowego. W pracy przedstawiono i wykorzystano także nowe, zaprojektowane przez autora metody oparte na biometrii (analiza składu ciała oraz mierzenie czasu pomiędzy metodami). Praca prezentuje także pierwszy opublikowany w literaturze przykład użycia algorytmów sztucznej inteligencji do podejmowania decyzji o poprawnym uwierzytelnianiu użytkownika końcowego na podstawie wielu różnych metod.

Ponadto zaprojektowano i zrealizowano badania zaimplementowanego systemu z uwzględnieniem znanych metryk mierzenia systemów i metod uwierzytelniania. Wykonano zarówno eksperymenty dla zgodnego z założeniami użycia systemu weryfikując jego skuteczność, jak i zasymulowano różne scenariusze i przypadki innego użycia z uwzględnieniem próby oszukania takiego systemu.

Zbadane rozwiązanie, skupione zarówno na wygodzie użytkowników jak i bezpieczeństwie i ochronie danych, wykazało 100% skuteczność w poprawnym uwierzytelnianiu użytkownika. Uzyskane wyniki pozwalają na kontynuację badań w wielu kierunkach oraz efektywne wykorzystanie takiego systemu komercyjnie.

Słowa kluczowe: uwierzytelnianie użytkownika, uczenie maszynowe, cyberbezpieczeństwo

dr hab. inż. Rafał Kozik, profesor uczelni
Uniwersytet Technologiczno-Przyrodniczy
im. Jana i Jędrzeja Śniadeckich w Bydgoszczy,
Wydział Telekomunikacji, Informatyki i Elektrotechniki,
Al. prof. S. Kaliskiego 7,
85-796 Bydgoszcz

Bydgoszcz, 16.08.2021

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY NAUKOWEJ DYSCYPLINY INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI WARSZAWSKIEJ

Tytuł rozprawy: **Wieloskładnikowe i transparentne uwierzytelnianie użytkownika z wykorzystaniem technik uczenia maszynowego,**

Autor rozprawy: **mgr inż. Paweł Łąka**

- 1. Jakie zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, itd.)?**

Rozprawa, której Autorem jest Pan mgr inż. Paweł Łąka, dotyczy wieloskładnikowego uwierzytelniania użytkowników, które u swych podstaw wykorzystuje niezależne metody potwierdzania tożsamości. Zrealizowane jest to na podstawie tego co użytkownik wie, posiadania, czy też na podstawie cech biometrycznych oraz behawioralnych.

W swych badaniach, Pan mgr inż. Paweł Łąka, duży nacisk kładzie na wygodę użytkownika. Jest to uzasadnione na podstawie analizy literaturowej, która wykazała, że aktualnie brakuje kompleksowego rozwiązania biorącego pod uwagę zarówno bezpieczeństwo samego procesu uwierzytelniania jaki i wygodę użytkownika końcowego.

Proponowane przez Autora pracy podejście do uwierzytelniania użytkownika nie wymaga od niego żadnych wymuszonych (dodatkowych) czynności, co sprawia iż cały proces uwierzytelniania jest dla niego mniej uciążliwy. W tym świetle jasno sformułowana została teza rozprawy.

Jeśli chodzi o charakter rozprawy to jest on w mojej ocenie koncepcyjno-doświadczalny. Autor pracy stworzył prototyp proponowanego systemu oraz zebrał dane niezbędne do przeprowadzenia badań. Ponadto, zaplanował i wykonał różne eksperymenty, które pozwoliły ocenić proponowane rozwiązanie pod względem skuteczności i niezawodności.

Dodatkowym elementem, jaki można było wykonać w ramach pracy nad rozprawą, to ankieta oceny transparentności (czy uciążliwości) proponowanych przez Autora modalności (metod). Można było to wykonać niskim nakładem pracy w trakcie tworzenia profili użytkowników.

2. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł (w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle) świadczący o dostatecznej wiedzy Autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonujący?

Niniejsza rozprawa obejmuje najnowsze osiągnięcia nauki. Autor przedstawił bardzo rozległy rozdział omawiający wcześniejsze dokonania oraz aktualną literaturę dotyczącą zagadnień związanych z rozprawą doktorską. W szczególności dokonany został przegląd różnych metod uwierzytelniania z uwzględnieniem metod wieloskładnikowych.

Autor rozprawy, przedstawił również stan badań dotyczący metod uznawanych potencjalnie za wygodne i bezinwazyjne. Również przegląd literatury dotyczący wykorzystania uczenia maszynowego w procesach logowania jest przeprowadzony i przedstawiony w sposób właściwy.

Wnioski i spostrzeżenia z przeglądu źródeł przedstawiono bardzo szczegółowo i jasno. Pozwoliło to dobrze podkreślić sposób w jaki niniejsza rozprawa wyróżnia się na tle innych rozwiązań w literaturze.

3. Czy Autor rozwiązał postawione zagadnienia? Czy użył do tego właściwych metod i czy przyjęte założenia są uzasadnione?

W mojej ocenie Autor w sposób właściwy rozwiązał postawiony problem. W procesie tym użyte zostały właściwe narzędzia i metody. Tym samym Autor dowiódł, że posiadał umiejętności związane z metodyką i metodologią prowadzenia badań.

W szczególności badania i eksperymenty osadzone zostały na solidnej i głębokiej analizie literaturowej. Autor rozprawy odniósł się także do aktualnych trendów rozwojowych dotyczących uwierzytelniania i kontroli dostępu. W tym świetle zaprojektowany i zaimplementowany został prototyp proponowanego rozwiązania.

5. Czy Autor wykazał umiejętności poprawnego i przekonującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?

Nie mam wątpliwości, że Autor rozprawy posiada dużą wiedzę dotyczącą zagadnień związanych z tematem rozprawy doktorskiej. Doktorant wykazał się przede wszystkim umiejętnościami dotyczącymi prowadzenia badań naukowych, eksperymentów, projektowania systemów informatycznych oraz implementacji i programowania.

Również zrealizowane przez Autora rozprawy eksperymenty nie odbiegają od obowiązujących dobrych praktyk w zakresie pomiaru skuteczności systemów weryfikacji. Autor w tym zakresie użył znanych metryk co pozwala odnieść się do innych rozwiązań dostępnych w literaturze.

Ponadto, eksperymenty zostały dodatkowo rozszerzone o scenariusze, które pozwalają ocenić skuteczność proponowanego rozwiązania w momencie gdy wybrane funkcjonalności systemu zostają celowo zaatakowane.

6. Jakie są wady i słabe strony rozprawy?

Rolą recenzenta jest zauważenie i wskazanie pewnych niedociągnięć (czy mankamentów) ocenianej pracy, oraz zgłoszenie tych uwag, które mogą być potencjalnie przydatne w dalszych pracach badawczo-rozwojowych. Dlatego też do wad i słabych stron rozprawy zaliczam:

- Prezentacja graficzna wyników w rozdziale 7. W mojej ocenie wykresy zaprezentowane w rozdziale 7 powinny wykorzystywać osobne skale dla błędu FRR i FAR (np. lewa i prawa oś). Pozwoliłoby to lepiej ocenić różnice w wartościach, gdyż w aktualnej formie przebiegi FRR są „płaskie” i ściśnięte do wartości zerowych. Ponadto, prezentowanie wykresów dla zerowych wartości błędów (np. „pusty” wykres 7.10) nie ma większego sensu. Choć przykuwa to uwagę czytającego i podkreśla dobrą efektywność proponowanego systemu to w mojej ocenie taki zabieg jest niepotrzebny. Ponadto, umieszczenie punktowych wartości błędów na wykresach słupkowych również polepszyłoby czytelność prezentowanych wyników.
- Symulacja wystąpienia pewnych zdarzeń celem oceny ich wpływu na odpowiedź systemu IdP. W mojej ocenie, zastosowanie takich narzędzi jak SHAP czy LIME pozwoliłoby głębiej zrozumieć jaki jest wpływ poszczególnych serwisów (metod) identyfikacji w wypracowywaniu finalnej odpowiedzi przez poszczególne algorytmy uczenia maszynowego. Idąc dalej, Autor mógł, przy tak małej liczbie cech (6 metod identyfikacji) i danych uczących, wytrenować modele dla wszystkich kombinacji zaistniałych sytuacji (czyli brak odpowiedzi z poszczególnych serwisów). Ponadto, jeżeli mowa o systemach autoryzacji użytkownika, to (w mojej ocenie) system nie

powinien sam „radzić” sobie w momencie gdy brakuje odpowiedzi (czy też informacji) dla poszczególnych serwisów (metod).

- Odrzucenie w rozdziale 7.2.1 celowości analizy współczynnika FAR. Zasadniczo powód dlaczego FAR nie jest analizowany został dobrze uzasadniony przez Autora, ale istnieje pewne ryzyko, że atakujący poprzez modyfikacje odpowiedzi jednej z metod (przykładowo poprzez blokowanie sygnału Bluetooth) będzie próbował podnieść poziom swoich uprawnień poprzez podszycie się pod innego użytkownika.
- Celowość demonstracji i analizy wykresów 7.1-7.6. Początek rozdziału 7 pozwala głębiej zrozumieć rozkład wartości dla poszczególnych cech, jednak jego forma w mojej ocenie jest dość nietypowa. Dla czytającego prawdopodobnie bardziej zrozumiałą mogłaby być typowa analiza EDA (ang. Exploratory Data Analysis) wykonana dla poszczególnych cech (metod identyfikacji użytkownika). Jedną z popularnych bibliotek wspierających ten proces analizy dla języka Python jest Sweetviz.
- Celowość prezentowania rozdziału 5.6.3 a w szczególności detali związanych ze sposobem działania algorytmów uczenia maszynowego. W mojej ocenie opisy te mają charakter bardzo ogólny i są zbędne, gdyż nie wnoszą wiele do lepszego zrozumienia rozprawy przez czytającego.
- Pewne niedomówienia jeżeli chodzi o fizyczną realizację całego systemu. Przykładowo w rozdziale 5.5 mowa jest o trzymaniu kierownicy przy badaniu składu ciała. Natomiast w rozdziale 6.1 mowa jest o staniu na urządzeniu. Rodzi to pytanie czy możliwym jest badanie składu ciała poprzez trzymanie urządzenia (nawet odpowiednio przystosowanego czy zmodyfikowanego) i jak wiarygodny będzie taki pomiar.
- Patrząc na tabele 5.6 a w szczególności na czasy akwizycji z poszczególnych modułów (serwisów) można odnieść wrażenie, że niektóre z pomiarów są znacznie rozciągnięte w czasie. Rodzi to pytanie w kontekście wygody użytkownika w momencie gdy proces akwizycji danych niezbędnych do uwierzytelnienia zajmuje ok. 18 sekund.
- Język w jakim napisano rozprawę. Pewne fragmenty niniejszej rozprawy są napisane językiem dość nieformalnym z pewnymi usterkami językowymi:
 - „Mierzenie systemu” czy „algorytmy uczące” – prawdopodobnie lepiej byłoby napisać „mierzenie skuteczności systemu” oraz „algorytmy uczenia maszynowego”.
 - Również stwierdzenie, że system „samodzielnie radzi sobie” jest dość potoczne i nieprecyzyjne.
 - Powstały system „nie jest progowy” (str. 42) – zwrot ten jest również nieprecyzyjny. Ponadto, jakby się przyjrzeć dokładniej klasycznym metodom uczenia maszynowego (np. drzewo decyzyjne) to metody te w

trakcie uczenia ustalają jednak pewien próg decyzyjny na wybranym atrybucie.

- W niektórych rozdziałach również można wskazać pewne ogólnikowe zwroty nacechowane emocjonalnie (np. „działają całkiem dobrze” (str.95), „trudne do przewidzenia” (str.95), „są łatwe w szkoleniu” (str.95))
- Za pewne niedopatrzenie edytorskie można też uznać odsyłacz do nieistniejącego rozdziału 0 (str. 105)

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Pomimo przedstawionych powyżej uwag, rozprawa mgr inż. Pawła Łąki posiada wiele mocnych stron.

Przede wszystkim zawiera ona oryginalną autorską propozycję systemu uwierzytelniania użytkownika. Rozprawa dotyczy ważnego zagadnienia, jest aktualna i wnosi interesujący wkład do biometrii, systemów rozpoznawania i zagadnień związanych z uwierzytelnianiem wieloskładnikowym.

Pomimo wymienionych usterek praca jest ciekawie napisana, czyta się ją bardzo dobrze i przyjemnie. Niewątpliwie recenzowana praca dowodzi dużej wiedzy Autora dot. zagadnień uwierzytelniania wieloskładnikowego.

Warto także zauważyć, że Autor ma udokumentowany dorobek publikacyjny w zakresie rozprawy. Doktorant jest pierwszym autorem, więc jego wkład można uznać za znaczący.

Wniosek

Biorąc pod uwagę przedstawioną przez Doktoranta rozprawę stwierdzam, że spełnia **ona wymagania stawiane rozprawom doktorskim** przez obowiązującą Ustawę o stopniach i tytule naukowym, i wnioskuję o **dopuszczenie** jej do publicznej obrony.



Podpis

Lublin, 28.08.2021 r.

PW WEiTI Kancelaria
wpłynęło dnia 13.09.2021 r.
numer

Recenzja rozprawy doktorskiej

Tytuł: Wieloskładnikowe i transparentne uwierzytelnianie użytkownika z wykorzystaniem technik uczenia maszynowego

Autor: mgr inż. Paweł Łąka

- 1. Jaki zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?**

Rozprawa doktorska dotyczy utworzenie systemu wieloskładnikowego uwierzytelniania z wykorzystaniem technik uczenia maszynowego. Podjęty temat jest aktualny, ponieważ od wielu lat stale zwiększa się nasza aktywność w świecie cyfrowym, a systemy uwierzytelnienia są podstawowymi systemami gwarantującymi odpowiedni poziom kontroli dostępu. Szczególnie istotne dzisiaj jest utworzenie takiego systemu, który będzie spełniał najwyższe wymagania bezpieczeństwa i będzie jednocześnie wygodny dla użytkownika końcowego.

Autor postawił następującą tezę badawczą: „**Możliwe jest stworzenie kompleksowego i efektywnego systemu uwierzytelniającego, podejmującego decyzje przy użyciu algorytmów sztucznej inteligencji, wykorzystującego wiele niezależnych i transparentnych dla użytkownika końcowego metod opartych na tym, co dany użytkownik wie, posiada, jego cechach oraz ciągłym uwierzytelnianiu behawioralnym**”.

W celu weryfikacji postawionej tezy, Autor stworzył system, który przeprowadza wieloskładnikowe uwierzytelnienie oraz podejmuje decyzje o udzieleniu dostępu z wykorzystaniem metod uczenia maszynowego. W celu potwierdzenia postawionej tezy określono dwanaście głównych zadań badawczych.





UMCS

UNIwersYTET MARII CURIE-SKŁODOWSKIEJ W LUBLINIE
Wydział Matematyki, Fizyki i Informatyki

dr hab. Bogdan Księżopolski, prof. uczelni | Kierownik Katedry Cyberbezpieczeństwa

Lublin, 28.08.2021 r.

PW WEiTI Kancelaria
wpłynęło dnia **13.09.2021r.**
numer

Recenzja rozprawy doktorskiej

Tytuł: Wieloskładnikowe i transparentne uwierzytelnianie użytkownika z wykorzystaniem technik uczenia maszynowego

Autor: mgr inż. Paweł Łąka

- 1. Jaki zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?**

Rozprawa doktorska dotyczy utworzenie systemu wieloskładnikowego uwierzytelniania z wykorzystaniem technik uczenia maszynowego. Podjęty temat jest aktualny, ponieważ od wielu lat stale zwiększa się nasza aktywność w świecie cyfrowym, a systemy uwierzytelniania są podstawowymi systemami gwarantującymi odpowiedni poziom kontroli dostępu. Szczególnie istotne dzisiaj jest utworzenie takiego systemu, który będzie spełniał najwyższe wymagania bezpieczeństwa i będzie jednocześnie wygodny dla użytkownika końcowego.

Autor postawił następującą tezę badawczą: „**Możliwe jest stworzenie kompleksowego i efektywnego systemu uwierzytelniającego, podejmującego decyzje przy użyciu algorytmów sztucznej inteligencji, wykorzystującego wiele niezależnych i transparentnych dla użytkownika końcowego metod opartych na tym, co dany użytkownik wie, posiada, jego cechach oraz ciągłym uwierzytelnianiu behawioralnym**”.

W celu weryfikacji postawionej tezy, Autor stworzył system, który przeprowadza wieloskładnikowe uwierzytelnienie oraz podejmuje decyzje o udzieleniu dostępu z wykorzystaniem metod uczenia maszynowego. W celu potwierdzenia postawionej tezy określono dwanaście głównych zadań badawczych.



1. Przeanalizowano szczegółowo metody uwierzytelnienia oraz istniejące systemy uwierzytelniające.
2. Zaprojektowano oraz zaimplementowano nową metodę uwierzytelnienia opartą o analizę składu ciała człowieka.
3. Zaprojektowano scharakteryzowany system przy uwzględnieniu obecnych trendów rozwojowych związanych z uwierzytelnianiem i kontrolą dostępu.
4. Zaimplementowano system podzielony na serwisy związane z każdą z wykorzystanych metod.
5. Zaprojektowano, zaimplementowano i zbadano profile użytkowników końcowych.
6. Zaprojektowano i zaimplementowano system uwierzytelniający uwzględniając bezpieczeństwo systemu w zakresie integracji oraz przetwarzania danych.
7. Zaprojektowano i zbudowano rozwiązanie uwzględniając wygodę użytkownika końcowego.
8. Zaprojektowano i zrealizowano badania eksperymentalne zaimplementowanego systemu.
9. Zaprojektowano i wykonano eksperyment i próby złamania systemu uwierzytelniającego w celu sprawdzenia bezpieczeństwa rozwiązania.
10. Zaprojektowano i przeprowadzono badania związane z wyborem odpowiednich algorytmów uczenia maszynowego.
11. Zbadano poziom ochrony danych przez projektowany system.
12. Dokonano analizy porównawczej zaproponowanego systemu z dotychczas znanymi rozwiązaniami.

Postawiona teza została sformułowana poprawnie, a jej wykazanie implikowało konieczność rozwiązania sformułowanych zadań badawczych oraz implementacji stosowych rozwiązań o stopniu złożoności adekwatnym do oczekiwanego poziomu prac doktorskich.

2. **Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł (w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle) świadczącą o dostatecznej wiedzy autora? Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonujący?**





Wprowadzenie teoretyczne wraz z analizą literatury zostało przeprowadzone w rozdziale 2 oraz 3 rozprawy. W rozdziale 2 Autor wprowadził w tematykę procesów uwierzytelniania, stosowanych architektur IT oraz poziomów ochrony danych. W tej części zawarto również, krótką charakterystykę algorytmów uczenia maszynowego. Rozdział 3 zawiera przegląd literatury odnoszący się do poruszanej w rozprawie tematyki badawczej. Ważną częścią tego rozdziału jest porównanie podejść opisanych w literaturze oraz systemów komercyjnych z proponowanym rozwiązaniem.

Przedłożona rozprawa doktorska obejmuje 138 pozycji bibliograficznych, które reprezentują poruszaną tematykę. Szczególnie wartościowe jest przedstawienie zestawienia, które prezentuje zaproponowane przez Autora rozwiązania w porównaniu z innymi podejściami określonymi w literaturze (Tabela 3.1). Takie zestawienia w sposób jasny i przekonujący charakteryzują rozwiązania zaproponowane w rozprawie.

3. Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

W mojej ocenie postawiony w pracy problem utworzenia systemu wieloskładnikowego uwierzytelniania z wykorzystaniem technik uczenia maszynowego, został rozwiązany. Zaproponowane rozwiązanie polegało na przygotowaniu trzech głównych elementów: dwóch nowych metody uwierzytelnienia opartych na analizie składu ciała człowieka oraz czasie pomiędzy wykonywanymi etapami uwierzytelnienia, utworzenie architektury systemu wraz z przygotowaniem jego prototypu oraz systemu podejmowania decyzji opartego o metody sztucznej inteligencji.

W ramach rozprawy Autor zaproponował dwie nowe metody uwierzytelnienia, pierwsza wykorzystując masę oraz analizę składu ciała oraz druga, czas pomiędzy użyciem poszczególnych metod w uwierzytelnieniu wieloskładnikowym. Metoda dotycząca analizy masy ciała została opisana przez Autora w uznanym czasopiśmie *Annals of Telecommunications*, w wydawnictwie Springer. Metoda została przeanalizowana na podstawie dobrze znanych kryteriów. Udowodniono, że nowa metoda spełnia wszystkie kryteria równie skutecznie, jak inne metody biometryczne. Tymi kryteriami były: uniwersalność, odrębność między użytkownikami, niezmiennosc cech w czasie, możliwość mierzenia, wydajność, akceptowalność w codziennym życiu oraz możliwość oszukania. Analiza składu ciała okazuje się być obiecującą metodą biometryczną, która spełnia wszelkie



wymogi stawiane taki metodom. Wyniki FAR (ang. False Acceptance Rate) i FRR (ang. False Reject Rate) są bardzo dobre, przyjmują wartości: $FRR = 0,00\%$ i $FAR = 2,65\%$.

Druga zaproponowana metoda uwierzytelnienia opiera się na analizie behawioralnej, która bazuje na analizie trwania całego procesu uwierzytelniającego z podziałem na poszczególne metody. Zakłada ona, że każdy użytkownik będzie inaczej przechodził przez cały proces uwierzytelnienia i w innym czasie potwierdzi swoją tożsamość w poszczególnych metodach. Metoda polega na stałej analizie czasu trwania procesów uwierzytelniania. Metoda ta jest metodą uwierzytelnienia ciągłego bez konieczności wymuszenia dodatkowych czynności użytkownika, takich jak użycie klawiatury lub myszy. Wyniki FAR oraz FRR dla tej metody zostały przedstawione na Rysunku 7.14. Wskaźnik FRR pozostaje stale na niskim poziomie, niestety współczynnik FAR spada liniowo do wartości 0.99. Uzyskanie takiego wyniku dla współczynnika FAR oznacza, że metoda nie może zostać użyta jako samodzielna metoda uwierzytelniania. Taki właśnie wniosek z przeprowadzonych badań przedstawił Autor w rozprawie i zasugerował zebrania większego wolumenu danych, ponieważ właśnie mały wolumen danych mógł mieć wpływ na uzyskane wyniki. Moim zdaniem metody uwierzytelnienia ciągłego oraz behawioralne spełniają bardzo ważną potrzebę użytkownika, czyli wygodę tego procesu, dlatego uważam, że są one przyszłością dla zastosowań komercyjnych. Zastosowanie takiej metody, pomimo braku optymalnych wyników, uważam za bardzo ciekawe, a wnioski przedstawione przez Autora rozprawy trafne naukowo.

Zaproponowana architektura bazuje na dobrze znanym i aktualnym podejściu, która zakłada użycie dwóch komponentów:

- IdP (ang. Identity Provider) - system uwierzytelniający, odpowiedzialny za proces potwierdzania tożsamości użytkownika końcowego;
- RP (ang. Relying Party) – strona pośrednicząca w dostępie do chronionej części systemu, do której dostęp jest przyznawany po poprawnej weryfikacji tożsamości.

Autor rozprawy utworzył protokół uwierzytelniający dla swojego rozwiązania w oparciu o znany standard OpenID Connect. W uproszczeniu, zaproponowany protokół działa w taki sposób, że strona pośrednicząca (RP) wysyła prośbę o uwierzytelnienie do strony weryfikującej tożsamość (IdP). IdP uwierzytelnia użytkownika końcowego i uzyskuje zezwolenie na dostęp. Następnie IdP odpowiada RP za pomocą tokena identyfikującego oraz tokena dostępu. RP może poprosić o dodatkowe informacje o użytkowniku końcowym IdP, które w takim przypadku przesyła IdP do RP. Komunikacja między stronami protokołu jest szyfrowana. Zaproponowany system został zaprojektowany oraz zaimplementowany w oparciu o architekturę zorientowaną na usługi (ang.

SOA). W tej architekturze, każda metoda uwierzytelnienia traktowana jest jako oddzielny komponent, dzięki czemu system może być dowolnie skalowany i konfigurowany. Takie podejście jest zgodne z najlepszymi praktykami obecnie przyjętymi w dziedzinie inżynierii oprogramowania.

Zaproponowany system wykorzystuje kombinację zastosowanych metod, które wykorzystują dane zebrane z poszczególnych etapów uwierzytelnienia i ostatecznie system decyzyjny, wykorzystujący algorytmy sztucznej inteligencji, podejmuje decyzję o uwierzytelnieniu użytkownika. System został zbudowany w taki sposób, aby możliwe do zastosowania metody były niezależne oraz żeby żadna z metod nie była bardziej znacząca od innych metod. Dzięki takiemu założeniu, jeżeli jakaś z metod uwierzytelniania zawiedzie, system może użyć innej, która pozwala na tym samym poziomie bezpieczeństwa potwierdzić tożsamość. Autor, w ramach zaproponowanego systemu wieloskładnikowego uwierzytelnienia, wybrał 6 metod (Tab. 5.2):

1. RFID bluetooth – coś co użytkownik ma;
2. rozpoznawanie twarzy – coś, czym użytkownik jest;
3. rozpoznawanie treści komunikatu – coś co użytkownik wie;
4. rozpoznawanie głosu - coś, czym użytkownik jest;
5. rozpoznawanie analizy składu ciała - coś, czym użytkownik jest;
6. czas między realizacją wyżej wymienionych metod uwierzytelniania – uwierzytelnienie behawioralne.

Zaproponowane rozwiązanie działa w taki sposób, że system ocenia uzyskane poświadczenia z sześciu zastosowanych metody i w wyniku czego zwraca wartość „SUKCES” lub „NIEPOWODZENIE”. Poprawne uwierzytelnienie (wynik „SUKCES”) zostaje uzyskany, gdy użytkownik przekroczy założony poziom ochrony określony przez administratora systemu.

Zaprojektowany przez Autora moduł podejmowania decyzji jest częścią systemu IdP i właśnie ten moduł podejmuje decyzję dotyczącą poprawności uwierzytelnienia. W ramach przeprowadzanych badań, Autor wybrał 10 algorytmów uczenia maszynowego zgodnie z zaproponowaną metodyką opracowaną przez Scikit-learn oraz analizą najlepszych praktyk w tej dziedzinie opisanych w literaturze. Autor wybrał następujące algorytmy:

- Najbliższego sąsiada (ang. Nearest Neighbors);
- Liniowy SVM (ang. Support Vector Machines Linear);
- RBF SVM (ang. Radial Basis Function SVM);
- Proces gaussowski (ang. Gaussian Process);
- Drzewo decyzyjne (ang. Decision Tree);
- Las losowy (ang. Random Forest);



- Sieci neuronowe (ang. Neural Networks);
- AdaBoost;
- Naiwny klasyfikator Bayesa (ang. Naive Bayes);
- Kwadratowa analiza dyskryminacyjna QDA (ang. Quadratic Discriminant Analysis).

W celu weryfikacji stworzonego systemu, a w szczególności algorytmów decyzyjnych, zostało opracowane środowisko testowe, przy pomocy którego wykonano badania eksperymentalne. Warto zaznaczyć, że środowisko eksperymentalne było bardzo zbliżone do realnego środowiska, w którym zaproponowane wieloskładnikowe uwierzytelnienie może być zastosowane. Narzędzia badawcze, jak i metodologii badań zostały dobrane prawidłowo i są zgodne z najlepszymi praktykami badawczymi. W pracy Autor wykonał porównanie wyżej wspomnianych algorytmów, wyliczając dla poszczególnych algorytmów współczynniki FAR oraz FRR. Wyniki zostały przedstawione w tabeli 7.3, które wskazują na bardzo dobre wyniki zaproponowanego rozwiązania. Przedstawione rezultaty potwierdzają postawioną tezę rozprawy.

4. Na czym polega problem oryginalności rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?

Moim zdaniem, najważniejszym oryginalnym osiągnięciem Autora jest zrealizowanie systemu wieloskładnikowego uwierzytelnienia, który swoją decyzję nie opiera na wartościach progowych poszczególnych czynników, tylko analizując dane z różnych stosowanych metod uwierzytelnienia i podejmuje decyzję na podstawie utworzonych algorytmów uczenia maszynowego. Zaprojektowany system uwzględnia jednocześnie użycie wielu metod z grupy wiedza, posiadanie, cechy oraz zachowanie. Ważnym elementem tutaj jest zachowanie przezroczystości procesu dla użytkownika, nie zmniejszając jednocześnie poziomu bezpieczeństwa. Wartym podkreślenia jest również fakt, że Autor zaprojektował oraz zaimplementował prototyp całego systemu, dzięki czemu mógł przeprowadzić weryfikację eksperymentalną zaproponowanego rozwiązania. Wykonanie prototypu oraz przeprowadzenie badań eksperymentalnych w takim środowisku zwiększa poziom gotowości technologicznej (TRL) rozwiązania. Moim zdaniem wykonane badania spełniają wysoki poziom 5, czyli komponenty zostały zweryfikowane w środowisku zbliżonym do rzeczywistego. W takim przypadku została utworzona technologia, która może w kolejnym kroku zostać zweryfikowana w warunkach operacyjnych.

Kolejnym wartym zaznaczenia osiągnięciem Autora jest utworzenie systemu wnioskowania oraz podejmowania decyzji, który pozwala podjąć decyzję w sytuacji, braku odpowiedzi z jakiegos źródła danych uwierzytelniających. W systemie nie została określona konkretna ścieżka decyzyjna dotycząca postępowania w sytuacjach nieprzewidzianych, tylko właśnie zaprojektowane algorytmy uczenia maszynowego podejmują decyzję na podstawie wcześniej zebranych danych. Uzyskane wyniki zostały porównane z innymi metodami i wskazują na dobre wyniki proponowanego rozwiązania.

Trzecim osiągnięciem Autora, które warto podkreślić jest zaprojektowanie oraz zaimplementowanie nowej metody potwierdzania tożsamości użytkownika wykorzystującej mechanizm rozpoznawania masy oraz składu ciała. Uzyskane wyniki są bardzo obiecujące, ponieważ FAR (ang. False Acceptance Rate) i FRR (ang. False Reject Rate) są równe: $FRR = 0,00\%$ i $FAR = 2,65\%$. Dodatkowo, Autor zaproponował metodę uwierzytelnienia ciągłego, opartą na czynniku behawioralnym użytkownika. Metoda ta polega na analizie trwania całego procesu uwierzytelniającego z podziałem na poszczególne metody. Pomimo uzyskania wysokiego wskaźnika FAR dla tej metody, uważam, że metody oparte o analizę ciągłą i behawioralna są przyszłością rozwiązań w tej dziedzinie.

5. Czy autor wykazał umiejętność poprawnego i przekonującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?

Praca została napisana w języku polskim. Język jest na bardzo dobrym poziomie, nie zauważyłem większych problemów językowych. Praca została zredagowana w sposób bardzo dobry. Autor wykazał się umiejętnością poprawnego i przekonującego przedstawienia uzyskanych przez siebie wyników. Zaproponowana architektura oraz moduły zostały doskonale oraz licznie zilustrowane odpowiednimi grafikami, schematami, tabelami oraz przykładami. Moim zdaniem poziom redakcyjny rozprawy doktorskiej jest na bardzo dobrym poziomie.

6. Jakie są słabe strony rozprawy i jej główne wady?

Moim zdaniem, zaprezentowane badania mają kilka słabości. Pierwsza z nich dotyczy faktu, że algorytmy decyzyjne zwracające wartość „SUKCES” w przypadku, gdy dowolne dwie metody uwierzytelniania, z sześciu użytych, zakończą się powodzeniem (LoA 3). Z punktu widzenia wygody użytkownika jest to dobre rozwiązanie, ale wydaje się, że zmniejsza to poziom



bezpieczeństwa. Dzięki możliwości wyboru dwóch metod z sześciu możliwych, atakujący może wybrać takie dwie, które w danym momencie może zastosować.

Innym minusem pracy jest fakt, że zaproponowany system wykorzystuje serwisy zewnętrzne do rozpoznawanie twarzy, rozpoznawanie treści komunikatu oraz rozpoznawanie głosu. Zastosowanie takiego rozwiązania wiąże się z koniecznością połączenia z siecią Internet. Taki wymóg może być problemem w przypadku, gdy będziemy chcieli uwierzytelnić osobę właśnie w samochodzie, który stoi na parkingu podziemnym, gdzie nie ma dostępu do Internetu. W takim przypadku, automatycznie trzy metody zakończą się niepowodzeniem. Dodatkowo, zastosowanie własnej implementacji dla tych trzech metod, pozwoliłoby uzyskać dodatkowe wartości do analizy behawioralnej bazującej na czasie wykonywania poszczególnych operacji uwierzytelniania. Wykorzystanie trzech dodatkowych interwałów czasowych wpłynęłoby na precyzję wspomnianej metody.

Inną słabością pracy jest brak bardziej szczegółowej analizy algorytmów decyzyjnych opartych na metodach sztucznej inteligencji. Brakuje mi analizy zachowania algorytmów uczenia maszynowego w przypadku, gdy dwie lub więcej metod uwierzytelnienia nie będzie użytych lub uzyskają niepoprawne wyniki. Pytanie, jak zachowują się algorytmy decyzyjne w zależności od liczby poprawnie zweryfikowanych metod oraz czy same metody wpływają na decyzję algorytmów?

Ostatnim elementem, który jest pewną słabością pracy, jest nie w pełni miarodajne porównanie uzyskanej dokładności proponowanego rozwiązania z tymi, które są znane z literatury. Zestawienie to zostało zaprezentowane w tabeli 7.4 i przedstawia skuteczność rozwiązania (IdP) wyłącznie z metodami biometrycznymi. Wskazano, że przedstawione rozwiązanie ma 100% skuteczność, ale w przypadku zaproponowanego rozwiązania IdP zastosowano wieloskładnikowe uwierzytelnienie. Warto byłoby wykonać porównanie z innymi rozwiązaniami, które również wykorzystują wieloskładnikowe uwierzytelnienie.

Jednocześnie, chciałbym dodać, że wskazane uwagi nie wpływają w istotny sposób na moją merytoryczną pozytywną ocenę pracy jako całości. Ich uwzględnienie może okazać się przydatne w dalszej działalności naukowej doktoranta.

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Przydatność uzyskanych wyników w naukach technicznych oceniam wysoko. Zaproponowany system wieloskładnikowego uwierzytelnienia dotyczy aktualnego problemu w dziedzinie



bezpieczeństwa IT. Warte podkreślenia jest, że Autor w ramach rozprawy doktorskiej przedstawił rozwiązanie wraz z jej realizacją praktyczną, której gotowość technologiczną rozwiązania oceniam na poziom - TRL 5 (Test w środowisku symulującym rzeczywiste warunki). Myślę, że komercjalizacją zaproponowanego rozwiązania mogą być zainteresowani inwestorzy z sektora bezpieczeństwa IT.

8. Do której z następujących kategorii Recenzent zalicza rozprawę:

- a) nie spełniająca wymagań stawianych rozprawom doktorskim przez obowiązujące przepisy,
- b) wymagająca wprowadzenia poprawek i ponownego recenzowania,
- c) spełniająca wymagania,
- d) spełniająca wymagania z wyraźnym nadmiarem,
- e) wybitnie dobra, zasługująca na wyróżnienie.

Uważam, że rozprawa doktorska magistra inżyniera Pawła Łąki spełnia wymogi stawiane rozprawom doktorskim przez obowiązujące przepisy. Należy podkreślić, że część wyników rozprawy została już opublikowana w literaturze międzynarodowej, a w szczególności w czasopiśmie Annals of Telecommunications indeksowanym w JCR.

Bogdan Księżopolski
Kierownik Katedry
dr hab. Bogdan Księżopolski
prof. UMCS