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.

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 wymogi 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 przekonywujący?**

Wprowadzenie teoretyczne wraz z analizą literatury zostało przeprowadzona 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 przekonywujący 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 wykorzystuję 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, niezmienność cech w czasie, możliwość mierzenia, wydajność, akceptowalność w codziennym życiu oraz możliwość oszukania. Analiza skład 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 niskimi 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 systemy, 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 zgodnie 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 wieloskładniowego uwierzytelnienia, który swoją decyzję nie opiera na wartościach progowych poszczególnych czynników, tylko analizuję 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 weryfikacje 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 systemy wnioskowania oraz podejmowania decyzji, który pozwala podjąć decyzję w sytuacji, braku odpowiedzi z jakiegoś 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 zaproponowanego 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 mety oparte o analizę ciągłą i behawioralna są przyszłością rozwiązań w tej dziedzinie.

5. Czy autor wykazał umiejętność poprawnego i przekonywującego 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 przekonywującego 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 rozwiązanie 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 zachowają 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.

Kierownik Katedry
dr hab. Bogdan Księżopolski
prof. UMCS