Bydgoszcz, 08.03.2024

Prof. dr hab. inż. Michał Choraś
Wydział Telekomunikacji, Informatyki i Elektrotechniki
Politechnika Bydgoska im. J.J. Śniadeckich, Bydgoszcz

Recenzja rozprawy doktorskiej

Biometryczna weryfikacja użytkownika systemu komputerowego z automatyczną aktualizacją profilu aktywności,

której Autorem jest Pan

mgr inż. Tomasz Wesołowski

realizowanej na Uniwersytecie Śląskim

1. Wprowadzenie.

Niniejsza recenzja rozprawy doktorskiej, której Autorem jest Pan mgr inż. Tomasz Wesołowski, została wykonana na podstawie umowy WU.W400.00026.24 z dnia 18.01.2024 pomiędzy mną a Uniwersytetem Śląskim w Katowicach reprezentowanym przez Dziekana Wydziału Nauk Ścisłych i Technicznych prof. dr. hab. Danutę Stróż. Recenzję wysłałem w wyznaczonym umową terminie przed 18.03.2024.

Promotorem niniejszej rozprawy jest Pan prof. dr hab. inż. Piotr Porwik. Promotorem pomocniczym jest Pan dr hab. inż. Rafał Doroz, prof. UŚ.

Praca doktorska składa się ze streszczenia, spisów, sześciu rozdziałów, czterech dodatków oraz bibliografii.

Niniejsza praca została częściowo wsparta przez Narodowe Centrum Nauki w ramach grantu nr DEC-2013/09/B/ST6/02264. Dodatkowo, Autor rozprawy był stypendystą projektu „DoktoRIS – Program stypendialny na rzecz innowacyjnego Śląska" współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.

Niniejsza recenzja (poza wprowadzeniem i wnioskiem) zawiera odpowiedzi na siedem pytań dotyczących rozprawy doktorskiej.

2. Jaki jest problem naukowy (teza) rozprawy? Czy został on trafnie i jasno sformułowany? Jaki charakter ma rozprawa?

Rozprawa, której Autorem jest Pan mgr inż. Tomasz Wesołowski, dotyczy biometrycznych metod rozpoznawania osób. W szczególności, Autor zajął się

zagadnieniem weryfikacji tożsamości na podstawie cech biometrycznych zawartych w pozyskanych wzorcach dynamiki użytkowania klawiatury. Tym samym, Autor zajął się behawioralnym typem biometrycznej weryfikacji użytkowników.

Głównym efektem i rezultatem prac Autora jest opracowanie własnych metod weryfikacji tożsamości osób w oparciu o cechy dynamiki użytkowania klawiatury, w szczególności w scenariuszu weryfikacji ciągłej (*Continuous Authentication/Continuous Verification (CA/CV)*).

Niniejsza praca naukowa ma charakter teoretyczny oraz koncepcyjno-eksperymentalny.

Problemy naukowe rozprawy zostały dość jasno i trafnie sformułowane, a także rozwiązane przez Autora. Teza rozprawy znajduje się w rozdziale 1.2 na stronie 6. Autor zdecydował się postawić tezę, iż możliwa jest poprawa skuteczności weryfikacji użytkowników systemu komputerowego poprzez wprowadzenie ciągłej weryfikacji wykorzystującej biometryczny profil aktywności bazujący na obserwowanej dynamice użytkowania klawiatury.

Niniejsza teza została potwierdzona w dalszej części rozprawy.

Autor postawił sobie także 5 celów pracy (przedstawionych i omówionych w Rozdziale 1.3), z których większość zrealizował w całości lub częściowo.

3. **Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł, w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle? Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?**

W niniejszej rozprawie niestety brakuje wydzielonego rozdziału poświęconego analizie literatury przedmiotu pracy, czyli w szczególności prac poświęconych behawioralnej biometrii oraz cech i systemom biometrii bazującej na analizie uderzeń w klawisze klawiatury. Co najważniejsze, brakuje krytycznego przeglądu literatury oraz analizy aktualnych trendów w biometrycznym rozpoznawaniu osób bazującym na cechach uderzeń w klawisze.

Rozdział 2 jest ogólnym wprowadzeniem do systemów biometrycznych i prezentuje bardzo podstawowe informacje. Nie jestem przekonany, że ten Rozdział jest konieczny i że musiał być wydzieloną częścią pracy (np. miary można było przedstawić w rozdziale z eksperymentami i wynikami).

Sama bibliografia zawiera odpowiednią liczbę źródeł (197), ale w pracy zabrakło szerszej analizy trendów oraz krytycznej oceny stanu wiedzy przedstawionego w wykorzystanych pracach.

4. **Czy autor rozwiązał postawione zagadnienia? Czy użył do tego właściwych metod dowodząc, że posiadł umiejętności związane z metodyką i metodologią prowadzenia badań naukowych? Czy przyjęte założenia są uzasadnione?**

Generalnie, Autor w sposób odpowiedni rozwiązał problemy, których dotyczy rozprawa. Autor posiada wiedzę dot. zagadnień związanych z systemami biometrycznymi. Autor posiada bogatą wiedzę dotyczącą ewaluacji (w tym systemów biometrycznych) oraz analizy dynamiki i profili uderzeń w klawisze i użytkowania klawiatury.

Przyjęte założenia są uzasadnione i merytorycznie poprawne, pomimo iż Autor nie zaproponował zbyt wielu własnych rozwiązań oraz cech/metod.

Autor posiada duże umiejętności oraz wiedzę teoretyczną w konstruowaniu, analizie oraz wykorzystywaniu metod ewaluacji systemów biometrycznych.

Natomiast jestem krytycznie nastawiony do elementów pracy, które odnoszą się do cyberbezpieczeństwa i systemów IDS (*Intrusion Detection Systems*). Uważam, iż Doktorant mógł poświęcić pracę aspektom biometrycznym, bez próby odniesienia ich do systemów wykrywania ataków sieciowych (więcej uwag w części 7 niniejszej recenzji).

5. **Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu nauki reprezentowanych przez literaturę światową?**

Głównymi osiągnięciami rozprawy oraz propozycjami Autora są:

- Opracowanie metody profilowania i weryfikacji użytkowników systemów komputerowych polegającej na analizie poleceń systemowych wpisywanych z klawiatury oraz weryfikacja użytkowników wykorzystująca profile i wnioskowanie rozmyte (ta część pracy została przedstawiona w Rozdziale 3).
- Opracowane własnej metody weryfikacji tożsamości osób w oparciu o analizę dynamiki pisania na klawiaturze (ta część pracy została przedstawiona w Rozdziale 3).
- Wykorzystanie szeregu metod klasyfikacji (m.in. komitety klasyfikatorów) do weryfikacji użytkowników.

Ponadto, Autor wykonał szereg testów i prac eksperymentalnych w celu zbadania i porównania zaproponowanych metod, wkładając bardzo dużo pracy w tę część rozprawy oraz prezentując bogaty zestaw wyników i porównań (w szczególności w Rozdziale 5 niniejszej rozprawy).

Realizując cele pracy, Autor zebrał szereg danych do analizy, ale niestety nie znalazłem informacji o publicznym udostepnieniu bazy *realKDD* (zwiększyłoby to znacznie wpływ pracy).

6. **Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników? Jaka jest poprawność redakcyjna rozprawy?**

Niniejsza rozprawa stanowi przykład profesjonalnie przygotowanej pracy doktorskiej. Praca napisana jest na wysokim poziomie edycyjnym oraz graficznym.

W pracy występują oczywiście drobne usterki, literówki i błędy językowe, ale jest ich niewiele i nie są znaczące.

Praca jest przemyślana i ma dobrą strukturę oraz czytelny układ. Brakuje jedynie wydzielonego rozdziału z analizą literatury przedmiotu.

Drobne usterki nie zmieniają ogólnej opinii o bardzo dobrym i profesjonalnym poziomie językowym i edycyjnym rozprawy.

7. **Jakie są słabe strony rozprawy i jej główne wady?**

Rolą recenzenta jest zauważenie ewentualnych niedociągnięć i mankamentów przedstawianej pracy, oraz zgłoszenie uwag, które mogą być pomocne i przydatne w dalszych pracach.

Uwagi krytyczne to między innymi:

- Praca rozpoczyna się niefortunnie. Na str. 1 umieszczono Rysunek 1.1, który podaje informacje z lat 2009-2014/2015. To już 10 lat temu! Nawet jeśli doktorant rozpoczął pracę tak dawno, mógł zaktualizować dane przed oddaniem ostatecznej wersji pracy.
- Na str. 1 jest także zdanie „Z najnowszych raportów wynika [...]". Wiem, że czas doktorantom płynie inaczej, ale Autor nie przytacza najnowszych raportów. Nie wiadomo także dlaczego akurat takie raporty zostały wybrane, a nie np. dane pochodzące z OWASP lub ENISA lub NASK/CERT. Kryteria doboru raportów i danych nie są jasno sprecyzowane.
- Na stronie 2 umieszczono rysunek „Różne poziomy bezpieczeństwa systemu komputerowego". Zabrakło jednak odwołania lub referencji popierającej treść rysunku. Nie wiem na jakiej podstawie Autor rozprawy zdecydował co jest najwyższym poziomem bezpieczeństwa i dlaczego?
- Z rozprawy (nie tylko z Rys 1.2) wynika, iż Autor nie jest świadomy wad i niebezpieczeństw dot. biometrycznych cech i metod rozpoznawania osób.
- Rozdział 2.3 „Miary biometryczne" nie zawiera wszystkich stosowanych w literaturze miar, a Autor nie podaje jasnych kryteriów wyboru opisanych miar. Tematyka miar biometrycznych jest dużo bardziej złożona i rozbudowana.
- Podobnie z rozdziale 2.4 wymienione są tylko dwie metryki - skuteczność ACC i Precyzja. Autor pominął m.in. metryki *Recall*/czułość, a *g-measure* i *f-measure* są

zaledwie wspomniane, ale bez definicji i omówienia. Nie wspomniano także np. o *balanced accuracy*.

- Autor często nie powołuje się na żadne wiarygodne informacje prezentując opinie lub dane (np. Rys. 2.1). Dla przykładu na stronie 18 znajduje się zdanie „W literaturze bardzo często spotyka się opisy eksperymentów, w których jedynym podanym wynikiem klasyfikacji jest jej skuteczność ACC", ale nie ma przy nim żadnego cytowania ani odniesienia do źródeł.
- Jak wspomniałem w części 3 niniejszej recenzji, w pracy nie ma oddzielnego rozdziału z analizą literatury. Opis literatury jest jedynie wpleciony w rozdziale 3 (w pierwszych trzech paragrafach) i później fragmentarycznie rozrzucony po pracy. Zabrakło głębszej analizy prac, trendów, kierunków rozwoju itp.
- W pracy zabrakło szerszej dyskusji na temat ograniczeń proponowanej modalności biometrycznej i wykorzystania analizy dynamiki uderzeń w klawisze w praktyce. Natomiast bardzo podoba mi się krytyczne podejście do własnych wyników dot. analizy wpisywania komend przedstawione w Rozdziale 3. Ta uczciwa analiza krytyczna własnych prac świadczy pozytywnie o dojrzałości Doktoranta i nie jest często spotykana w rozprawach doktorskich.
- Nie umieszczono informacji czy pozyskany zbiór danych biometrycznych *realKDD* został opublikowany, czy jest otwarty, ani informacji na temat sposobu udostepnienia tego zbioru dla innych badaczy.
- W pracy nie zawarto dyskusji na temat ewentualnych problemów związanych z etyką wykorzystania opisywanej technologii, ani elementów dot. ochrony danych osobowych.
- W pracy często brakuje informacji na temat istotności statystycznej różnic między uzyskanymi wynikami, parametrami itp.
- Niniejsza rozprawa moim zdaniem powinna pozostać w temacie biometrii. Autor niepotrzebnie próbował nawiązać do zastosowań w cyberbezpieczeństwie. Niestety z pracy nie wynika, iż Autor rozumie metody, problemy i zastosowania metod ochrony systemów i sieci komputerowych przed atakami sieciowymi.
- Autor wspomina zastosowanie swoich metod w systemie IDS (*Intrusion Detection System*). Niestety w pracy nie pojawia się nazwa/y systemów IDS, sposób ich użycia, informacja na temat topologii sieci/chronionego systemu, rysunek architektury, itp.
- Tym samym nie jest dla mnie do końca jasne w jakim stopniu został zrealizowany cel 5 niniejszej rozprawy, dotyczący testowania metod na danych/systemach rzeczywistych. Autor nie odniósł się do rzeczywistych systemów, które mogą być chronione proponowanymi metodami ani nie wspomniał o zaawansowaniu technologii , w tym na jakim jest aktualnie poziomie TRL.

Pomimo wymienionych uwag krytycznych, często natury dyskursywnej, niniejszą pracę oceniam wysoko.

Warto zauważyć, że Doktorant ma bogaty dorobek publikacyjny, w tym prace w prestiżowych czasopismach, m.in.:

- Porwik P., Doroz R., Wesołowski T.E., Dynamic keystroke pattern analysis and classifiers with competence for user recognition, *Applied Soft Computing* (ISSN 1568-4946), Vol. 99, art. No 106902, 2021, DOI 10.1016/j.asoc.2020.106902 (IF 8,7, punktacja MEiN: 200)
- Wesołowski T.E., Porwik P., Doroz R., Electronic Health Record Security Based on Ensemble Classification of Keystroke Dynamics, *Applied Artificial Intelligence*, Vol. 30, Issue 6, pp. 521-540, Taylor & Francis 2016, DOI 10.1080/08839514.2016.1193715 (IF 0,527)11:9213952246
- Kudłacik P., Porwik P., Wesołowski T., Fuzzy Approach for Intrusion Detection Based on User's Commands, *Soft Computing*, Vol. 20 Issue 7, pp. 2705-2719, Springer-Verlag Berlin Heidelberg 2016, DOI 10.1007/s00500-015-1669-6 (IF 1,271).

8. Jaka jest przydatność rozprawy dla nauk technicznych?

Praca dotyczy bardzo aktualnych i potrzebnych zagadnień nowoczesnej informatyki technicznej i telekomunikacji, a w szczególności metod biometrycznej identyfikacji osób, w tym z wykorzystaniem mniej popularnych modalności oraz metod tzw. biometrii behawioralnej.

Niniejsza rozprawa i przedstawione metody mogą być szczególnie interesujące i przydatne dla komercyjnych i publicznych podmiotów wykorzystujących systemy rozpoznawania osób oraz systemy zabezpieczania systemów komputerowych.

Ponadto, być może, zaprezentowane w pracy metody mogą znaleźć zastosowanie w cyberbezpieczeństwie oraz być może w naukach społecznych (badanie stresu, psychologia), itp.

9. Wniosek.

Biorąc pod uwagę przedstawioną przez Doktoranta rozprawę stwierdzam, że recenzowana praca **spełnia wymagania stawiane rozprawom doktorskim** przez obowiązujące przepisy.

Dlatego wnoszę o przyjęcie niniejszej rozprawy i **dopuszczenie** Pana mgr inż. Tomasza Wesołowskiego do publicznej obrony.

Prof. dr hab. inż. Michał Choraś