

dr hab. Andrzej Kobyliński, prof. SGH
Instytut Informatyki i Gospodarki Cyfrowej
Kolegium Analiz Ekonomicznych
Szkola Główna Handlowa w Warszawie
Al. Niepodległości 162
02-554 Warszawa

Warszawa, 2021-08-28

**Recenzja rozprawy doktorskiej
dla Rady Awansów Naukowych
Uniwersytetu Ekonomicznego w Poznaniu**

Tytuł rozprawy: **Behaviour-based user authentication for financial services
(Behawioralne uwierzytelnianie użytkowników usług sektora
finansowego)**

Autor rozprawy: **mgr Piotr Kałużny**

Promotor: **prof. dr hab. Witold Abramowicz**

Promotor pomocniczy: **dr hab. Agata Filipowska**

Przedstawiona mi do oceny rozprawa doktorska mgr. Piotra Kałużnego p.t. „Behaviour-based user authentication for financial services (Behawioralne uwierzytelnianie użytkowników usług sektora finansowego)” jest obszerną pracą dotyczącą problematyki skutecznego uwierzytelniania użytkowników, którzy próbują uzyskać dostęp do aplikacji finansowych z wykorzystaniem aplikacji mobilnych. Ten obszar badawczy wpisuje się w tematykę będącą w kręgu badań naukowych prowadzonych w zakresie dyscypliny ekonomii i finansów, w dziedzinie nauk społecznych.

1. Podstawa opracowania recenzji

Podstawą formalną opracowania recenzji jest pismo Przewodniczącej Rady Awansów Naukowych Uniwersytetu Ekonomicznego we Poznaniu prof. dr hab. Barbary Jankowskiej z



dnia 21 czerwca 2021 r. w sprawie powierzenia mi obowiązków recenzenta rozprawy doktorskiej mgr Piotra Kałużnego.

2. Omówienie układu pracy

Praca, o całkowitej objętości 243 stron, składa się z trzech części merytorycznych (podzielonych na 4 rozdziały merytoryczne), poprzedzonych wstępem, uzupełnionych o zakończenie, 9 załączników i bibliografię.

We obszernym wstępie, liczącym aż 30 stron (nazwanym: rozdział 1), Autor scharakteryzował problem badawczy, wyjaśniając motywację, jaka skłoniła go do zajęcia się tą tematyką, jak również sformułował główną tezę pracy, pytania i odpowiadające im cele badawcze. Następnie opisał wykorzystane przez siebie metody badawcze i źródła wykorzystywanych informacji. W dalszej części Autor omówił strukturę rozprawy.

Pierwsza część pracy, na którą składają się dwa rozdziały, ma charakter szczegółowego wprowadzenia do zagadnień poruszanych w dalszej części pracy i stanowi bogaty przegląd literatury z zakresu omawianych zagadnień. Rozdział 2 (liczący 31 stron) stanowi przegląd piśmiennictwa z zakresu mobilnych aplikacji finansowych, a zwłaszcza wykorzystywanych metod uwierzytelniania użytkownika; w zakończeniu rozdziału przedstawiono też model wymagań dla metod uwierzytelniania w finansowych aplikacjach mobilnych. Rozdział 3 (54 stron) przedstawia stan wiedzy i praktyki w odniesieniu do metod biometrycznych i procesów uwierzytelniania użytkowników za pomocą tego rodzaju metod; rozdział kończy analiza porównawcza zaprezentowanych metod.

Druga część pracy stanowi liczący 25 stron rozdział 4. Został on poświęcony zaprojektowaniu własnej, autorskiej metody uwierzytelniania opartej na interakcji użytkownika z systemem przy pomocy ekranu dotykowego smartfona. Przedstawiono w nim założenia i ograniczenia zaprojektowanej metody.

Na trzecią część pracy składa się bardzo obszerny rozdział 5 (49 stron). Znalazł w nim miejsce opis 5 eksperymentów przeprowadzonych przez Autora, mających na celu zweryfikowanie zaprojektowanej metody na licznych zbiorach danych oraz uwiarygodnienie jej w scenariuszach użycia mobilnych aplikacji finansowych.

Podsumowanie pracy stanowi rozdział 6 (7 stron). Doktorant przedyskutował tam osiągnięcia swojej pracy, omówił osiągnięte wyniki badawcze oraz przedstawił kierunki i perspektywy dalszych badań.



Pracę kończy 9 załączników i zawierająca około 200 pozycji bibliografia oraz spis rysunków i listingów.

Reasumując: omawiana rozprawa doktorska ma układ typowy dla tego rodzaju prac – przegląd literatury, zaproponowanie własnego modelu i jego weryfikacja. Nie da się nic temu układowi zarzucić, bowiem jest czytelny i klarowny, a sam wywód został przeprowadzony logicznie.

3. Waga podjętej problematyki

Wartość rynków finansowych jest ogromna, aktywa globalne szacowane są na ponad 100 bilionów dolarów. I wzrost tych rynków jest ciągły, z niewielkimi zakłóceniami obserwowanymi podczas kryzysów. Usługi finansowe świadczone na tych rynkach również charakteryzują się dużym wolumenem (powyżej 20 bilionów rocznie) i bezustannym wzrostem. Świadczenie usług finansowych napotyka przy tym na oczywiste wyzwania organizacyjne i technologiczne, przy czym dotyczą one nie tylko podmioty bezpośrednio w nie zaangażowane po stronie dostawców (banki i inne instytucje finansowe), ale również odbiorców – klientów. Jest zupełnie oczywiste, że szybki wzrost sektora finansów nie byłby możliwy, gdyby nie wsparcie, jakie uzyskuje on od sektora ICT (*Information and Communication Technology*), który dostarcza urządzeń technicznych i środków oraz rozwiązań organizacyjnych, które pozwalają na szybki, bezpieczny, niezawodny i łatwy dostęp do informacji finansowych.

Sektor finansów jest w czołówce działów gospodarki, które wydatkują na ICT największy odsetek wartości produkcji (na 2. miejscu, zaraz po branży telekomunikacyjnej – zgodnie z badaniami prof. Michała Golińskiego (IiGC SGH)). Również wg danych McKinsey Global Institute z lat 2015-2017 wyliczony wskaźnik informatyzacji przemysłu plasuje sektor finansów i ubezpieczeń w ścisłej czołówce – na 4. miejscu (za teleinformatyką, mediami i usługami specjalistycznymi) na 22 uwzględnione sektory. Obliczony przez ten sam Instytut indeks digitalizacji przemysłu plasuje finanse i ubezpieczenia na 3. miejscu (za mediami i usługami specjalistycznymi).

Pomimo wydatkowania znaczących kwot i podejmowania ciągłych działań związanych z wdrażaniem technologii teleinformatycznych przez uczestników sektora, mających na celu szybszą i bezpieczną wymianę niezakłóconych informacji, bezustannie obserwuje się wzrost wartości nieuprawnionych operacji (fraudów). Problem nasilił się, gdy banki wprowadziły możliwość obrotu bezgotówkowego przy pomocy kart bankowych (płatniczych i kredytowych), a szczególnie w ostatnich latach, gdy dotychczasowe formy płatności

gotówkowych i kartowych, uzupełnione zostały przez możliwość dokonywania płatności bez karty – CNP (ang. *Card Not Present* – płatności przez telefon, pocztę, Internet).

I w odniesieniu do systemu finansowego, podobnie jak to jest w przypadku każdego systemu, którego elementem jest człowiek, biorąc pod uwagę bezpieczeństwo systemu – najsłabszym ogniwem jest właśnie człowiek. Przy czym o ile po stronie banku/institucji finansowej stosowanie odpowiednich procedur bezpieczeństwa można na pracownikach wymusić, implementując i kontrolując stosowanie rekomendowanych polityk bezpieczeństwa, to po drugiej stronie stoi człowiek (a w zasadzie miliardy ludzi) – klient banku (institucji finansowej) o różnym poziomie wykształcenia, uważności, obycia technicznego, łatwości... , często spieszący się, który chciałby stosowną operację finansową wykonać szybko i wygodnie. I nie zawsze zwracający wystarczającą uwagę na kwestię bezpieczeństwa dokonywanej transakcji.

Nastąpiła ewolucja kanałów dostępu do usług finansowych. Do lat 90. ubiegłego wieku jedyną możliwością wykonania dowolnej transakcji finansowej była wizyta w fizycznym oddziale banku (placówki pocztowej). Lata 90. przyniosły popularyzację płatności kartą, które też wymagały fizycznego kontaktu ze stosownym urządzeniem (bankomatem, terminalem POS (ang. *point of sale*), w najgorszym razie tzw. „żelazkiem” wymagającym autoryzacji podpisem). Rozpowszechnienie się urządzeń mobilnych, zwłaszcza telefonów komórkowych, które w procesie swej ewolucji coraz częściej przybierają formę smartfonów, skłoniła instytucje finansowe do prób ich zastosowania jako kanału dostępu do usług finansowych.

Na każdym etapie ewolucji kanałów dostępu banki, instytucje finansowe i uczciwi klienci stawali przed koniecznością walki z nieuczciwością – możliwymi przypadkami fraudów. Przy czym o ile początkowo były to próby fałszowania pieniędzy i czeków, kopiowaniem paska magnetycznego kart bankowych (tzw. *skimming*), to obecnie repertuar przestępców poszerzył się (bo ze starych metod przecież nie zrezygnowali) o przejmowanie urządzeń mobilnych (zarówno fizyczne – poprzez kradzież urządzenia, jak i niefizyczne – poprzez wyłudzenie informacji logowania lub zainstalowanie szkodliwego oprogramowania (ang. *malware*)).

Rezygnacja przez klientów z operacji gotówkowych, a nawet kartowych i przejście na korzystanie z bankowości mobilnej, jest spowodowana wygodą. W jednym urządzeniu, z którym się praktycznie nie rozstają, mają wielofunkcyjne narzędzie, które oprócz udostępniania typowych funkcjonalności, pozwalających na prowadzenie rozmów, słuchanie muzyki, robienie zdjęć etc., może również służyć jako urządzenie dostępowe do banku, zastępujące kartę bankową. Można przy jego pomocy sprawdzać stan konta, ale również dokonywać płatności i korzystać z innych usług bankowych. Użyteczność jest tutaj najważniejsza,

bezpieczeństwo schodzi na plan drugi. Wielu użytkowników nie dba nawet o najprostsze oferowane zabezpieczenie, jakim może być hasło PIN lub wzór, który należy odwzorować na ekranie dotykowym, by odblokować telefon. Z drugiej strony tylko część spośród dostępnych na rynku i używanych urządzeń posiada odpowiednio wysokiej jakości czujniki biometryczne, pozwalające na uruchomienie urządzenia dopiero po autentykacji przy pomocy danych biometrycznych (np. odcisku palca lub fotografii twarzy).

Mobilna aplikacja finansowa zainstalowana na telefonie klienta stanowi punkt wejścia do systemu transakcyjnego banku. I banki są zobowiązane do tego, by zaprojektować taki sposób dostępu do systemu, by jednoznacznie zidentyfikować i uwierzytelnić klienta. Stosowane są przy tym różnego rodzaju mechanizmy, coraz częściej dwuetapowe: PIN, hasła jednorazowe, biometria fizyczna. W ostatnim czasie banki coraz częściej wykorzystują metody biometrii behawioralnej, szczególnie predystynowane do tego, by móc je stosować w środowiskach mobilnych. Metody tego rodzaju wykorzystują różne czujniki, w jakie standardowo wyposażane są współczesne smartfony. Scenariusze, w jakich metody te mogą być stosowane obejmują możliwość identyfikacji klienta poprzez tzw. podpis behawioralny, wykrywanie fraudów, jak również jako jeden z elementów służących do uwierzytelniania klienta.

I z racji przedstawionej sytuacji, zajęcie się przez Doktoranta problemem wykorzystania biometrii behawioralnej do opracowania nowych metod uwierzytelniania, które praktycznie bez świadomych działań użytkownika pozwalają na dostarczenie tarczy, która ochroni go przed oszustwami, szkodliwym oprogramowaniem, zapobiegnie przed kradzieżą danych uwierzytelniających, należy znać za ważne, oryginalne i mieszczące się w nurcie aktualnych badań.

4. Sformułowanie celu badawczego i tezy pracy

W swej rozprawie mgr Piotr Kałużny zdefiniował następujący problem badawczy (str. 13): *instytucje finansowe wymagają opracowania metod uwierzytelniania dostosowanych do środowiska aplikacji mobilnych, które mogą wzbogacić obecne systemy wykrywania nadużyć na poziomie transakcyjnym, zachowując jednocześnie bezpieczeństwo i poprawiając użyteczność samego procesu w porównaniu z obecnie stosowanymi metodami.*

To pozwoliło mu na sformułowanie 5 pytań badawczych (RQ1 ÷ RQ5), które uszczegóławiają problem główny odnośnie do: wymagań nakładanych na metodę uwierzytelniania w aplikacjach mobilnych; sensorów i metod, jakie można zastosować przy opracowywaniu nowej metody uwierzytelniania; właściwości wzorca behawioralnego



użytkownika; właściwości, które potraktowane łącznie pozwolą na zaprojektowanie metody autentykacji do realizacji płatności bankowych; scenariuszy, które mogą posłużyć do oceny i uwiarygodnienia wyników użycia nowej metody (str. 13).

Głównym celem badań, dla którego Autor tak wnikliwie scharakteryzował problemy związane z zastosowaniem mobilnych aplikacji finansowych, a zwłaszcza wykorzystywanych w nich metod uwierzytelniania użytkowników, było zaprojektowanie własnej metody uwierzytelniania, która mogłaby działać w mobilnej aplikacji finansowej i wykazywać przy tym niższy poziom błędów niż obecnie stosowane metody mobilnego uwierzytelniania (str. 13).

Przy tak zdefiniowanym problemie badawczym i celu badań, postawiona przez niego teza pracy jest dość oczywista (str. 14):

Zaprojektowana przy użyciu biometrii behawioralnej metoda uwierzytelniania może zostać wdrożona w mobilnej aplikacji finansowej i osiągnąć niższy poziom błędów niż obecnie stosowana mobilna metoda wykrywania twarzy, zapewniając przy tym wyższą użyteczność.

Wzmiankowane wyżej pytania badawcze, skutkowały sformułowaniem przez Doktoranta następujących cząstkowych celów badawczych (RG1 ÷ RG5) (str. 14-15):

RG1 Budowa modelu wymagań dla metody uwierzytelniania biometrii behawioralnej w środowisku finansowym.

RG2 Analiza wyników badań z zakresu biometrii behawioralnej w celu doboru metody dopasowanej do środowiska mobilnych aplikacji finansowych.

RG3 Charakterystyka właściwości, które mogą identyfikować i pozwalać na uwierzytelnienie użytkowników w oparciu o wybraną metodę.

RG4 Zaprojektowanie metody uwierzytelniania, która będzie spełniać kryteria odnośnie do dokładności i współczynnika błędów, a jednocześnie będzie spełniać inne wymagania podczas realizacji różnych scenariuszy bankowych i płatniczych.

RG5 Ocena wydajności zaprojektowanej metody na podstawie wcześniej zdefiniowanych kryteriów i uwiarygodnienie jej w scenariuszach właściwych dla mobilnych aplikacji finansowych, aby udowodnić jej użyteczność w wybranym środowisku.

A zatem problem badawczy i wynikające z niego pytania badawcze, teza i cel główny oraz cele szczegółowe pracy sformułowane zostały klarownie. Pozwala to stwierdzić, że zostały trafnie sformułowane i znalazły swoje odbicie w dalszej części pracy.

Doktorant szczegółowo opisuje zastosowaną w prowadzonych przez siebie badaniach i w efekcie w napisanej przez siebie pracy, metodę badawczą. Prace te prowadził zgodnie z paradygmatem projektowania DSR (*Design Science Research*) Hevnera, Marcha, Parka i Rama. Zgodnie z tym paradygmatem artefakty powstałe podczas procesu projektowania muszą

stanowić nowatorskie (lub ulepszone) rozwiązanie problemu, który jest ważny dla środowiska i uzasadniony naukowo. W przypadku omawianej pracy środowiskiem jest sektor usług finansowych, a artefaktem opracowana przez Doktoranta metoda nawiązująca do biometrii behawioralnej, wykorzystująca profil dotyku ekranu urządzenia mobilnego. Z kolei weryfikacja i walidacja opracowanej metody została przeprowadzona podczas serii eksperymentów badawczych, w które zaangażowano sporą grupę osób. Pozwala to stwierdzić, że przeprowadzone badania plasują się na przecięciu finansów, ekonomii ilościowej i informatyki. Cały zaprojektowany przez siebie proces badawczy został przez Doktoranta szczegółowo opisany w podrozdz. 1.3, zrobione to zostało klarownie i z pełnym uzasadnieniem.

5. Wiedza Autora oraz znajomość współczesnej literatury z dyscypliny naukowej, której dotyczy rozprawa

Autor rozprawy wykazuje dobrą znajomość dorobku literaturowego dotyczącego zagadnień, którym poświęcona jest rozprawa. Przegląd tych zagadnień został dokonany w pierwszej części pracy (rozdz. 2 i 3).

Rozdział 2 poświęcony został przeglądowi piśmiennictwa z zakresu mobilnych aplikacji finansowych. Opisał w nim rolę, jaką pełni bankowość i systemy płatnicze we współczesnym systemie gospodarki cyfrowej. Scharakteryzował trendy rozwojowe oraz problemy, przed jakimi staje sektor finansów. W przekonujący sposób scharakteryzował rynek i panujące na nim tendencje, kształtujące produkty i usługi oferowane klientom sektora finansowego, zwracając szczególną uwagę na problem związany ze stopniową konwersją sektora finansowego w kierunku modelu mobilnego, zwracając szczególną uwagę na innowacje w tym sektorze (podrozdział 2.1). Omówił rolę banków i systemów płatności w gospodarce cyfrowej, omawiając przede wszystkim rodzaje płatności mobilnych i nowych usług finansowych, jak również systemy wykrywania przestępstw (podrozdział 2.2). Podrozdział 2.3 poświęcony został wymaganiom, jakim muszą sprostać systemy weryfikacyjne w branży finansowej, aktualną praktyką stosowanych rozwiązań i ich niedogodnościami, i to zarówno z punktu widzenia banków, jak i ich klientów.

Bardzo obszerny rozdział 3 został poświęcony opisowi stanu wiedzy teoretycznej i praktyki w odniesieniu do metod biometrycznych uwierzytelniania klientów. Autor przeanalizował dostępne sensory i metody, które mogą służyć i służą do identyfikacji, uwiarygodniania i autoryzowania użytkowników. Przedstawiony został proces autentykacji i kształtujące go czynniki (3.1), miary oceny poszczególnych metod uwierzytelniania (3.2),



atrybuty biometryczne i ich właściwości (3.3) i metody biometrii behawioralnej (3.4). W rozdziale tym, w oparciu o liczną, bardzo aktualną literaturę, przeprowadzono analizę poszczególnych metod, wskazując na ich zalety i wady. W oparciu o tę analizę, Autor zdecydował się w dalszych badaniach skupić się na najbardziej obiecujących i niezbyt dotychczas wyeksploatowanych, metodach biometrii behawioralnej.

Dołączony do pracy spis literatury jest bardzo obszerny, liczy około 200 pozycji i wydaje się, że rzeczywiście na wszystkie te źródła Doktorant powołał się w tekście. Trochę niepokojące jest, że Autor nie powołuje się na źródła polskojęzyczne, ale prawdopodobnie na gruncie teoretycznym tematyka ta nie jest w Polsce popularna, a po drugie – w związku z ogólną polityką grantową, wszystkie znaczące publikacje muszą być publikowane w językach konferencyjnych. Zdając sobie sprawę z tego, że literatura dotycząca tych zagadnień może być jeszcze bogatsza, niż przedstawił to Autor, zwłaszcza w odniesieniu do tematyki, jaką poruszył w rozdziale 2, stwierdzam, że dobór literatury został dokonany właściwie i w pełni odpowiada potrzebom pracy.

A zatem, podsumowując, Doktorant wykazał się wiedzą teoretyczną i znajomością literatury z zakresu finansów, rynków finansowych, płatności mobilnych, metod weryfikacji, ale również metodyki prowadzenia prac naukowych.

5. Logika argumentacji

Głównym celem pracy było scharakteryzowanie warunków, jakie powinna spełniać nowa metoda, która mogłaby być zastosowana w bankowości mobilnej i zaprojektowanie własnej metody uwierzytelniania, która mogłaby działać w mobilnej aplikacji finansowej i wykazywać przy tym niższy poziom błędów niż obecnie stosowane metody mobilnego uwierzytelniania (str. 13), oprócz tego Autor sformułował dodatkowe cele szczegółowe, rozwijające i uzupełniające cel zasadniczy (str. 13-14). Własna metoda uwierzytelniania, czyli główny cel pracy, został opisany w rozdz. 4. Ale zanim do tego doszło, Autor zrealizował cel szczegółowy RG1, czyli sformułował wymogi, jakie musi spełniać każda rozsądna, wiarygodna i efektywna metoda uwierzytelniania (podrozdz. 2.3); opisał istniejący stan rzeczy (*state of the art*) w odniesieniu do biometrycznych metod identyfikacji (podrozdz. 3.4) – czyli zrealizował cel RG2; scharakteryzował właściwości, jakie powinna posiadać każda biometryczna metoda weryfikacyjna (rozdz. 3 – realizacja celu RG3); zaprojektował własną metodę – cel RG4 (rozdz. 4) i ją zweryfikował przy zastosowaniu różnych scenariuszy – RG5 (rozdz. 5).

Zastosowana procedura badawcza jest w pełni logiczna: sformułował wymagania stawiane przed metodami uwierzytelniania – dokonał krytycznego przeglądu istniejących metod – opracował własną – zweryfikował jej skuteczność i użyteczność.


Warto zaznaczyć, że niezależnie od wielkiej pracy włożonej przez Doktoranta w przegląd literaturowy, trzeba podkreślić wielość działań, których dokonał podczas weryfikacji i walidacji stworzonej przez siebie metody. Eksperymenty przeprowadził nie tylko na dostępnych publicznie zbiorach danych, ale również zastosował zbiór danych utworzony samodzielnie, uzyskany z wykorzystaniem aplikacji zrobionej przez studentów, pracujących pod jego kierunkiem.

Podsumowując: Doktorant zrealizował zarówno cel główny, jak i cele szczegółowe, a osiągając cele szczegółowe – wykazał tezę pracy. Zastosowana metoda badawcza, logika argumentacji, sposób dowodzenia tezy – nie budzą zastrzeżeń i są adekwatne do tematyki pracy.

6. Nowatorstwo wyników

W rezultacie przeprowadzonych badań, Doktorantowi udało się osiągnąć wyniki, które można uznać za wnoszące wkład do nauki. Za największy wkład należy jednoznacznie uznać opracowanie metody biometrycznego uwierzytelnienia behawioralnego wykorzystującej profil dotyku ekranu urządzenia mobilnego. Podkreślić trzeba, że jest to metoda bardzo bezpieczna (wykazująca niską wartość wskaźnika EER), ale z punktu widzenia użytkownika – zupełnie „przezroczysta”, wykorzystywane dane z ekranu dotykowego nie są wymuszane przez system, ale klient wprowadza je bezwiednie, niejako przy okazji, dokonując manipulacji na ekranie dotykowym, przez co systemy informatyczne wykorzystywane w sektorze finansowym (w bankach i innych instytucjach finansowych), mogą być bezpieczniejsze i w lepiej zapobiegać fraudom i nieuczciwemu użyciu. I w tym sensie zaproponowana nowatorska metoda, która jest innowacyjna w odniesieniu do usług finansowych, stanowi autorski wkład w dyscyplinę ekonomii i finansów, w dziedzinie nauk społecznych. Metoda ta, oprócz walorów naukowych, może mieć również bezpośrednie zastosowanie praktyczne. I w tym miejscu rodzą się pytania: czy metoda została opatentowana? i czy została już gdzieś praktycznie wykorzystana?

Za ważny wkład Autora uważam również opracowany przez niego model wymagań stawianych przed metodami autentykacji stosowanymi w mobilnych usługach finansowych. Opisany on został w rozdz. 2.3.4, nie tylko specyfikuje on najważniejsze cechy metod, które stosowane są do identyfikacji i uwierzytelniania klientów w aplikacjach finansowych, ale



również wskazuje na relacje i zależności istniejące pomiędzy poszczególnymi właściwościami tych modeli (rys. 2.12, str. 58).

7. Kompozycja/konstrukcja pracy/przeprowadzone badania

Układ pracy jest typowy dla tego rodzaju prac: przegląd literatury – opracowanie modelu – analiza i weryfikacja modelu – wnioski. Wszystkie przeprowadzone na rzecz pracy i opisane eksperymenty zakończone zostały logicznie wyciągniętymi z nich wnioskami.

Ponieważ o przeglądzie literatury i samym modelu była już w recenzji mowa, w tym miejscu warto zwrócić uwagę na przeprowadzone przez Doktoranta eksperymenty, mające na celu uwiarygodnienie jego nowej metody. W tym celu posłużył się dwoma rodzajami źródeł danych: danymi powszechnie dostępnymi (zarówno bezpłatnymi, jak i komercyjnym zbiorem danych), ale również zbiorem własnym, otrzymanym z przebadania 88 uczestników, którzy korzystali z napisanej przez studentów aplikacji. Warto podkreślić tę dwoistość źródeł danych. Oparcie się wyłącznie na zbiorze własnym mogłoby budzić obawę, że zbiór ten został sztucznie dobrany w taki sposób, by wykazać doskonałość opracowanej metody autorskiej. Z drugiej strony – wykorzystanie wyłącznie źródeł publicznych mogłoby budzić obawę, że metoda „została skrojona” pod dostępne dane. Wykorzystanie obydwu rodzajów źródeł danych pozwala rozwiązać te wątpliwości.

Nawiązując jeszcze do eksperymentów Doktoranta warto zauważyć, że jego metoda pozwala nie tylko na stosowanie do wykrywania fraudów, ale również, ze stosunkowo dobrą skutecznością, rozpoznawać wiek i płeć osoby poddanej eksperymentowi.

Reasumując tę część recenzji stwierdzam, że Doktorant wykazał się bardzo dobrą umiejętnością samodzielnego prowadzenia pracy naukowej, czego efekty przedstawił w dobrze skomponowanej dysertacji doktorskiej.

8. Jasność przekazu myśli / redakcja pracy / kwestie techniczne

Tekst pracy napisany jest dobrym językiem, Doktorant dość jasno przekazał swoje myśli. Literówki są bardzo nieliczne. Czytanie dysertacji bardzo ułatwił zabieg redakcyjny polegający na tym, że każdy rozdział rozpoczyna się kilkuzdaniową zapowiedzią treści, a kończy się podsumowaniem, zawierającym kompendium zrealizowanych prac i osiągniętych wyników.

Redakcja pracy jest bardzo staranna, nie znalazłem żadnych typowych błędów polegających, przykładowo, na błędnej numeracji rysunków i tabel.



Ale nie mogę się pohamować, by nie zgłosić jednego zastrzeżenia o charakterze technicznym, którego winowajcą w żadnej mierze nie jest Doktorant. Otóż, egzemplarz pracy doktorskiej, który otrzymałem pocztą, zaraz po wyjęciu z koperty rozpadł mi się w rękach na pojedyncze kartki. Co w sumie okazało się korzystne, bo wyjeżdżając na wakacje mogłem zabrać ze sobą tylko połowę pracy. Ale może to tylko symbol tego, że praca była za długa? Abstrahując od dodatków, praca liczy 200 stron i w moim przekonaniu, bez utraty jakości, można by ją skrócić o 50 stron.

9. Sprawy dyskusyjne

Wymienionych poniżej uwag jest wyjątkowo mało, co świadczy o jakości pracy, na dodatek mają one charakter trzeciorzędny. Niemniej, pozwolę sobie je wyspecyfikować:

- w całej pracy Doktorant opracowaną przez siebie metodę nazywa „*proposed method*” (proponowana metoda), „*own method*” (metoda własna) lub „*designed method*” (zaprojektowana metoda). Wszystkie te sformułowania są wyjątkowo niezręczne. O wiele wygodniejsze dla czytelnika, a jednocześnie potencjalnie lepsze promocyjnie, byłoby nadanie tej metodzie nazwy własnej (choćby „Kaluźny Method” lub POZmet) i ewentualnie jakiegoś pochodzącego od nazwy skrótu (np. PKM), który po wielokrotnym powtórzeniu w tekście utrwaliłby się w pamięci odbiorcy. Nie można marnować takiej sposobności na promowanie metody, tym bardziej, że byłoby to z korzyścią dla klarowności tekstu i stanowiło ułatwienie dla czytelnika.
- podobną uwagę (dotyczącą nazwy indywidualnej) można mieć w odniesieniu do zgromadzonego przez Autora zbioru danych, nazywanego przez niego *Own Dataset*.
- czy zgromadzony przez Autora własny zbiór danych nie mógłby być większy? Czy nie udało mu się dotrzeć do większej liczby chętnych do współpracy osób? Na cudze zbiory danych nie ma się wpływu, ale zbiór własny można by rozbudować.
- czy *Own Dataset* zostanie (a może już został?) upubliczniony?

Uwagi redakcyjne:

- w spisie treści (str. iv, po załącznikach) zabrakło „Bibliografii” oraz strony, na której się zaczyna.
- numeracja sekcji 3.1.1 , 3.5.1 , 5.1.1 , 5.3.1 – są to jedyne sekcje w odpowiednich podrozdziałach i w takim przypadku opatrzenie jej numerami jest niewskazane.

10. Wnioski końcowe

Praca stanowi ważny wkład Autora w rozwój badań naukowych odnoszących się do dyscypliny ekonomii i finansów, a ogólniej – do dziedziny nauk społecznych. Opracowanie jest w pełni oryginalne. Doktorant opracował temat z dużym wkładem pracy własnej, a postawione przed sobą cele udało mu się osiągnąć. Logika argumentacji jest jasna, a propozycje teoretyczne zostały poparte eksperymentami. Warto też dodać, że tematyka podjęta w pracy nie jest wydumana, lecz wyrosła bezpośrednio z praktycznych potrzeb sektora finansowego, który, jak cała gospodarka, podlega cyfryzacji. Praca mgra Piotra Kałużnego spełnia wymogi stawiane rozprawom doktorskim i dlatego wnoszę o dopuszczenie jej do publicznej obrony.

A. Upiński