UNIWERSYTET EKONOMICZNY W POZNANIU

Piotr Kałużny

Behaviour-based user authentication for financial services

Behawioralne uwierzytelnianie użytkowników usług sektora finansowego

Streszczenie pracy doktorskiej

Promotor: prof. dr hab. Witold Abramowicz

Promotor pomocniczy: dr hab. Agata Jolanta Filipowska

Poznań 2021

Uzasadnienie tematu pracy

Rosnąca liczba oszustw internetowych w sektorze finansowym (European Central Bank, 2019), wraz ze znaczącym wzrostem udziału kanału mobilnego w liczbie klientów, stwarza nowe zagrożenia dla sektora. Problem oceny skuteczności i bezpieczeństwa uwierzytelniania zyskuje na istotności w artykułach naukowych (Fridman i in., 2017; Patel i in., 2016), badaniach rynkowych (Visa, 2017) oraz w dyrektywie unijnej PSD 2 - Payment Services Directive (Europen Comission, 2015).

W roku 2018 (Meola, 2019) wartość globalnych aktywów rynków finansowych oszacowano na 124 biliony dolarów. Usługi finansowe na tych rynkach charakteryzują się znacznym wzrostem. Przy skumulowanym rocznym wskaźniku wzrostu wynoszącym 5,9% (The Business Research Company, 2019), powinny osiągnąć ok. 22,5 tys. mld USD w 2021 r. Potencjalne wyzwania technologiczne i organizacyjne związane z ich świadczeniem stają się coraz ważniejsze z perspektywy podmiotów bezpośrednio zaangażowanych: klientów, banków i innych instytucji finansowych.

Jednak pomimo szybkiego rozwoju technologii pozwalającej na lepszą wymianę informacji, pomiędzy uczestnikami sektora, łączna wartość nieuprawnionych transakcji (ang. fraud) rośnie. Całkowita liczba płatności bezgotówkowych w strefie euro została oszacowana przez Europejski Bank Centralny (EBC) na 98 mld w 2019 r., przy łącznej wartości 162,1 mld euro, co oznacza wzrost o 8,1% od 2018 r. W Europie, przy użyciu kart wyemitowanych na całym świecie w ramach SEPA (Jednolity Obszar Płatności w Euro) straty w związku z oszustwami wyniosły 1,80 mld euro tylko w 2018 r. (European Central Bank, 2019). Jeśli chodzi o karty wydane tylko w strefie euro, łączna wartość nieuprawnionych transakcji kartowych na całym świecie wyniosła 0,94 mld euro w 2018 r. 79% wartości oszustw należało do kategorii płatności wykonanych bez karty (ang. CNP, tj. płatności przez Internet, pocztę lub telefon). Oszustwa CNP w 2018 r. (Wzrost o 17,7% w porównaniu z 2017 r.) sumowały się do kwoty 1,43 mld euro strat związanych z nieuprawnionymi transakcjami. Stwarza to poważny problem dla współczesnej gospodarki, a w szczególności dla sektora finansowego, który powinien zminimalizować wartości oszustw, aby stworzyć lepsze warunki rynkowe i zagwarantować stabilność sektora.

Wzrasta również popularność urządzeń mobilnych jako kanału dostępu do usług finansowych. W związku z tym tradycyjny model oddziałów fizycznych w instytucjach fi-

nansowych ustępuje nowemu, mobilnemu. Klienci z wykorzystaniem komórki nie tylko sprawdzają stan swojego konta, ale także dokonują płatności i korzystają z nowych usług. Raport dotyczący perspektyw bankowych Deloitte 2018 uwidacznia trudności związane z transformacją obecnych modeli bankowych. Jako cel uznano bankowość „mobilną" (ang. mobile-centric) i „zorientowaną na klienta" (ang. customer-centric) (Srinivas i in., 2018). Oprócz szans dla nowych sposobów realizacji usług istnieje także wiele zagrożeń dla tego środowiska, nieodłącznie związanych z transakcjami finansowymi, ale także z wykorzystywanymi urządzeniami i systemami operacyjnymi w sferze mobilnej.

Badania ankietowe pokazują, że klienci banków i instytucji finansowych nie są w stanie ocenić, w jakim stopniu bezpieczne są używane przez nich usługi (Imgraben i in., 2014; Visa, 2017). W przypadku kanału mobilnego wzrasta zaufanie do takich rozwiązań, ale nie świadomość zagrożeń (w rozumieniu ang. security awareness). Problemem może być złożoność stosowanej obecnie technologii.

Wygoda jest jednym z głównych powodów, dla których użytkownicy korzystają z bankowości mobilnej i nie chcą nosić przy sobie gotówki. Interesuje ich również bezpieczeństwo oferowanych usług (Visa, 2017). Zapewnienie ochrony urządzenia jest natomiast składnikiem bezpieczeństwa realizacji usługi. Jednak korzystanie z tradycyjnego modelu zabezpieczeń w postaci haseł i biometrii fizycznej okazuje się niewystarczające. Nie wszystkie urządzenia mobilne są wyposażone w wymagane czujniki biometryczne odpowiedniej jakości, a około 40% usługobiorców w żaden sposób nie zabezpiecza swojego urządzenia - czy to za pomocą kodu PIN, czy danych biometrycznych (Fridman i in., 2017). Stanowi to poważne zagrożenie i barierę dla możliwości zapewnienia bezpieczeństwa transakcji i zapobieganiu oszustwom finansowym.

Dostawcy nie tylko udostępniają klientom swoje usługi w kanale mobilnym, ale muszą również brać pod uwagę możliwość przejęcia urządzenia w sposób nieuprawniony. Może się to zdarzyć w wyniku kradzieży, wyłudzenia informacji logowania lub poprzez zainstalowanie złośliwego oprogramowania (ang. malware). Obecnie banki wykorzystują głównie dane statyczne i transakcyjne do swoich systemów zwalczania nadużyć finansowych, nie mając narzędzi do przeciwdziałania wyżej wymienionym zagrożeniem. Mając do dyspozycji urządzenia mobilne, mogłyby wzbogacić je o dane behawioralne generowane przez te urządzenia.

Model bezpieczeństwa wykorzystujący hasła lub kody PIN staje się niewystarczający dla osób, które używają bardzo prostych, przewidywalnych haseł lub ponownie wykorzystują je do różnych aplikacji. Dzieje się tak, ponieważ klienci muszą pamiętać wiele haseł do różnych usług (Bonneau i Preibusch, 2010). Zastosowanie czynnika wrodzonego (ang. inherence) i tokenów pozwala na stosowanie prostszych, jednorazowych haseł (OTP), generowanych w aplikacjach typu BLIK lub udostępnianych przez SMS. Jednak bezpieczeństwo generowania takiego tokenu nadal zależy od bezpieczeństwa samego urządzenia, które może być zagrożone przez wspomniane powyżej rodzaje ataku. Istotnym problemem jest również uwierzytelnianie w przypadku zagrożenia nazwanego wewnętrznym zagrożeniem uwierzytelniania (ang. „insider authentication threat") (Hayashi i in., 2012; Muslukhov i in., 2013), w którym osoba znana właścicielowi urządzenia, mająca dostęp do niego lub czynników uwierzytelniania, uzyskuje celowy lub nie, nieuprawniony dostęp do usług i może w ten sposób wykonać niechcianą transakcję. Katalog potencjalnych sprawców obejmować może rodzinę użytkownika, współmałżonka/e lub dzieci dokonujące transakcji bez wiedzy posiadacza rachunku. Scenariusz ten staje się coraz powszechniejszy, chociażby w sytuacjach, gdy dzieci mogą dokonywać nieautoryzowanych transakcji kartą płatniczą dostępną w telefonie komórkowym rodzica za pośrednictwem gier mobilnych i podobnych aplikacji.

Problemy związane z przejściem sektora finansowego do modelu mobilnego (ang. „mobile centric") (Deloitte Center for Financial Services, 2018) są różnorodne, bezsprzecznie związane z adopcją metod uwierzytelniania i wykrywania nadużyć dla tego środowiska. Aby zapobiegać oszustwom i zapewnić bezpieczeństwo transakcji, banki i firmy finansowe mogą korzystać z niedawno opracowanych metod biometrii behawioralnej, które są szczególnie dostosowane do środowiska mobilnego. Wykorzystują one różnorodność czujników dostępnych we współczesnych smartfonach. Ta nowa grupa metod może być używana w różnych scenariuszach, od wzbogacania istniejących mechanizmów autoryzacji o podpis behawioralny, po wykrywanie oszustw lub pracę jako samowystarczalny komponent w procesie uwierzytelniania. Mogą również odpowiedzieć na pytanie: czy dane generowane przez urządzenia mobilne (wykorzystywane również w metodach biometrii behawioralnej) można wykorzystać do ulepszenia usług finansowych?

Ogromnym znaczeniem dla tego sektora byłoby opracowanie metody niezawodnej, bardziej dostosowanej do tego środowiska, zapewniającej nie tylko bezpieczne, ale i użyteczne procesy uwierzytelniania. Umożliwienie oceny ryzyka i dostarczenie mechanizmów chroniących użytkowników przed oszustwami, złośliwym oprogramowaniem i wykorzystywaniem skradzionych danych uwierzytelniających przy jednoczesnym zachowaniu użyteczności i ochrony ich poufnych danych to nowe wyzwania, którym metoda powinna sprostać. W związku z powyższym uzasadnione jest przeprowadzenie badań nad wymaganiami dla nowych metod, które mogą być wykorzystywane w bankowości mobilnej i aplikacjach płatniczych oraz opracowanie rozwiązania mogącego poprawić bezpieczeństwo i użyteczność obecnego procesu uwierzytelniania w bankowości mobilnej i aplikacjach płatniczych.

Zgodnie z przedstawionymi powyżej potrzebami, zdecydowano się na sformułowanie w pracy następującej tezy:
Możliwe jest zaprojektowanie metody uwierzytelniania wykorzystującej biometrię behawioralną, która wdrożona w mobilnej aplikacji finansowej osiągnie poziom błędów niższy niż obecnie stosowane metody wykrywania twarzy na urządzeniach mobilnych, zapewniając przy tym wyższą użyteczność.

Metoda badawcza

Prace badawcze prowadzone były zgodnie z paradygmatem projektowania Hevnera (ang. Design Science) (Hevner i in., 2004). Temat pracy znajduje się na przecięciu ekonomii ilościowej, finansów i informatyki. Obowiązują również specjalne wytyczne dotyczące systemów informacyjnych. Nauka o projektowaniu w badaniach nad systemami informacyjnymi (IS) prowadzi do tworzenia artefaktów, w celu rozwiązywania problemów badawczych (Prat i in., 2014). Artefakty powstałe w trakcie tego procesu muszą stanowić nowatorskie lub ulepszone rozwiązanie ważnego problemu, który jest istotny dla środowiska (w tym wypadku usług sektora finansowego) i naukowo uzasadniony. Dowodzi tego weryfikacja i walidacja przeprowadzona podczas eksperymentów w procesie badawczym. Głównym przedmiotem rozprawy było opracowanie metody biometrycznego uwierzytelniania behawioralnego wykorzystującej profil dotyku ekranu urządzenia mobilnego. Jednak pomimo praktycznego charakteru wy-

ników, przyjęta metodologia obejmuje również bardziej teoretyczne typy artefaktów. Konstrukty (ang. constructs) wprowadzają terminologię używaną do opisu problemów i rozwiązań. Mimo tego, że niektóre artefakty mogły być wynikiem wcześniejszych prac, dążenie do rozszerzenia lub ujednolicenia konstruktów w literaturze jest przyczynkiem do wkładu teoretycznego. Modele (ang. models) używają konstruktów do tworzenia reprezentacji problemów i potencjalnych rozwiązań. Metody (ang. methods) są powiązane z konkretnym rozwiązaniem wspomnianego problemu i mogą przedstawiać algorytmy lub opisy tekstowe. Instancje (ang. instantiations) są dowodem na to, że zaprojektowane konstrukcje, modele i metody mogą być wykorzystywane w działających systemach i dowodzą ich wykonalności. Mogą być one pomyślną implementacją metody przeprowadzoną na rzeczywistych danych i podlegać rygorystycznemu procesowi oceny, który mierzy użyteczność, jakość jak i osiągnięty poziom dokładności artefaktu projektowego. Wszystkie wymienione kategorie obiektów opracowanych w pracy są wymienione w tabeli 1.

Cele badawcze

Tematem rozprawy było zaproponowanie nowatorskiego podejścia, które dzięki zastosowaniu metod biometrii behawioralnej, będzie w stanie uwierzytelnić użytkowników usług sektora finansowego. W ramach proponowanego podejścia opracowano metodę wykorzystującą algorytmy uczenia maszynowego i biometrię profilu dotyku ekranu urządzenia mobilnego. Może ona zapewnić ocenę ryzyka na poziomie transakcyjnym oraz zwiększyć bezpieczeństwo mobilnych aplikacji finansowych. W trakcie badań, do weryfikacji wydajności metody uwierzytelniania i osiągniętych wskaźników błędów, wykorzystano zbiory danych z wielu urządzeń z ekranem dotykowym. Wykorzystane dane uwzględniały łącznie 390 użytkowników. Obejmowały one także własny zbiór danych, zebrany na urządzeniach pracujących na systemie operacyjnym Android. Zawierał on unikalne informacje na temat osi pomocniczej i głównej obszaru dotyku oraz odczyty czujników bezwładnościowych tj. akcelerometr, które mogą poprawić dokładność klasyfikatora.

Głównym celem badań było zaprojektowanie metody uwierzytelniania, która może działać w mobilnej aplikacji finansowej i osiągać poziom błędów niższy niż obecnie stosowane metody uwierzytelniania mobilnego (takie jak rozpoznawanie twarzy). Zapew-

Tabela 1. Opis artefaktów zaprojektowanych i przedstawionych w dysertacji.

Typ artefaktu	Opis
Konstrukt	Ujednolicenie stosowanych pojęć jest zawarte w glosariuszu, a poszczególne istotne terminy finansowe są szczegółowo opisane w rozdziale 2. Budowanie modelu wymagań i konstrukty w nim stosowane przedstawiono w rozdziale 2. Opis pojęć związanych z uwierzytelnianiem i biometrią behawioralną zawarto w rozdziale 3.
Model	Na podstawie wprowadzonych konstruktów związanych z tematyką sektora finansowego, przedstawionych na końcu rozdziału 2, zaprezentowano model wymagań dotyczących metod uwierzytelniania w środowiskach finansowych. Różnorodne podejścia do uwierzytelniania behawioralnego wskazujące możliwe rozwiązania problemu przedstawione są na końcu rozdziału 3.
Metoda	W rozdziale 4 znajduje się sposób opracowania rozwiązania adresującego problem badawczy zawarty w rozprawie. Wykorzystując określone cechy wyodrębnione z zachowania użytkownika podczas interakcji z ekranem dotykowym urządzenia mobilnego, zapewnia on formalizację prezentowanego artefaktu.
Instancja	W rozdziale 5 metoda jest weryfikowana z wykorzystaniem wielu zbiorów danych, co dowodzi jej zgodności z wymaganiami i możliwości implementacji. W dalszej części rozdziału przedstawiono podejście wykorzystujące wdrożoną instancję i zwalidowano je pod kątem scenariuszy użycia w aplikacji finansowej, co prezentuje wykonalność jej wdrożenia.

Źrodło: opracowanie własne

niając przy tym wyższą użyteczność, a także wykorzystanie do wzbogacenia obecnych systemów wykrywania nadużyć i oszustw finansowych.

Uwzględniając wybrany temat badawczy, mając na uwadze motywację przedstawioną w pracy, stan wiedzy na temat metod biometrycznych oraz wyzwania i wymagania dla sektora finansowego, postawiono następujące pytania badawcze:

RQ1: *Jakie są wymagania dotyczące metody uwierzytelniania, która może być wykorzystana w bankowości mobilnej i aplikacjach płatniczych z punktu widzenia klientów, dostawców (banków i instytucji finansowych) oraz stron trzecich?*

RQ2: *Jakie czujniki, metody i ich kombinacje, można wykorzystać do behawioralnego uwierzytelniania w mobilnych aplikacjach finansowych?*

RQ3: *Jakie cechy użytkownika mogą być wykorzystane do stworzenia jego profilu behawioralnego?*

RQ4: *Czy można wybrać metody komplementarne, w stosunku do zdefiniowanych cech i połączyć je w celu stworzenia modelu, który może spełnić wymagania dotyczące bankowości i wykorzystania w scenariuszu płatności?*

RQ5: *Jakie scenariusze można wykorzystać do porównania opracowanej metody w wybranej domenie oraz jak zewaluować i zwalidować rezultaty osiągnięte przez metodę w mobilnej aplikacji finansowej?*

Zaprojektowanie metody dostosowanej do wymagań mobilnych usług finansowych, zweryfikowanej na wielu zbiorach danych (w tym nowego zbioru danych aplikacji zbieranych wyłącznie na potrzeby tego badania), prezentuje oryginalność rozwiązania. Proces przeprowadzenia eksperymentów z wykorzystaniem klasyfikatorów takich jak XGboost, wykorzystanie wielu akcji użytkowników do klasyfikacji i porównanie różnic mierzonych na podstawie zaprojektowanego scenariusza weryfikacyjnego to główne elementy wskazujące na wkład pracy w stosunku do aktualnego stanu wiedzy.

Struktura pracy

Rozprawa składa się z 6 rozdziałów, w tym wprowadzenia i podsumowania. W pierwszym rozdziale przedstawiono motywację, pytania badawcze, cele i tezę pracy. Zagadnienia dotyczące mobilnych aplikacji finansowych zostały opisane w rozdziale 2 wraz z modelem wymagań metod uwierzytelniania odpowiednich dla środowiska usług finansowych. Rozdział 3 przedstawia aktualny stan wiedzy na temat rodzajów danych i metod biometrycznych, a także przebiegu samego procesu uwierzytelniania. Rozdział 4 wskazuje na założenia, rozważania projektowe i ograniczenia, które są związane z kryteriami weryfikacji zaprojektowanej metody. Po drugie, w rozdziale tym szczegółowo opisano zaprojektowaną metodę uwierzytelniania. Rozdział 5 zawiera opis eksperymentów zapewniających weryfikację, przeprowadzoną na wielu zbiorach danych oraz walidację metody w scenariuszach aplikacji finansowych. Wreszcie, szósty i zarazem ostatni rozdział, jest podsumowaniem pracy i przeglądem osiągniętych wyników badawczych wraz z opisaniem wkładu pracy i kierunkami dalszych prac możliwych w tematyce rozprawy.

Analiza literatury dla metod biometrii behawioralnej

Biometria behawioralna obejmuje unikalne lub dostatecznie rozróżnialne cechy, które można zmierzyć i przypisać osobie w celu identyfikacji i potwierdzenia jej tożsamości - uwierzytelniania (Saeed, 2012). Wykorzystuje ona różne metody wyodrębniania, kwantyfikacji i porównywania wyekstrahowanych cech użytkownika do wzorca (uwierzytelniania). Korzysta przy tym z przymiotów wywodzących się z zachowania użytkownika. Kategoria metod behawioralnych może potencjalnie oferować szeroką gamę potencjalnych korzyści, które wyróżniają ją od tradycyjnych cech biometrycznych:

- **Ciągłe / bezwarunkowe uwierzytelnianie** (ang. continuous / implicit authentication) (Gascon i in., 2014; F. Li i in., 2014) - w przeciwieństwie do systemów uwierzytelniania z punktem wejścia (ang. *point-of-entry*)[1], ich behawioralny odpowiednik jest w stanie uwierzytelniać użytkowników w sposób ciągły na podstawie wzorców przechwyconych podczas ich interakcji z urządzeniem. Można je zbierać w sposób nienatrętny dla usługobiorcy.
- **Autoryzacja niebinarna** - związana z powyższą cechą. W trakcie interakcji z urządzeniem, metoda tworzy miarę podobieństwa pomiędzy zapisanym wzorcem zachowania a stanem bieżącym. Wykorzystując te informację, możliwe jest określenie różnych poziomów autoryzacji, w zależności od pewności co do tożsamości użytkownika (Crawford i Renaud, 2014).
- **Integracja uwierzytelniania wielowarstwowego i multimodalnego** (Bailey i in., 2014) - ze względu na ich zróżnicowany charakter, metody behawioralne można łatwo stworzyć z zestawu różnych cech behawioralnych (F. Li i in., 2014) bez utraty użyteczności, w postaci dodatkowych interakcji a także bez potrzeby instalacji dodatkowych sensorów.
- **Niezależność od dostawcy, wysokie wskaźniki penetracji** - metody behawioralne opierają się głównie na czujnikach zainstalowanych już na każdym smartfonie. Ich wysoki poziom spójności działania jest wymagany od interfejsów API systemu operacyjnego urządzeń, na przykład przy przetwarzaniu zdarzeń na ekranie dotykowym. Oznacza to, że opracowana metoda behawioralna mogłaby potencjalnie zostać zastosowana na wielu urządzeniach.

[1] Pojęcie to odnosi się do systemów, które przed umożliwieniem dostępu wymagają interakcji w procesie uwierzytelnienia (np. pobrania odcisku palca), a następnie na jego podstawie dokonują procesu autoryzacji o stałym, zwykle maksymalnym, poziomie uprawnień.

- **Unikanie dodatkowych kosztów** - nie ma potrzeby instalowania dodatkowych czujników (F. Li i in., 2014), dlatego metody te często oferują wysoką opłacalność. Może to jednak być nieoczywiste, jeśli metoda pociąga za sobą znaczne nakłady obliczeniowe. Sam proces zbierania danych może być w pełni zautomatyzowany i charakteryzować się niskim kosztem.
- **Wysoka użyteczność** metod (Buriro i in., 2016; Xu i in., 2014) - ze względu na swój nieinwazyjny charakter niektóre metody mogą działać w sposób ciągły, nie wymagając interakcji użytkownika ani monitowania o wprowadzenie danych uwierzytelniających. Oznacza to, że można oczekiwać od nich wysokiej użyteczności. Gromadzenie biometrycznych danych behawioralnych jest stosunkowo łatwe i nie ogranicza użyteczności procesu. W niektórych przypadkach użytkownik może nawet nie zdawać sobie sprawy, że zbierane są dane (Yampolskiy i Govindaraju, 2008).
- **Minimalizacja niebezpieczeństwa kradzieży wzorca** - wzorce zachowań są trudne do uchwycenia i zmierzenia, a czasami można je wyekstrahować tylko na podstawie długotrwałej obserwacji zachowania użytkownika. Korzystanie z jednej lub wielu metod często prowadzi do powstania zagregowanego wzorca, który nie jest przydatny dla atakującego, ponieważ w przypadku wycieku firma stosująca te metody może po prostu zmienić czynniki wykorzystywane w procesie tworzenia wzorca. Uchwycony wzorzec również zmienia się w czasie (Kayacik i in., 2014).
- **Odporność na próby podszycia się (ang. spoofing)** - fałszowanie wzorca zachowań jest stosunkowo trudne. O ile dla niektórych cech behawioralnych wystarczyć może obserwacja, w połączeniu z cechami swoistymi, takimi jak prędkość dotyku, przyspieszenie i specyfika urządzenia, bardzo trudno jest skutecznie naśladować wzorzec użytkownika. Może być on również przechowywany w niemal nieodwracalnej formie, takiej jak model uczenia maszynowego lub sieć neuronowa z dużą liczbą wag.

Omawiana kategoria metod obejmuje biometrię profilu dotyku - która przy użyciu czujników zainstalowanych w nowoczesnych telefonach komórkowych może wykorzystywać proces interakcji użytkownika z urządzeniem mobilnym (Bo i in., 2013) i klasyfikować wykonywane przez nich akcje (L. Li i in., 2013). Ten typ biometrii behawioralnej

został wybrany jako najbardziej odpowiadający wymaganiom dla metody uwierzytelniania w usługach sektora finansowego na urządzeniach mobilnych.

Większość badań w literaturze opiera swoje podejścia na pracach przeprowadzonych w 2013 r. (Frank i in., 2012) w ramach projektu „Touchalytics". Frank i in. zidentyfikowali tzw. akcje inicjujące (ang. „trigger actions"). Są one często wykonywanymi przez użytkowników zdarzeniami, rejestrowanymi podczas korzystania z ekranu dotykowego. Stanowią część bardziej złożonych gestów nawigacyjnych[2], dlatego uważa się je za pierwotne[3]. Wyodrębniając ponad 30 zmiennych dla każdego przesunięcia i pociągnięcia (2 rodzaje zidentyfikowanych akcji), autor dla 41 użytkowników testowych osiągnął EER na poziomie 0-4% (równy poziom błędu, punkt przecięcia gdzie współczynnik wyników fałszywie pozytywnych równy jest współczynnikowi wyników prawdziwie pozytywnych.) między sesjami. Poziom błędu uzyskany na zbiorze danych był niski, a możliwość zwiększenia dokładności klasyfikatora poprzez włączenie czujników inercyjnych, takich jak odczyty akcelerometru, zaproponowali Li i in. w 2013 (L. Li i in., 2013). Wyniki innych badań, które osiągnęły poniżej 1% EER omówili Serwadda i in. (Serwadda i in., 2013) na wielu zbiorach danych, ograniczeniem była jednak liczba zmiennych użytych w konstrukcji poszczególnych klasyfikatorów. Podsumowując, wyniki różnych badaczy w zakresie obserwowanej dokładności i wskaźników błędów metod wykorzystujących biometrię profilu dotyku ekranu urządzenia mobilnego różnią się w literaturze. Dzieje się tak pomimo faktu, iż autorzy wykorzystywali ten sam aspekt zachowania użytkownika (wzorce interakcji na ekranie dotykowym urz. mobilnego), te same gesty (przeciągnięcia i stuknięcia) i często identyfikowali podobne zmienne. Omówienie wyników osiągniętych przez badaczy wskazuje na znaczenie innych czynników wykorzystywanych w projektowaniu eksperymentu badawczego, takich jak: zastosowany interfejs użytkownika aplikacji, długość procesu uczenia się, czas potrzebny na klasyfikację oraz metodologia weryfikacji wyników. Niektóre elementy, takie jak porównanie ważności (w rozumieniu ang. feature importance) zmiennych w różnych zestawach danych lub pokazanie wzrostu wydajności przy wykorzystaniu czujników bezwładnościowych nie były omawiane w literaturze. Mogą się okazać bardzo ważne, w celu wykorzystania wymienionych klasyfikatorów w rzeczywistych scenariuszach.

[2]Do gestów nawigacyjnych zaliczamy m.in. przesunięcia, kliknięcia, a także przybliżanie elementów na ekranie dotykowym.

[3]W rozumieniu tego, że są to zdarzenia o niskim poziomie skomplikowania, które pozwalają budować bardziej skomplikowane interakcje tj. powiększanie czy obracanie obiektów.

Aby scharakteryzować zmienne, jakie zostały użyte przez cytowanych badaczy i określenie czy mogą one wyjaśnić różnice w uzyskanych wynikach wykonano przegląd literatury, przeprowadzono ponowną analizę i integrację wyników badań przeglądowych (Abdulhak i Abdulaziz, 2018; Patel i in., 2016; Serwadda i in., 2013). Uzupełniono je o nowe wyniki opublikowane po 2016r. uwzględniając wielkości zbiorów danych, liczbę próbek użytą w procesie uczenia i klasyfikacji, publiczną dostępność badanych zbiorów danych i różnorodność wykorzystanych badaniach urządzeń. Charakterystyki metodologicznie poprawnych podejść z niskimi poziomami błędów przedstawiono w tabeli 2, wraz z wykorzystywanymi przez nich miarami np. prędkości, dystansu czy odczytów żyroskopu. Jedną z najbardziej istotnych różnic między podejściami, jest liczba próbek użytych w procesie klasyfikacji. Podczas gdy niektórzy badacze mierzyli poziom błędu, po kilku akcjach, niektórzy z nich mierzyli błąd na poziomie sesji lub aż 70 akcji. Ten fakt, wraz z różnymi projektami aplikacji testowych (ponieważ używano różnych zestawów danych), może wyjaśniać duże różnice w uzyskanych wynikach. Kolejną przeszkodą jest rozmiar danych uczących pod względem liczby próbek i użytkowników. Na przykład w badaniu Li i in.(L. Li i in., 2013) 75 użytkowników było dostępnych w zbiorze danych, ale uczenie modelu dotyczyło tylko 28 z nich. Reszta została wykorzystana tylko jako przykłady oszustw w procesie testowania klasyfikatora.

Mając na uwadze, że różnice w uzyskanych wynikach mogą być spowodowane czasem uczenia i klasyfikacji oraz wielkością zbioru danych, konieczne było porównanie działania metody dla różnych zbiorów, aby potwierdzić, że może ona stabilnie osiągać poniżej 1 % EER. Osiągnięcie stabilnych wyników mogłoby również wskazywać, że wyekstrahowane dane biometryczne pochodzące z ekranu dotykowego mają charakter uniwersalnego klasyfikatora biometrycznego, a metodę można uznać za mającą uniwersalny charakter, opierając się na unikalności kombinacji opisujących profil dotyku w różnych środowiskach badania. Mniej ważne w naszym przypadku jest udowodnienie, czy potrafimy rozróżniać użytkowników niezależnie od samego zadania. Celem jest uwierzytelnienie z wykorzystaniem konkretnych akcji (akcji przesunięć i pociągnięć) wykonanych przez użytkownika w aplikacji. Jeśli te wyniki można osiągnąć w wielu zestawach danych przy użyciu pierwotnych zdarzeń, takich jak przewijanie to będą one mogły mieć zastosowanie do większości projektów aplikacji, określając uniwersalny charakter metody.

Podsumowując, badanie literaturowe wykazało, że istnieją znaczne różnice w uzyskiwanych wynikach dokładności działania i nie można udzielić jasnej odpowiedzi precyzującej próg poziomu błędu metod uwierzytelniania behawioralnego za pomocą profilu dotyku. W związku z tym w badaniu zaproponowano projekt eksperymentu, który mógłby udowodnić ich skuteczność i przydatność w scenariuszu uwierzytelniania finansowego. Uniwersalny charakter tego podejścia zostanie zewaluowany, poprzez wykorzystanie wielu zbiorów danych zebranych w różnych eksperymentach na różnych urządzeniach.

Weryfikacja metody

W przeprowadzonych badaniach autor zaproponował metodę uczenia maszynowego, korzystając z walidacji krzyżowej (ang. cross-validation). Objął 5 zbiorów danych, wykorzystując klasyfikator binarny do uwierzytelniania użytkownika i oceny ryzyka akcji wykonywanych przez niego w aplikacji finansowej. Opracowano różne klasyfikatory i wartości hiperparametrów, wykorzystując metodę wyszukiwania w siatce macierzy (ang. grid search) z 5-krotną walidacją krzyżową. Klasyfikator XGboost zapewnił najlepszą dokładność i najniższe wskaźniki błędów. Podobnie, aby zapewnić wystarczającą dokładność w perspektywie uwierzytelniania i możliwości wykrywania oszustw, wykorzystano różną liczbę interakcji do klasyfikacji, gdzie dokładność metody była testowana po 1, 3, 5 i 7 akcjach użytkownika. Listy ważności cech dla różnych zbiorów danych porównano na podstawie wartości całkowitego zysku informacyjnego (gain) wyliczonego dla przykładów. Pozwoliło to na wskazanie, które cechy najlepiej charakteryzują zachowanie użytkowników podczas interakcji z ekranem dotykowym urządzenia mobilnego i które można uznać za znaczące. To częściowo pozwoliło na udzielenie odpowiedzi na pytanie „co sprawia, że wzór profilu dotyku użytkownika jest wyjątkowy?”.

We wstępnych eksperymentach problem uwierzytelniania został przedstawiony jako problem klasyfikacji z wieloma klasami reprezentującymi użytkowników. Posłużył on do porównania metody z wynikami osiągniętymi przez literaturę. Następnie został przekształcony w problem klasyfikatora binarnego. Jest to zamierzone podejście w kwestii walidacji procesu uwierzytelniania, a uzyskane wyniki okazały się lepsze od zakładanych w pracy kryteriów. Metoda zapewniła poniżej 1 % EER dla 3 przewinięć (ang. swipe) i poniżej 0,1% EER dla klasyfikacji 5 przewinięć.

Tabela 2. Charakterystyka, opis wykorzystywanych miar i wyniki metod uwierzytelniania mobilnego wykorzystujących biometrię profilu dotyku urządzeń mobilnych w literaturze.

	Pozycyjne	Dystansu	Czasowe	Obszaru	Nacisku	Prędkości	Przyspieszenia	Kierunku	Orientacji palca	Orientacji telefonu	Zdarzenia z wieloma pkt. dotyku	Akcelerometr	Żyroskop	Liczba uż.	Liczba sesji dla uż.	L. telef.	Dostępność zbioru	EER
(Saevanee i Bhattarakosol, 2009)	-	-	-	✓	-	✓	-	-	-	-	-	-		10	30	1	-	1% EER dla sesji
(Damopoulos i in., 2013)	✓	-	✓	-	-	-	-	-	-	-	-	-	-	18	1 (24h)	18	-	0.205% EER dla 24h sesji
(Frank i in., 2012)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	-	-	41	7	4	✓	2-4% EER dla 11 akcji
(L. Li i in., 2013)	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	-	✓	✓	28	600 akcji	2	-	3% EER dla 14/20 akcji
(Serwadda i in., 2013)	✓	✓	✓	-	-	-	-	-	-	✓	-	✓	✓	138	80 akcji	1	✓	10% EER dla 10 akcji
(Zhang i in., 2015)	✓	✓	✓	✓	-	✓	✓	✓	-	✓	-	-	-	50	3	9	✓	1% EER dla 70 akcji
(Meng i in., 2012)	✓	-	✓	-	-	✓	-	✓	-	-	✓	-	-	20	6	1	-	3% EER dla 10 min. sesji
(Jain i Kanhangad, 2015)	✓	✓	✓	✓	-	-	-	✓	✓	-	✓	✓	✓	104	3 próbki	1	-	0.31% EER dla sesji
(Samet i in., 2019)	✓	✓	✓	✓	✓	✓	-	-	✓	✓	-	-	-	15	dla 7 akcji 7	1	-	3% EER dla sesji

Źródło: tłumaczenie na podstawie (Kałużny, 2019)

Wykorzystując dane wyjściowe, utworzono miarę ryzyka, który odpowiada prawdopodobieństwom wykonania transakcji przez nieuprawnionego użytkownika, generowanym przez bazowy model uczenia maszynowego w metodzie. Wykorzystując SHAP (SHapley Additive exPlanations) (Lundberg i Lee, 2017) udało się opisać, na podstawie których zmiennych dana metoda podjęła decyzję, w celu uzyskania wysokiej wyjaśnialności modelu.

Tabela 3. Porównanie średniej dokładności metody i średnich makro w scenariuszu uwierzytelniania ze współczynnikiem danych oszusta 1 : 1.

Zbiór danych / Charakterystyka	Touchalytics	Sapienta BioIdent	Serwadda	Own Dataset
Dokładność	93,52%	94,34%	94,25%	91,26%
Precyzja	94,96%	96,06%	97,13%	95,30%
Czułość	91,89%	92,51%	91,21%	86,33%
F-Score	93,37%	94,14%	94,03%	90,15%
EER	6,52%	5,94%	5,71%	7,66%
N=3 Dokładność	98,36%	98,78%	98,61%	97,43%
N=3 Precyzja	98,89%	99,06%	99,03%	98,61%
N=3 Czułość	98,85%	99,00%	98,99%	98,23%
N=3 F-score	98,85%	99,00%	98,99%	98,26%
N=3 EER	0,89%	0,72%	0,48%	<0,01%
N=5 Dokładność	99,62%	99,67%	99,56%	99,14%
N=5 Precyzja	99,74%	99,72%	99,76%	99,54%
N=5 Czułość	99,74%	99,69%	99,76%	99,38%
N=5 F-score	99,74%	99,69%	99,76%	99,37%
N=5 EER	0,06%	0,03%	0,02%	<0,01%

Źródło: opracowanie własne

Szczegółowe wyniki przedstawiono w tabeli 3, gdzie parametr N odpowiada liczbie czynności użytych do oceny klasyfikatora.

Przeprowadzono również eksperymenty dotyczące rozpoznawania wieku i płci z wykorzystaniem danych dotyczących profilu dotyku urządzenia mobilnego. Wyniki klasyfikatora XGBoost uzyskały dokładność 71,51% dla próbki z zestawu danych BrainRun (5. zbiór danych) i 88,54% dla zbioru danych własnych w scenariuszu zaklasyfikowania do jednej z następujących klas wiekowych: 11- 20, 21-30, 31-40, 41-50, 51-60, 60+. To samo podejście zastosowano do rozpoznawania płci, bez uwzględniania infor-

macji o wieku. Dało to dokładność 82,88% dla pierwszego zbioru, a w odniesieniu do 88 użytkowników w zbiorze danych własnych - 92,84%. Wynikowy poziom precyzji, osiągnięty dla rozpoznawania płci uzyskany na podstawie własnego zbioru, z wykorzystaniem danych z akcelerometru, był podobny do uzyskanego w badaniach z 2019r. (Jain i Kanhangad, 2019).

W dalszej części rozdziału 4, zaproponowano scenariusze walidacji metody potwierdzające wykonalność wdrożenia w środowisku mobilnych aplikacji finansowych. Przedstawiono diagramy obrazujące przebieg procesu komunikacji z systemem wykrywania oszustw, wyróżniając dwa projekty architektury rozwiązana. Zaprezentowano zalety i wady obu architektur, prezentując podejścia przetwarzania brzegowego (ang. „edge computing") i centralnego. W pierwszym przypadku zaproponowano model i format danych pozwalający na ochronę prywatności danych użytkownika. Umożliwia on wdrożenie metody przy niewielkim ryzyku ujawnienia danych użytkownika. W drugim natomiast opisano scenariusz centralnego przetwarzania, sklasyfikowany jako stwarzający niski, choć wyższy niż w poprzednim przypadku, poziom zagrożenia dla poufności danych ze względu na przetwarzanie tylko danych dotyczących interakcji z ekranem dotykowym. Zanalizowano ogólną możliwość implementacji metody w mobilnej aplikacji finansowej, przedstawiając scenariusze w których klasyfikator będzie trenowany i oceniany na próbkach zapewniając uwierzytelnianie ciągłe i adaptacyjną autoryzację.

Wyniki przeprowadzonych badań

Proponowana metoda może być przydatna dla sektora finansowego. Na podstawie przeprowadzonych eksperymentów, autor potwierdził, że metoda ta może osiągnąć niski poziom błędu, porównywalny lub lepszy niż obecnie stosowane metody rozpoznawania twarzy dla urządzeń mobilnych. Zaprojektowane podejście może być więc stosowane jako ich alternatywa. Może być wykorzystana jako czynnik wrodzony (ang. inherence factor) w procesach uwierzytelniania zgodnych z PSD 2. Według modelu wymagań dla metody określonej w rozdziale 2 rozprawy, spełniła ona wszystkie kryteria wyspecyfikowanie dla jej wykorzystania w środowisku usług finansowych:

- Bezpieczeństwo [A1] - poziomy błędów osiągnięte przez metodę okazały się mniejsze niż 0,08 % EER, zgodnie z wynikami scenariusza uwierzytelniania z tabeli 3, przy założeniu 5 akcji użytkownika. Można wykorzystać ją do zapobiegania

kradzieżom urządzenia, nieautoryzowanym przez użytkownika transakcjom oraz złośliwemu oprogramowaniu udającemu właściciela urządzenia.

- Użyteczność [C1] - udowodniono, że metoda zwiększa użyteczność w $>$ 99,9% przypadków uwzględniając osiągnięty poziom EER przy założeniu wykorzystania funkcji wymagających 5 akcji przed potwierdzeniem transakcji w aplikacji mobilnej. Możliwość poprawy użyteczności można również uzyskać już od pierwszej akcji, stosując uwierzytelnianie ciągłe i zaproponowany model autoryzacji.
- Prywatność [A2] - na podstawie analizy zmiennych wykorzystanych w metodzie, żadne poufne informacje nie są wykorzystywane w procesie uwierzytelniania. Korzystając z możliwości scenariusza przetwarzania brzegowego, ryzyko ujawnienia wzorca użytkownika byłoby minimalne. Nawet w alternatywnym scenariuszu centralnego przetwarzania, jedyną możliwą do ujawnienia rzeczą byłyby informacje dot. dotyku i oszacowania prawdopodobieństwa metody z wagą zmiennych - które mogą się zmieniać wraz z samym urządzeniem i być szyfrowane w infrastrukturze dostawcy. To z kolei ogranicza problemy z odwołalnością (ang. revocability) wzorca.
- Wymogi prawne [B3] - opracowana metoda może zostać sklasyfikowana jako czynnik wrodzony uwierzytelniania biometrycznego, zgodnie z zaprezentowanymi badaniami literatury, z zakresu bankowości i metod autoryzacji. W kwestii wymagań dla procedur uwierzytelniania (EBA, 2019), Europejski Urząd Nadzoru Bankowego również uznaje biometrię behawioralną za akceptowalny czynnik dla PSD 2. Oznacza to, że metoda jest może zostać wykorzystana w środowisku finansowym i spełnia wymagania czynnika silnego uwierzytelniania (ang. strong customer authentication SCA) dyrektywy PSD 2. Można ją również bezpiecznie stosować, w celu przypisywania ryzyka do pojedynczych transakcji.
- Wykrywanie oszustw [B1] - umożliwienie określenia ryzyka dla pojedynczych transakcji, dzięki oszacowaniu niepewności co do tożsamości użytkownika podczas korzystania z aplikacji. Wyjaśnienie decyzji podjętej przez metodę jest możliwe dzięki zastosowaniu SHAP, co pozwala na spełnienie wymogu rozliczalności i oceny ryzyka względem RODO. Scenariusze, w których można by zastosować koncepcję, przedstawiono w rozprawie. W metodzie przeanalizowano również możliwości wykorzystania mechanizmów uwierzytelniania przed zagrożeniami typu

„authentication insider threat”[4] oraz zapewnienia „Proof of Presence” - dowodu, że to użytkownik fizycznie autoryzuje transakcję.

- Interoperacyjność [P1] - działanie pozwala na przekazywanie do infrastruktury bankowej szacunków poziomu ryzyka, wraz z możliwymi do wyjaśnienia rezultatami decyzji metody dla klientów i podmiotów z sektora FinTech. Przy niewielkim ryzyku ujawnienia prywatnych informacji, firmy z tego sektora mogłyby wykorzystać tę metodę do komunikacji z infrastrukturą bankową w scenariuszu oceny ryzyka transakcji. Koncepcja wykorzystuje hardware (ekran dotykowy) i software (API mobilnego systemu operacyjnego) dostępne na praktycznie każdym smartfonie. Pozwala to na łatwą implementację.
- Efektywność kosztowa i niezależność od platformy [B2] - metoda nie wymaga instalacji dodatkowych czujników i wykorzystuje najbardziej podstawowe interfejsy API mobilnych systemów operacyjnych. Oznacza to, że można ją wykorzystać na prawie każdym urządzeniu obsługującym ekran dotykowy. Eksperymenty przedstawione w pracy obejmowały wiele różnych modeli telefonów od roku 2011 do 2020 i wykazały bardzo podobne wyniki miar błędów.

Metoda, zgodnie z tezą pracy, powinna umożliwić integracje z aplikacją mobilną i zapewnić osiągnięcie poziomu błędów niższego, niż obecnie stosowane metody wykrywania twarzy na urządzeniach mobilnych, zapewniając przy tym wyższą użyteczność. Zaprezentowane w dysertacji wyniki dowiodły spełnienia powyższej tezy poprzez spełnienie celów badawczych i odpowiedź na postawione pytania. Podsumowując, przeprowadzone badania potwierdziły, że metoda wykorzystująca biometrię profilu dotyku ekranu urządzenia mobilnego spełnia kryterium dokładności i umożliwia ocenę ryzyka na poziomie transakcyjnym. Przedstawiono wykonalność potencjalnej implementacji oraz scenariusze wdrożenia wraz z prezentacją niefunkcjonalnych kryteriów wymagań. Zastosowanie proponowanej metody zostało zwalidowane za pomocą propozycji architektury i interfejsu własnej aplikacji bankowej. Ocena skuteczności została natomiast potwierdzona z wykorzystaniem wielu zbiorów danych. Metoda pozwoliła na spełnienie założeń tezy, że: *możliwe jest zaprojektowanie metody uwierzytelniania wykorzystującej biometrię behawioralną, która wdrożona w mobilnej aplikacji finansowej osiągnie poziom*

[4]Mamy tutaj na myśli sytuacje, gdy osoba znająca posiadacza urządzenia, wykorzystując często znajomość standardowych czynników uwierzytelniania tj. hasło, dokonuje nieuprawnionego dostępu.

błędów niższy niż obecnie stosowane metody wykrywania twarzy na urządzeniach mobilnych, zapewniając przy tym wyższą użyteczność.

Przeprowadzone badania miały charakter interdyscyplinarny, wykorzystując metody uczenia maszynowego i behawioralnego uwierzytelniania biometrycznego w środowisku finansowym. Skoncentrowano się na różnych subdyscyplinach ekonomii sklasyfikowanych przez Journal of Economic Literature (JEL): G2 - instytucje i usługi finansowe, D81 - kryteria podejmowania decyzji w warunkach ryzyka i niepewności, C8 - metodologia zbierania i szacowania danych, programy komputerowe.

Bibliografia

Abdulhak, S. A. & Abdulaziz, A. A. (2018). A systematic review of features identification and extraction for behavioral biometrie authentication in touchscreen mobile devices. *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 68–73.

Bailey, K. O., Okolica, J. S. & Peterson, G. L. (2014). User identification and authentication using multi-modal behavioral biometrics. *Computers & Security*, *43*, 77–89.

Bo, C., Zhang, L., Li, X.-Y., Huang, Q. & Wang, Y. (2013). Silentsense: silent user identification via touch and movement behavioral biometrics. *Proceedings of the 19th annual international conference on Mobile computing & networking*, 187–190.

Bonneau, J. & Preibusch, S. (2010). The Password Thicket: Technical and Market Failures in Human Authentication on the Web. *WEIS*.

Buriro, A., Crispo, B., Del Frari, F., Klardie, J. & Wrona, K. (2016). ITSME: Multi-modal and Unobtrusive Behavioural User Authentication for Smartphones. *Technology and Practice of Passwords*, 45.

Crawford, H. & Renaud, K. (2014). Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management*, *1*(1), 7.

Damopoulos, D., Kambourakis, G. & Gritzalis, S. (2013). From keyloggers to touchloggers: Take the rough with the smooth. *Computers & security*, *32*, 102–114.

Deloitte Center for Financial Services. (2018). *2018 Banking Outlook* [Online; Accessed 10.10.2019]. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-dcfs-2018-banking-outlook.pdf

EBA, E. B. A. (2019). *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* [Online; Accessed 10.10.2019]. https://

ec.europa.eu/info/publications/190621-eba-opinion-strong-customer-authentication_en

European Central Bank. (2019). *European Central Bank, 2018. Fifth report on card fraud*. https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202008~521edb602b.en.html

Europen Comission. (2015). *PSD 2, Directive (EU) 2015/2366*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366

Frank, M., Biedert, R., Ma, E., Martinovic, I. & Song, D. (2012). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security*, *8*(1), 136–148.

Fridman, L., Weber, S., Greenstadt, R. & Kam, M. (2017). Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal*, *11*(2), 513–521.

Gascon, H., Uellenbeck, S., Wolf, C. & Rieck, K. (2014). Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior. *Sicherheit*, 1–12.

Hayashi, E., Riva, O., Strauss, K., Brush, A. & Schechter, S. (2012). Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2.

Hevner, A. R., March, S. T., Park, J. & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Imgraben, J., Engelbrecht, A. & Choo, K.-K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, *33*(12), 1347–1360.

Jain, A. & Kanhangad, V. (2015). Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touchscreen gestures. *Pattern recognition letters*, *68*, 351–360.

Jain, A. & Kanhangad, V. (2019). Gender recognition in smartphones using touchscreen gestures. *Pattern Recognition Letters*, *125*, 604–611.

Kałużny, P. (2019). Touchscreen behavioural biometrics authentication in self-contained mobile applications design. W W. Abramowicz i A. Paschke (Red.), *International Conference on Business Information Systems* (s. 672–685).

Kayacik, H. G., Just, M., Baillie, L., Aspinall, D. & Micallef, N. (2014). Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors. *arXiv preprint arXiv 1410 7743*.

Li, F., Clarke, N., Papadaki, M. & Dowland, P. (2014). Active authentication for mobile devices utilising behaviour profiling. *International journal of information security*, *13*(3), 229–244.

Li, L., Zhao, X. & Xue, G. (2013). Unobservable re-authentication for smartphones. *NDSS*, 1–16.

Lundberg, S. M. & Lee, S.-I. (2017). A Unified Approach to Interpreting Model Predictions. W I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan i R. Garnett (Red.), *Advances in Neural Information Processing Systems 30* (s. 4765–4774). Curran Associates, Inc.

Meng, Y., Wong, D. S., Schlegel, R. i in. (2012). Touch gestures based biometric authentication scheme for touchscreen mobile phones. *International Conference on Information Security and Cryptology*, 331–350.

Meola, A. (2019). *The digital trends disrupting the banking industry in 2019*. https://www.businessinsider.com/banking-industry-trends?IR=T

Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J. & Beznosov, K. (2013). Know your enemy: the risk of unauthorized access in smartphones by insiders. *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, 271–280.

Patel, V. M., Chellappa, R., Chandra, D. & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, *33*(4), 49–61.

Prat, N., Comyn-Wattiau, I. & Akoka, J. (2014). Artifact Evaluation in Information Systems Design-Science Research-a Holistic View. *PACIS*, 23.

Saeed, K. (2012). Biometrics principles and important concerns. *Biometrics and Kansei Engineering* (s. 3–20). Springer.

Saevanee, H. & Bhattarakosol, P. (2009). Authenticating user using keystroke dynamics and finger pressure. *2009 6th IEEE Consumer Communications and Networking Conference*, 1–2.

Samet, S., Ishraque, M. T., Ghadamyari, M., Kakadiya, K., Mistry, Y. & Nakkabi, Y. (2019). TouchMetric: a machine learning based continuous authentication feature testing mobile application. *International Journal of Information Technology*, 1–7.

Serwadda, A., Phoha, V. V. & Wang, Z. (2013). Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms. *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*, 1–8.

Srinivas, V., Fromhart, S., Goradia, U. & Richa, W. (2018). *Banking Outlook Ąccelerating the transformation*" [Online; Accessed 07.12.2018]. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-dcfs-2018-banking-outlook.pdf

The Business Research Company. (2019). *Financial Services Global Market Report*. https://www.thebusinessresearchcompany.com/report/financial-services-global-market-report

Visa. (2017). *Visa - Annual Digital Payments Study 2017* [Online; Accessed 07.12.2018]. https://www.visaeurope.com/newsroom/news/mobile-money-takes-off-as-77-of-europeans-use-their-phones-to-bank-and-make-everyday-payments

Xu, H., Zhou, Y. & Lyu, M. R. (2014). Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones. *Symposium On Usable Privacy and Security, SOUPS*, *14*, 187–198.

Yampolskiy, R. V. & Govindaraju, V. (2008). Behavioural biometrics: a survey and classification. *International Journal of Biometrics*, *1*(1), 81–113.

Zhang, H., Patel, V. M., Fathy, M. & Chellappa, R. (2015). Touch gesture-based active user authentication using dictionaries. *2015 IEEE Winter Conference on Applications of Computer Vision*, 207–214.