Uniwersytet Śląski
Wydział Nauk Ścisłych i Technicznych
Instytut Informatyki

Autoreferat rozprawy doktorskiej

mgr inż. Tomasz Wesołowski

Biometryczna weryfikacja użytkownika systemu komputerowego z automatyczną aktualizacją profilu aktywności

Promotor:
prof. dr hab. Piotr Porwik

Promotor pomocniczy:
dr hab. inż. Rafał Doroz, prof. UŚ

Sosnowiec, 2023

1 Wstęp

Wykorzystywanie komputerów i urządzeń przenośnych zwiększa ryzyko nieuprawnionego dostępu do procesów lub wrażliwych danych. Z najnowszych raportów wynika, że częstotliwość ataków związanych z cyberprzestępczością stale wzrasta [5]. Szkody finansowe powodowane cyberprzestępczością przekraczają już skalę tradycyjnej przestępczości. Popularne metody uwierzytelniania i weryfikacji, oparte na hasłach lub tokenach, są zazwyczaj przełamywane – są więc niewystarczające.

Alternatywnym rozwiązaniem jest wykorzystanie specjalistycznych technik biometrycznych, gdzie fałszerstwo indywidualnych cech biometrycznych nie jest niemożliwe, ale jest trudniejsze niż w przypadku metod opartych na systemach łamania haseł (np. rainbow tables). W automatycznym rozpoznawaniu osób na podstawie cech biometrycznych wykorzystuje się analizę cech behawioralnych [20], cech fizycznych [6] lub stosuje się hybrydę tych metod [14]. Metody biometrii behawioralnej wykorzystują dane pochodzące z manipulatorów takich jak myszka komputerowa [16], czy klawiatura [2, 19]. Taka analiza sprowadza się do wykrywania zależności czasowych związanych z obserwacją charakterystycznych, indywidualnych cech użytkownika w trakcie użytkowania klawiatury komputera [28]. Wyznaczone cechy pozwalają na zbudowanie profilu użytkownika, który może być stosowany do weryfikacji uprawnień w systemach autoryzacji dostępu i w systemach wykrywania intruzów IDS (*ang.* Intrusion Detection System).

Weryfikacja ciągła

Proste mechanizmy kontroli dostępu wykorzystujące hasła są powszechnie stosowanym środkiem ochrony przed nieautoryzowanym dostępem. Ten typ kontroli jest zwykle implementowany jako jednorazowe potwierdzenie tożsamości w trakcie wstępnej procedury logowania do systemu komputerowego. Jest to tak zwane uwierzytelnianie statyczne (*ang.* Static Authentication – SA). Metody te można łatwo przełamać. Dlatego należy je zastępować (lub uzupełniać) bardziej wyrafinowaną analizą biometryczną. Zastosowanie metod biometrycznych w SA nie eliminuje wszystkich zagrożeń, gdyż urządzenie w trakcie pracy (już po uwierzytelnieniu uprawnionego użytkownika) może być przejęte przez osobę nieuprawnioną. Zastosowanie SA sprawia, że uprawnienia dostępu są weryfikowane przy rozpoczynaniu pracy i pozostają ważne w czasie sesji – czyli aż do momentu wylogowania. Jeżeli w czasie sesji urządzenie pozostanie bez nadzoru (i bez wylogowania), nieuprawniona osoba może przejąć kontrolę nad systemem bez wiedzy prawowitego użytkownika. Oznacza to, że system traci odporność na ataki intruza.

Podniesienie poziomu bezpieczeństwa systemu wymaga, aby moduł wykrywania włamań IDS nadzorował system przez cały czas. Moduł w sposób ciągły monitoruje aktywność użytkownika i prowadzi permanentną weryfikację tożsamości. Jest to tzw. weryfikacja ciągła CV (*ang.* Continuous Verification), gdzie autentyczność użytkownika jest weryfikowana na podstawie ustalonego wcześniej rzeczywistego, niezakłóconego profilu użytkownika uprawnionego. Po wykryciu nieprawidłowości zachowań użytkownika, system stosujący mechanizm CV generuje

alert i blokuje dostęp do zasobów, żądając równocześnie ponownej autoryzacji statycznej SA.

Zaproponowany algorytm biometryczny pozwala tworzyć w sposób ciągły behawioralne profile użytkowników. Algorytm pozwala na weryfikację użytkowników z zastosowaniem klasyfikatorów wspieranych kompetencjami i progami decyzyjnymi z automatycznym tworzeniem i aktualizacją profilu behawioralnego. Ta strategia umożliwia również automatyczne wykrywanie intruzów (nieuprawnionych użytkowników) systemów komputerowych. Jest to równoznaczne z ciągłym porównywaniem bieżącej aktywności użytkownika z wcześniej opracowanym profilem uprawnionego użytkownika. Proponowane rozwiązanie pozwala na zastąpienie nieefektywnego modelu jednorazowej weryfikacji SV, nowym, lepszym modelem weryfikacji wykorzystującym CV.

1.1 Teza pracy

Możliwa jest poprawa skuteczności weryfikacji użytkowników systemu komputerowego poprzez wprowadzenie weryfikacji ciągłej wykorzystującej biometryczny profil aktywności bazujący na obserwacji dynamiki użytkowania klawiatury oraz strategii automatycznej aktualizacja profilu aktywowanej progami decyzyjnymi.

1.2 Cele pracy

Głównym celem jest opracowanie autorskiego algorytmu tworzenia biometrycznego profilu użytkownika oraz nowatorskiej metody ciągłej weryfikacji użytkowników opartej na klasyfikatorach, pozwalającej na automatyczną aktualizację profilu behawioralnego. Zadaniem autorskiego algorytmu będzie wyznaczenie biometrycznego profilu uprawnionego użytkownika na podstawie analizy dynamiki pisania na klawiaturze. Profil będzie wykorzystywany do weryfikacji użytkownika na podstawie jego bieżącej aktywności, powinien on umożliwiać weryfikację użytkowników w sposób ciągły. Opracowane algorytmy zostaną porównane z innymi technikami weryfikacji bazującymi na analizie dynamiki pisania na klawiaturze.

Kolejne etapy realizacji głównego celu pracy obejmują następujące cele szczegółowe:

1. **Akwizycja danych biometrycznych.** Ciągła rejestracja behawioralnej aktywności użytkowników systemów komputerowych z ciągłym zapisywaniem zdarzeń klawiatury. Aplikacja rejestrująca aktywność może również rejestrować dodatkowe informacje, przykładowo zdarzenia myszki komputerowej do przyszłego wykorzystania w metodach hybrydowych.

2. **Opracowanie bazy danych do testów.** Biorąc pod uwagę niewielką dostępność referencyjnych baz danych, konieczne jest opracowanie zbioru danych pozwalających na wiarygodne testowanie zaproponowanych rozwiązań. Baza danych będzie zawierać dane rzeczywistej aktywności użytkowników w naturalnym środowisku pracy.

3. **Opracowanie algorytmu biometrycznego profilowania użytkowników, wykorzystującego zdarzenia związane z użytkowaniem klawiatury.** W celu weryfikacji ciągłej konieczna jest ciągła rejestracja danych i określenie na ich podstawie profilu uprawnionego użytkownika, co pozwala na modyfikację profilu w przypadku zmian wzorca zachowań prawowitego użytkownika.

4. **Opracowanie metody weryfikacji użytkowników na podstawie biometrycznego profilu aktywności.** Dysponując profilem aktywności użytkownika można przeprowadzić weryfikację aktywnego użytkownika systemu, stosując wybrane klasyfikatory.

5. **Testowanie opracowanych metod na danych rzeczywistych.** Systemy weryfikacji są projektowane w celu konkretnego zastosowania. Aby potwierdzić przydatność zaproponowanego rozwiązania do zastosowania w systemach wykrywania włamań IDS konieczne jest przeprowadzenie testów z wykorzystaniem rzeczywistych danych.

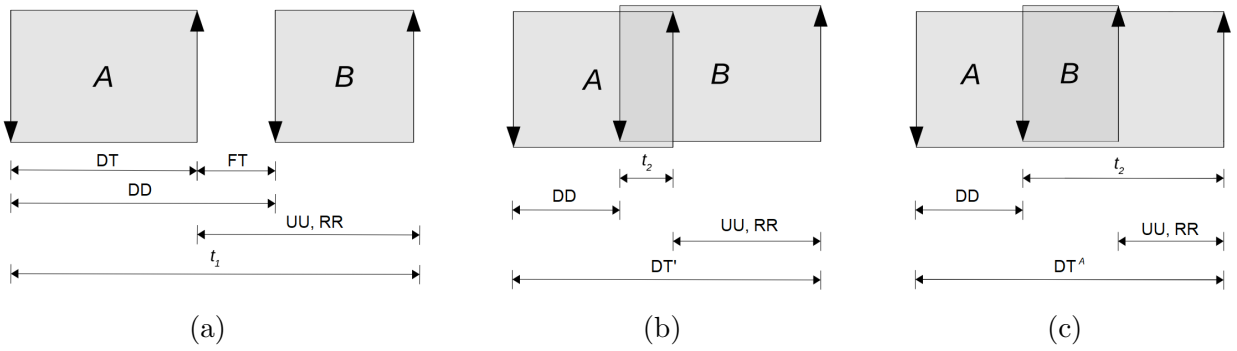
2 Analiza dynamiki pisania na klawiaturze

Aktywność użytkownika systemu komputerowego może być analizowana poprzez obserwację dynamiki pisania na klawiaturze KDA (*ang.* Keystroke Dynamics Analysis). W pomiarach rejestrowane są zależności czasowe występujące podczas używania klawiszy klawiatury. Są to tzw. interwały czasowe (*ang.* time intervals). Z zależności czasowych można wydobyć cechy, które mogą być wykorzystywane w biometrii behawioralnej [9]. Jedna z pierwszych prac wykorzystujących analizę interwałów czasowych do uwierzytelniania użytkownika systemu komputerowego opublikowana została w 1980 roku. Wyniki badań w tym obszarze były również publikowane w wielu pracach, gdzie charakterystyki czasowe zostały potwierdzone poprzez badania empiryczne jako cechy biometryczne [4].

2.1 Zależności czasowe jako cechy w KDA

Biometryczne modelowanie zachowania użytkowników wymaga zdefiniowania typów interwałów czasowych, które mogą być traktowane jako cechy. Wpisywane przy pomocy klawiatury znaki identyfikowane są na podstawie przypisanych, unikalnych kodów *ASCII* lub obecnie częściej wykorzystywanego standardu *Unicode*. Standardowa klawiatura posiada mniej przycisków niż liczba dostępnych kodów znaków, tak więc inne znaki uzyskuje się używając odpowiedniej kombinacji klawiszy. W praktyce do identyfikacji przycisków klawiatury wykorzystywane są jednak tak zwane *wirtualne kody klawiszy* VK (*ang.* Virtual Key codes), przypisane odpowiednim klawiszom klawiatury. Na potrzeby badań klawisz j, niezależnie od systemu kodowania, będzie oznaczany symbolem ω_j.

Ze względu na różnice w nazewnictwie występujące w literaturze należy usystematyzować terminologię. Pojedyncza akcja związana z wykorzystaniem dowolnego przycisku klawiatury wymaga wystąpienia dwóch zdarzeń: **wciśnięcia przycisku** (*ang.* key down) oraz **zwolnienia (puszczenia) przycisku** (*ang.* key up). Na tej podstawie wyznacza się sekwencje zdarzeń i interwały czasowe przedstawione poglądowo na Rys. 1, gdzie strzałka w dół oznacza wciśnięcie, a strzałka w górę zwolnienie klawisza.



(a) (b) (c)

Rys. 1: Zależności czasowe zdarzeń klawiatury dla: (a) niezależnie użytych przycisków A i B, (b) i (c) pary przycisków A i B użytych jednocześnie

Poprawne sekwencje zdarzeń zawsze powinny występować parami – dla każdego użytego klawisza pojawia się zgłoszenie zdarzenia wciśnięcia oraz jedno zgłoszenie zwolnienia przycisku klawiatury. Systemy operacyjne mogą generować także dodatkowe zdarzenia. Dodatkowo, w wyjątkowych sytuacjach może się zdarzyć, że w danych wejściowych będzie brakować pewnych informacji. Takie niepełne dane są odrzucane na etapie wstępnego przetwarzania danych wejściowych.

Na podstawie interwałów czasowych określonych dla przypadków użycia pojedynczych klawiszy (Rys. 1a) oraz par klawiszy (Rys. 1b i 1c) definiowane są między innymi następujące (najczęściej stosowane) zależności czasowe wykorzystywane jako cechy biometryczne w KDA: **czas trzymania DT** (*ang.* dwell time) – różnica czasu między zdarzeniami wciśnięcia i zwolnienia tego samego klawisza; **czas lotu FT** (*ang.* flight time) – różnica czasu między zdarzeniem zwolnienia klawisza, a zdarzeniem wciśnięcia kolejnego, związana z czasem „lotu" palca nad klawiaturą; **czas wciśnięcie-wciśnięcie DD** (*ang.* down-down time, d-d time) – czas od wciśnięcia pierwszego klawisza do wciśnięcia kolejnego klawisza; **czas puszczenie-puszczenie UU** (*ang.* up-up time) – czas od zwolnienia pierwszego klawisza do zwolnienia kolejnego klawisza.

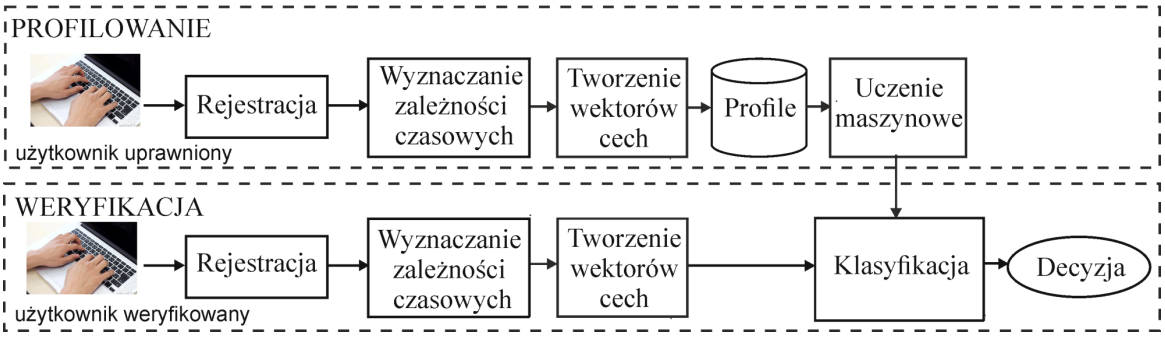
Metody profilowania użytkownika zaproponowane w autoreferacie wykorzystują zależności DT oraz DD.

Interwał DT charakteryzuje wykorzystanie konkretnego klawisza niezależnie od innych, stąd wykorzystywany jest w przypadku użycia pojedynczych klawiszy. Interwał DD obsługuje zdarzenia wciśnięcia klawiszy w określonej kolejności, podczas gdy dla interwału UU zwalnianie przycisków może następować w różnej kolejności – takiej samej jak wciśnięcia (Rys. 1b) lub odwrotnej (Rys. 1c).

Najlepiej wyjaśni to przykład. W celu wpisania wielkiej litery należy użyć kombinacji klawiszy SHIFT+litera wciskanych we wskazanej kolejności. Wciśnięcie ich w odwrotnej kolejności spowoduje błędne wpisanie małej litery. Kolejność zwalniania przycisków nie ma znaczenia. Można więc założyć, ze względu na częste powtórzenia, że bardziej charakterystyczny dla aktywności użytkownika będzie interwał DD.

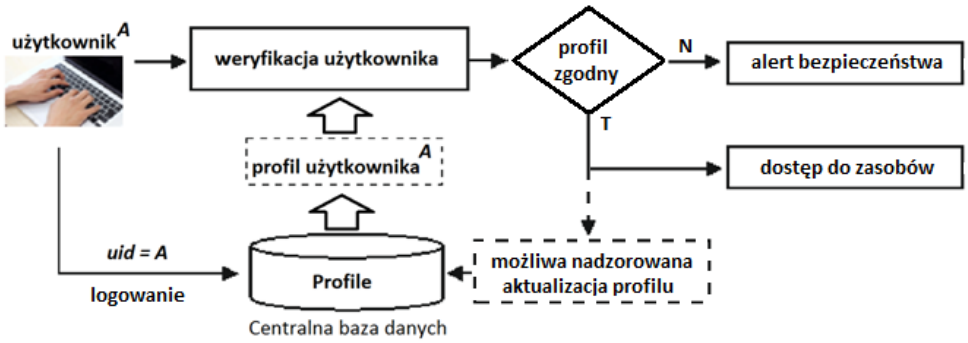
3 Proponowany model systemu weryfikacji użytkownika

System profilowania i weryfikacji ma budowę modularną. Ogólna struktura systemu zaprezentowana została na Rys. 2. Na potrzeby *profilowania* użytkownika tworzony jest jego profil biometryczny charakteryzujący zachowanie użytkownika. Następuje rejestracja rzeczywistej (niezakłóconej dodatkowymi zadaniami) aktywności uprawnionego użytkownika i wyznaczenie zależności czasowych pochodzących z wykorzystanych przycisków klawiatury. Następnie, na podstawie zarejestrowanych zależności czasowych, tworzone są wektory cech behawioralnych. Zbiór wektorów cech uprawnionego użytkownika *uid* staje się jego profilem. Proces wyznaczania profilu użytkownika na podstawie zarejestrowanej w czasie rzeczywistym aktywności może zostać przeprowadzony w trybie offline, po utworzeniu określonej liczby wektorów cech. Proces ten nie angażuje profilowanego użytkownika. Profil każdego uprawnionego użytkownika *uid* przechowywany jest w bazie danych na serwerze.



Rys. 2: Proponowana struktura modułowa systemu weryfikacji użytkownika

Etap *weryfikacji* jest podobny do etapu profilowania użytkownika, ale zgodnie z założeniami CV w tym przypadku cały proces (łącznie z podejmowaniem decyzji) odbywa się w czasie rzeczywistym (w trybie online). Na tym etapie użytkownik, z założenia, jest traktowany jako potencjalny intruz. Aktywność użytkownika na bieżąco weryfikuje moduł *klasyfikacji*, który podejmuje decyzję, czy aktualne działania użytkownika są zgodne z wcześniej zarejestrowanym profilem. W przypadku, gdy użytkownik zostanie rozpoznany jako intruz, moduł weryfikacji zgłosi alert (Rys. 3).



Rys. 3: Ogólny schemat proponowanego procesu weryfikacji użytkownika

4 Autorska metoda profilowania użytkowników na podstawie KDA

Postać rejestrowanych sekwencji zdarzeń klawiatury jest różna w różnych podejściach, co silnie ogranicza ich użycie w analizie porównawczej. Stosowane są krótkie teksty [11] lub hasła o ustalonej treści i różnej długości [28], wpisywane wielokrotnie przez tego samego użytkownika w fazie autoryzacji dostępu. Jest to zadanie uciążliwe i czasochłonne, opóźniające rozpoczęcie normalnej pracy. Innym rozwiązaniem jest tzw. rejestracja „tekstu swobodnego" (*ang.* free-text) [15]. Tego typu działania są naiwne, ponieważ jedynie symulują rzeczywiste warunki pracy użytkownika poprzez wykonywanie przez niego nietypowych zadań.

Nieliczni badacze zdecydowali się udostępnić zbiory danych wykorzystane w swoich eksperymentach [15]. Przeprowadzono analizę zbiorów stosowanych w opisywanych w literaturze badaniach i wskazano niedogodności z nimi związane. Z powodów ograniczeń zbiorów danych, autor zdecydował się na zgromadzenie własnej kolekcji danych, gdzie rejestrowana była aktywność ciągła w warunkach rzeczywistych. Dane były gromadzone przy pomocy autorskiego oprogramowania. Rejestracja danych odbywała się w tle, a w trakcie pracy użytkownik nie miał obowiązku wykonania żadnego dodatkowego zadania. Zarejestrowano w sumie 596 tys. zdarzeń klawiatury od 50 użytkowników: przeciętny użytkownik wygenerował około 12 tys. zdarzeń klawiszy, minimalnie około 7 tys., a maksymalnie około 16 tys. zdarzeń. **Autorska baza danych ma nazwę *realKDD*.**

Baza danych *realKDD*, wykorzystana została do testowania wielowariantowych metod profilowania i weryfikacji użytkowników na podstawie biometrycznego profilu aktywności. W bazie *realKDD* każda linia zaczyna się od wskazania typu zdarzenia, możliwe typy zdarzeń to (zapisane symbolicznie): *keyDown* dla zdarzenia polegającego na wciśnięciu klawisza i *keyUp* dla zwolnienia klawisza. Następnie zapisany jest znacznik czasu tego zdarzenia i identyfikator klawisza. Identyfikatory klawiszy mogą być zapisywane jako znaki wpisywane z klawiatury wprost (np. litery) lub w postaci zaszyfrowanej jako długie ciągi znaków. Dla uproszczenia zapisu w dalszej części autoreferatu identyfikatory klawiszy przedstawiono w postaci symbolicznej. Przykładowe dane wejściowe po wstępnym przetworzeniu są przedstawione na Rys. 4.

```
keyDown,   1396968151226,   ID12
keyUp,     1396968151471,   ID12
keyDown,   1396968153278,   ID31
keyUp,     1396968154176,   ID31
```

Rys. 4: Przykładowe zarejestrowane zdarzenia klawiatury w postaci symbolicznej

Dane są analizowane dla każdego użytkownika o identyfikatorze *uid* oddzielnie. Zarejestrowane dane j-tego zdarzenia klawiatury, użytkownika *uid* można przedstawić w postaci uporządkowanego wektora $\mathbf{e}_j$:

$$\mathbf{e}_j = [typ_j, t_j, \omega_j], \tag{1}$$

gdzie $typ_j \in \{keyDown, keyUp\}$ określa rodzaj j-tego zdarzenia: *keyDown* oznacza wciśnięcie, a *keyUp* zwolnienie klawisza; t_j jest znacznikiem czasowym tego zdarzenia; a ω_j jest identyfikatorem wykorzystanego klawisza.

Wszystkie wektory $\mathbf{e}_j$ danego użytkownika stanowią zbiór zdarzeń E^{uid} reprezentujący aktywność użytkownika *uid*. Dane w tej postaci są trudne do analizy, ponieważ nie dostarczają w bezpośredni sposób informacji o tym, jak użytkownik korzysta z klawiatury. Przeprowadzenie operacji KDA wymaga dodatkowo wyznaczenia dla każdego użytkownika zależności czasowych na podstawie aktywności zarejestrowanej w postaci zdarzeń klawiatury. W proponowanej metodzie profilowania zastosowano następujące interwały czasowe w zależności od użytych klawiszy:

a) wykorzystanie pojedynczego klawisza – sytuacja, w której klawisz jest wciśnięty, a następnie zwolniony przed wciśnięciem kolejnego. Z dwóch wektorów $\mathbf{e}_j$ reprezentujących wciśnięcie i zwolnienie klawisza wyznaczany jest **czas trzymania DT** klawisza,

b) jednoczesne wykorzystanie pary klawiszy – sytuacja, kiedy kolejny klawisz został wciśnięty przed zwolnieniem poprzedniego. Na przykład podczas użycia kombinacji klawiszy *SHIFT+litera*. Wtedy z dwóch wektorów $\mathbf{e}_j$ reprezentujących zdarzenia wciśnięcia obydwu klawiszy wyznaczany jest **czas wciśnięcie-wciśnięcie DD**.

W tym celu dla użytkownika *uid* tworzony jest pomocniczy zbiór interwałów czasowych D^{uid} składający się z wektorów $\mathbf{d}_i$:

$$\mathbf{d}_i = [d_i, \omega_j, \omega_{j+1}], \tag{2}$$

gdzie d_i jest zależnością czasową DT lub DD zdarzeń klawiszy ω_j i ω_{j+1}.

Wyznaczanie zależności czasowych na podstawie zarejestrowanych zdarzeń klawiatury odbywa się za pomocą Algorytmu 1.

Po wyznaczeniu zależności czasowych d_i, kolejnym krokiem jest podział tych zależności na grupy ze względu na klawisze, których dotyczą (wg zapisanych identyfikatorów ω_j). W profilowaniu użytkownika zaproponowano podział zależności czasowych na grupy G^k, $k \in \{1, \ldots, 113\}$

Algorytm 1: Wyznaczanie zbioru D^{uid} zależności czasowych w postaci wektorów $\mathbf{d}_i^{uid}$ na podstawie zbioru zdarzeń klawiatury E^{uid} użytkownika *uid*

Wejście: E^{uid} – zdarzenia klawiatury jako zbiór wektorów $\mathbf{e}_j^{uid} = [typ_j, t_j, \omega_j]$, gdzie $typ_j \in \{keyDown, keyUp\}$ określa rodzaj j-tego zdarzenia; t_j jest znacznikiem czasowym tego zdarzenia; a ω_j jest identyfikatorem wykorzystanego klawisza.

Wyjście: D^{uid} – zbiór wektorów zależności czasowych $\mathbf{d}_i^{uid} = [d_i, \omega_j, \omega_{j+1}]$

```
1  begin
2      i := 1; j := 1;
3      while (nie koniec danych wejściowych ze zbioru E^uid) do
4          czytaj dane wejściowe e_j^uid = [typ_j, t_j, ω_j] ∈ E^uid;
5          if (typ_j == keyDown) then
6              czytaj dane wejściowe e_{j+1}^uid = [typ_{j+1}, t_{j+1}, ω_{j+1}] ∈ E^uid;
7              if ((ω_j == ω_{j+1}) and (typ_{j+1} == keyUp)) or (typ_{j+1} == keyDown) then
8                  d_i := t_{j+1} − t_j;
9                  d_i^uid := [d_i, ω_j, ω_{j+1}];
10                 D^uid := D^uid ∪ {d_i^uid};
11                 i:=i+1; j:=j+2;
12             end
13         else
14             j:=j+1;
15         end
16     end
17 end
```

związane ze 113 grupami klawiszy. Podział taki wynika głównie z budowy standardowej klawiatury w układzie QWERTY. Ze względu na konieczną zwięzłość Autoreferatu, szczegóły implementacji grupowania dotyczące przydziału zależności do poszczególnych grup zostały opisane w pracy [13] (strona 4 i 5), która stanowi załącznik do Autoreferatu.

Zależności czasowe z kolejnych wektorów $\mathbf{d}_i$ są umieszczane wewnątrz odpowiednich grup G^k, które można traktować jak kontenery o określonej pojemności, aż do ich zapełnienia. W zaproponowanym podejściu maksymalna liczba elementów, które można umieścić w pojedynczym kontenerze, określona jest parametrem g i jest taka sama dla wszystkich grup klawiszy.

W momencie, w którym liczba elementów (interwałów czasowych d_i) w jednej z grup osiągnie wartość maksymalną g, następuje wyznaczenie biometrycznego wektora cech $\mathbf{F}$ (wzór (3)) danego użytkownika *uid*. Z kontenera, który osiągnął liczbę elementów równą g, usuwane są wszystkie elementy, a proces jest kontynuowany aż do osiągnięcia wymaganej liczby wektorów cech $\mathbf{F}$ dla danego użytkownika *uid*.

Bazując na zależnościach czasowych zarejestrowanych we wszystkich grupach G^k, k = 1,...,113, wyznaczany jest wektor cech:

$$\mathbf{F} = [f_1, f_2, \ldots, f_{113}], \tag{3}$$

gdzie f_1,...,f_{113} są cechami wyznaczanymi osobno dla każdej grupy G^k, na podstawie wzoru (4).

Procedura wyznaczania wektora $\mathbf{F}$ wyzwalana jest w momencie przepełnienia się dowolnego kontenera z grup G^k. Każdy k-ty element f_k wektora $\mathbf{F}$ obliczany jest na podstawie zależności czasowych przechowywanych w k-tej grupie $G^k = \{d_1,d_2,...,d_{n_k}\}$ zgodnie z zależnością:

$$f_k = \begin{cases} 0 & \text{dla } n_k = 0, \\ \sqrt{\frac{1}{n_k}\sum_{m=1}^{n_k}(d_m - \bar{t}_k)^2} & \text{dla } n_k > 0, \end{cases} \tag{4}$$

gdzie n_k jest bieżącą liczbą elementów w grupie G^k, a $\bar{t}_k$ jest średnią zarejestrowanego interwału czasowego:

$$\bar{t}_k = \frac{1}{n_k}\sum_{m=1}^{n_k} d_m. \tag{5}$$

Częstotliwość wyznaczania wektorów cech $\mathbf{F}$ jest związana z wartością parametru g, który jest istotnym wskaźnikiem metody profilowania. Parametr g został dobrany globalnie dla systemu weryfikacji użytkowników oraz indywidualnie dla każdego użytkownika osobno (g^{uid}). W proponowanym podejściu wartość parametru g^{uid} wyznaczanego dla użytkownika *uid* została zoptymalizowana za pomocą algorytmu rojowego PSO (*ang.* Particle Swarm Optimization) [25].

Na podstawie otrzymanych wektorów cech $\mathbf{F}^{uid}$ dla danego użytkownika *uid* wyznaczany jest profil Φ^{uid} jego aktywności:

$$\Phi^{uid} = \left\{\mathbf{F}_1^{uid},\mathbf{F}_2^{uid},\ldots,\mathbf{F}_r^{uid}\right\}, \tag{6}$$

gdzie r jest parametrem metody profilowania i oznacza liczbę wektorów cech wchodzących w skład profilu użytkownika.

Wartość parametru r została dobrana eksperymentalnie w toku badań. Wyznaczony biometryczny profil użytkownika Φ^{uid} zapisywany jest w bazie profili. Profil ten będzie wykorzystywany na etapie weryfikacji użytkownika (Rys. 3).

5 Weryfikacja użytkownika na podstawie biometrycznego profilu aktywności

Zbiór testowy, składa się z wektorów (biometrycznego profilu) uprawnionego użytkownika oraz innego użytkownika, który w eksperymencie będzie reprezentował intruza. Aby ustalić, czy mamy do czynienia z uprawnionym użytkownikiem czy intruzem, konieczne jest sprawdzenie, jak bardzo każdy testowany wektor cech różni się od ustalonego profilu. W eksperymentach założono, że biometryczny profil zachowań użytkownika Φ^{uid} budowany jest automatycznie. Testy zostały przeprowadzone z wykorzystaniem techniki 10-krotnej walidacji krzyżowej. Proces był

powtarzany 20-krotnie. Zbiory uczące i testowe w każdym eksperymencie były wybierane losowo, a otrzymane wyniki w poszczególnych przebiegach eksperymentów były uśrednione.

Weryfikacja użytkowników może przebiegać według różnych schematów i należy wybrać najlepszy. Zbadano dwa schematy weryfikacji – wykorzystujące pojedyncze klasyfikatory lub zespoły klasyfikatorów (patrz także Rys. 2).

Metoda profilowania użytkownika została sprawdzona eksperymentalnie z wykorzystaniem zestawu danych *realKDD*. W eksperymentach wykorzystano klasyfikatory z pakietu KNIME – WEKA. We wszystkich eksperymentach w fazie uczenia wykorzystywano te same zestawy danych wejściowych.

W eksperymentach poszukiwana jest optymalna skuteczność klasyfikacji ACC (*ang.* Accuracy), która jest jednak zależna od doboru wielu parametrów:

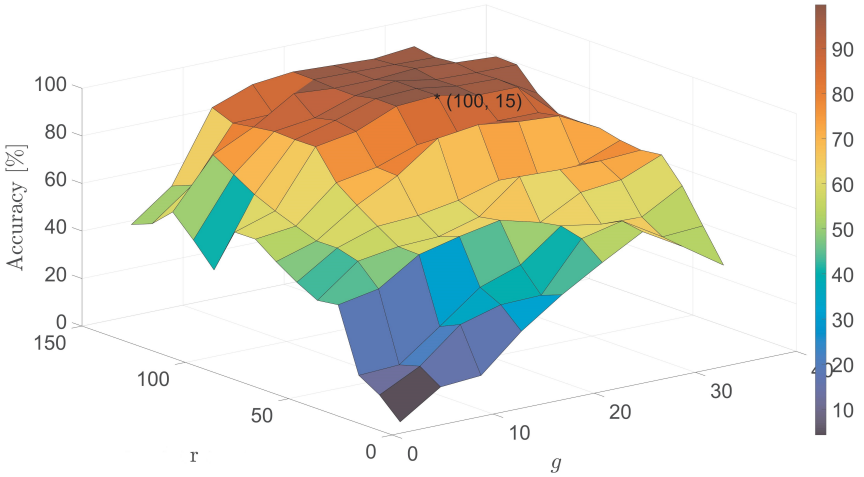
$$ACC = f(g, r) = f(x). \tag{7}$$

Niech $T = \{(g, r)\}$, wtedy wartości elementów zbioru T maksymalizują skuteczności klasyfikacji ACC według zależności:

$$\underset{x \in T}{\operatorname{argmax}} f(x) = \{x \in T : f(x) = \max_{u \in T} f(u)\}. \tag{8}$$

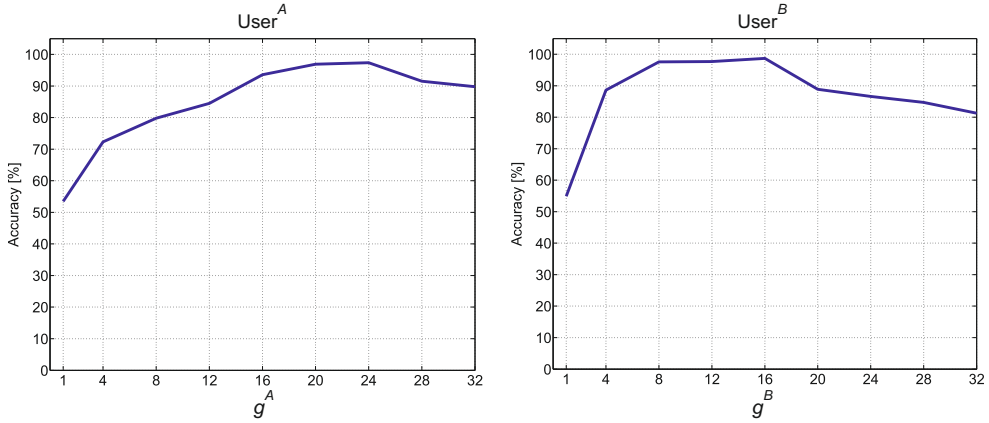
Kluczowym parametrem metody profilowania użytkownika jest parametr g mający wpływ na budowę wektora cech $\mathbf{F}$. Zbadano dwie strategie doboru parametru g: parametr g jest ustalany dla całego systemu (ta sama wartość g dla każdego użytkownika) oraz dobór wartości tego parametru dla każdego użytkownika osobno (g^{uid}).

Wykres na Rys. 5 prezentuje wyniki równoczesnej optymalizacji parametrów g oraz r profilu biometrycznego w wariancie globalnym, w celu maksymalizowania skuteczności klasyfikacji Accuracy (ACC).



Rys. 5: Wykres zależności skuteczności Accuracy od wartości parametrów g i r. Optymalne wartości parametrów $g = 15$, $r = 100$

Dla ustalonego parametru $r = 100$ zbadano także wpływ parametru g na skuteczność klasyfikacji wyznaczanej dla każdego użytkownika *uid* osobno (Rys. 6). Można zauważyć, że optymalna wartość parametru g^{uid} jest różna dla różnych użytkowników. W związku z powyższym, w kolejnych badaniach parametr g^{uid} był wyznaczany indywidualnie dla każdego użytkownika. Indywidualna wartość parametru g^{uid} została wyznaczona algorytmem rojowym PSO [25].



Rys. 6: Wpływ parametru g^{uid} na skuteczność klasyfikacji dla przykładowych użytkowników A i B

Profile użytkowników, wyznaczone na podstawie optymalnych wartości parametrów, w obu przypadkach zostały zweryfikowane w module klasyfikacji z wykorzystaniem zarówno klasyfikatorów pojedynczych, jak i zespołowych. W badaniu porównawczym wybrano klasyfikatory najczęściej wykorzystywane w praktyce i implementowane w wielu pakietach z wbudowanymi funkcjami uczenia maszynowego, takich jak Matlab, R, czy WEKA. Wyniki eksperymentów dla klasyfikatorów oferujących najlepszą skuteczność zostały przedstawione w Tabeli 1. Wyniki są wartościami uśrednionymi w przebiegu dwudziestu eksperymentów wraz z odchyleniem standardowym. Po wyłonieniu zestawu najlepszych klasyfikatorów, zastosowano je w klasyfikacji komitetowej.

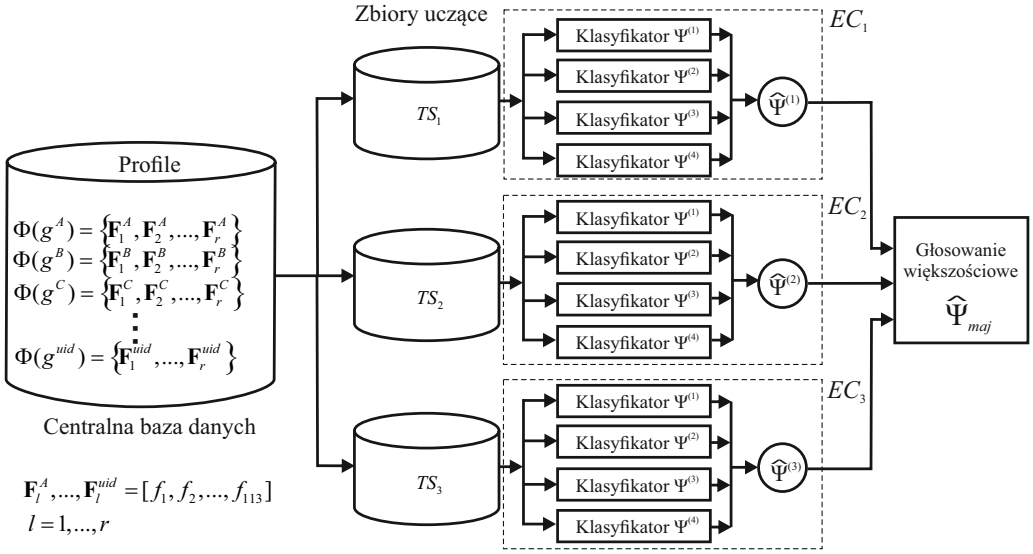
Tabela 1: Skuteczność klasyfikacji przy wykorzystaniu pojedynczego klasyfikatora z optymalizacją parametrów na poziomie użytkownika (baza *realKDD*)

Klasyfikator	ACC [%]
Random Forest RF*	88,81 ± 0,77
Bayes Net BN*	86,99 ± 0,91
C4.5*	86,74 ± 1,10
Support Vector Machine SVM*	84,56 ± 0,57
Naive Bayes	79,91 ± 0,33
Random Tree	79,24 ± 1,03
Ridor	78,58 ± 1,10

* wyróżnione klasyfikatory wejdą w skład komitetu

5.1 Komitety klasyfikatorów z głosowaniem większościowym

Moduł klasyfikacji (Rys. 2) może działać wykorzystując pojedyncze klasyfikatory lub komitet klasyfikatorów. Po ustaleniu zestawu najbardziej skutecznych klasyfikatorów, zbudowane zostały komitety klasyfikatorów. Klasyfikatory wchodzące w skład komitetu ustalają wynik w głosowaniu większościowym. Proponowane rozwiązanie bazuje na trzech komitetach klasyfikatorów EC_a, $a = 1,2,3$. Każdy z nich zbudowany jest z czterech heterogenicznych klasyfikatorów: $\Psi^{(1)}$, $\Psi^{(2)}$, $\Psi^{(3)}$ i $\Psi^{(4)}$. Struktura modułu klasyfikacji komitetowej pokazana jest na Rys. 7.



Rys. 7: Struktura zaproponowanego modułu klasyfikacji opartego na klasyfikacji komitetowej

Komitety EC_a działają równolegle, a każdy z nich uczony jest odrębnym zestawem danych uczących TS_a, składającym się z wektorów cech $\mathbf{F}$ losowo wybranych z profilu użytkownika.

Weryfikacja bieżącej aktywności użytkownika polega na przypisaniu go do jednej z dwóch klas: uprawniony lub intruz. Biometryczna aktywność weryfikowanego użytkownika rejestrowana w czasie rzeczywistym reprezentowana jest przez wektor cech $\mathbf{F} = [f_1, f_2, \ldots, f_{113}]$. W przypadku klasyfikacji binarnej, z którą mamy tutaj do czynienia, klasyfikator Ψ odwzorowuje dyskretną przestrzeń cech $\mathbf{F}$ w zbiór C etykiet klas c_j:

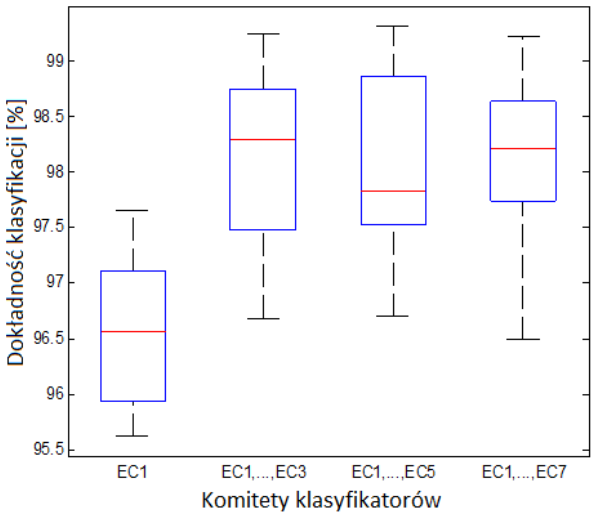
$$\Psi(\mathbf{F}) \rightarrow c \in C = \{c_1, c_2\}, \tag{9}$$

gdzie c_1 oznacza uprawnionego użytkownika, a c_2 intruza.

Każdy z komitetów klasyfikatorów EC_a, $a = 1,2,3$ ustala na wyjściu lokalną decyzję $\hat{\Psi}^{(a)}$. Na podstawie decyzji lokalnych, moduł klasyfikacji w głosowaniu większościowym podejmuje decyzję $\hat{\Psi}_{maj}(\mathbf{F})$, która wskazuje, czy wektor $\mathbf{F}$ został uzyskany na podstawie aktywności uprawnionego, czy też nieuprawnionego użytkownika.

Wyniki eksperymentów przeprowadzonych dla pojedynczego komitetu (EC_1) i zestawu komitetów wchodzących w skład modułu weryfikacji (Rys. 7) przedstawia wykres na Rys. 8.

Wykorzystanie trzech komitetów klasyfikatorów daje lepsze wyniki, niż w przypadku zastosowania pojedynczego komitetu. Dalsze zwiększanie liczby komitetów nie powoduje istotnego zwiększenia dokładności klasyfikacji, co jasno wynika z wykresów pudełkowych (Rys. 8).



Rys. 8: Dokładność klasyfikacji w zależności od wariantu klasyfikatora zespołowego

Wyniki weryfikacji opartej na komitetach klasyfikatorów dla przypadków wyznaczania parametrów na poziomie systemu i użytkownika zebrano w Tabeli 2, która zawiera wartości skuteczności klasyfikacji ACC, błędu zrównoważenia systemu biometrycznego EER, współczynnika niesłusznych akceptacji FAR oraz współczynnika niesłusznych odrzuceń FRR. Komitety ze strategią głosowania większościowego (*ang.* majority voting) składające się z czterech różnych klasyfikatorów w strukturze komitetu oznaczone zostały jako **KomitetyMaj**. W tej samej tabeli umieszczono także wyniki najlepszego pojedynczego klasyfikatora RF.

Tabela 2: Porównanie wyników weryfikacji z optymalizacją parametrów na poziomie systemu (parametry globalne) i użytkownika (baza *realKDD*)

Klasyfikator	**ACC** [%]	**EER** [%]	**FAR** [%]	**FRR** [%]
KomitetMaj $^{u)}$	98,89 ± 0,17	1,11 ± 0,01	0,74 ± 0,00	1,59 ± 0,01
KomitetMaj $^{g)}$	97,83 ± 0,31	2,17 ± 0,04	2,01 ± 0,02	3,74 ± 0,04
RF $^{u)}$	88,81 ± 0,77	11,19 ± 0,02	9,17 ± 0,03	14,22 ± 0,02
RF $^{g)}$	87,98 ± 0,81	12,02 ± 0,01	10,54 ± 0,02	16,11 ± 0,02

$^{u)}$ parametry optymalizowane na poziomie użytkownika
$^{g)}$ parametry optymalizowane na poziomie systemu (globalnie)

Jednym z założeń metody weryfikacji użytkowników jest możliwość aktualizacji profilu, w celu uwzględnienia naturalnych, behawioralnych zmian zachowań uprawnionego użytkownika. Zmiany profilu behawioralnego użytkownika mogą mieć różne przyczyny. Mogą wynikać ze zmiany natężenia aktywności użytkownika czy też doznanego urazu. Takie sytuacje powodują, że system IDS częściej wygeneruje alerty dla uprawnionego użytkownika (błędy fałszywego odrzucenia FR, *ang.* False Reject) negatywnie wpływając na komfort pracy użytkownika. Aby

zapobiec takim sytuacjom, należy w systemie autoryzacji ciągłej CA wprowadzić automatyczną aktualizację profilu użytkownika. W związku z tym, zaproponowano strategię klasyfikacji wspieranej kompetencjami, która to umożliwi.

5.2 Klasyfikatory wspierane kompetencjami i proponowana strategia automatycznej aktualizacji profilu

Rozszerzenie poprzedniej metody wykorzystuje klasyfikatory wspierane kompetencjami. Badania przeprowadzono dla maksymalizacji wartości współczynnika ACC zgodnie ze wzorem (8).

Dla każdego klasyfikatora z puli Υ za pomocą algorytmu Round Robin (turniej all-play-all) można ustalić najlepsze wartości parametrów r i g, które maksymalizują skuteczność danego klasyfikatora. Eksperymenty zostały przeprowadzone dla różnych klasyfikatorów w puli. Wyniki eksperymentów dla klasyfikacji wspieranej kompetencjami klasyfikatorów opartej na pojedynczych klasyfikatorach i komitetach (**KomitetKomp**) przedstawia Tabela 3. Dla porównania tabela zawiera wyniki otrzymane dla komitetów ze strategią głosowania większościowego **KomitetMaj**. Najlepsze wyniki weryfikacji uzyskano dla rozwiązania wykorzystującego kompetencje klasyfikatorów, do którego dodano strategię automatycznej aktualizacji profilu.

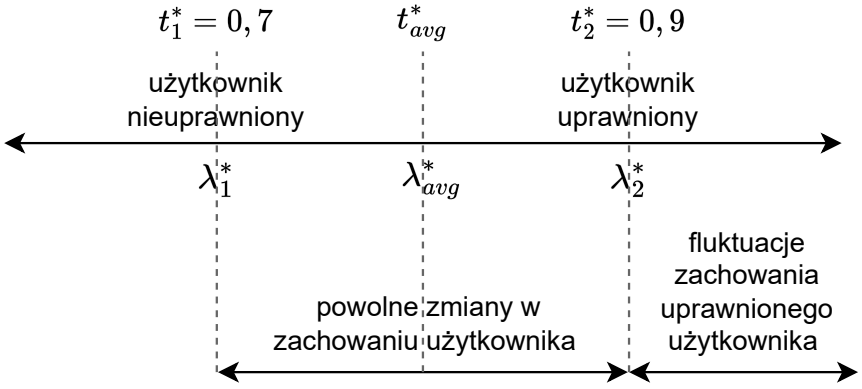
Jeżeli normalna aktywność uprawnionego użytkownika *uid* zostanie zakłócona, spowoduje to zmianę charakterystyki behawioralnej. Gwałtowne zmiany zachowania można wykryć stosunkowo łatwo – oznacza to, że w danym momencie działa nieautoryzowana osoba. Powolne zmiany i fluktuacje zachowań są trudniejsze do wykrycia, gdyż autoryzowana osoba pracuje jednak w dopuszczanym biometrycznym profilu zachowań. Wyzwaniem jest znalezienie progu, który wykryje te zmiany, czyli pozwoli na odróżnienie aktywności autoryzowanej od nieautoryzowanej.

W proponowanej strategii, klasyfikator Υ_d wybiera klasę o najwyższym prawdopodobieństwie a posteriori. W praktyce prawdopodobieństwo jest ustalane na podstawie funkcji wsparcia λ klasyfikatora. Różne wartości funkcji wsparcia będą traktowane jako progi t_1^* (dla λ_1^*) i t_2^* (dla λ_2^*), które kategoryzują zachowania użytkownika *uid*. Idea tej separacji jest przedstawiona na Rys. 9. Wartości progów zostały ustalone eksperymentalnie i ich optymalne wartości wynoszą $t_1^* = 0{,}7$ i $t_2^* = 0{,}9$.

Dla takich założeń można utworzyć trzy progi: t_1^*, t_2^* oraz t_{avg}^*, gdzie $t_{avg}^* = (t_1^* + t_2^*)/2$, a $\lambda_{avg}^* = (\lambda_1^* + \lambda_2^*)/2$ (Rys. 9).

W przypadkach, gdy aktywność użytkownika nie jest stabilna, system weryfikacji wygeneruje alerty, informując, że dany użytkownik powinien zostać dodatkowo skontrolowany, na przykład za pomocą innej biometrii lub przez administratora.

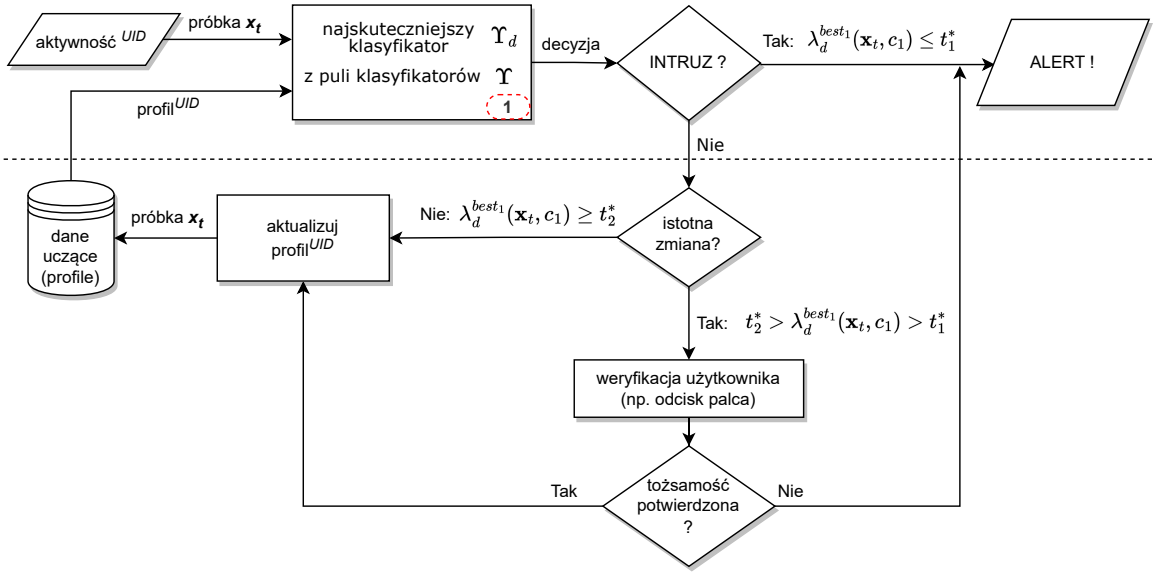
Progi t_1^* i t_2^* są wykorzystywane w strategii z automatyczną aktualizacją profilu. Zgodnie z przyjętymi założeniami powoduje to ciągłą aktualizację danych uprawnionego użytkownika *uid*. Łagodne zmiany zachowania użytkownika nie będą generować alertów w przeciwieństwie



Rys. 9: Progi t_1^* i t_2^* oddzielające użytkowników autoryzowanych od nieautoryzowanych

do działań intruza. Analizowano dwa rodzaje zmian danych, charakteryzujących zachowanie użytkownika: zmiany następują nagle – oznacza to, że nieautoryzowany użytkownik korzysta z komputera, zmiany następują stopniowo lub przyrostowo – wynika to ze zmian zachowania uprawnionego użytkownika.

Dla wygody czytelnika główne etapy metody przedstawiono w postaci schematu blokowego (Rys. 10). Z komitetu klasyfikatorów zawsze dynamicznie wybierany jest klasyfikator o największym współczynniku wsparcia próbki $\mathbf{x}_t$ (weryfikowanego bieżącego wektora $\mathbf{F}$). To zadanie realizowane jest w bloku **1** (Rys. 10). Dolną część diagramu na Rys. 10 można pominąć, wtedy klasyfikatory komitetu pracują w trybie głosowania większościowego bez kompetencji i bez aktualizacji profilu, co opisano wcześniej (Rys. 2 i 7).



Rys. 10: Schemat blokowy algorytmu klasyfikacji danych biometrycznych użytkownika i aktualizacji jego profilu

5.3 Podsumowanie eksperymentów wykorzystujących bazę *realKDD*

Wyniki eksperymentów wykorzystujących bazę *realKDD* przedstawia Tabela 3. Można zauważyć, że strategia komitetowa z kompetencją klasyfikatorów **KomitetKomp** daje korzystniejsze wyniki dla współczynników ACC, EER, FAR i FRR w porównaniu z komitetem opartym na głosowaniu większościowym **KomitetMaj**. Używając tych samych klasyfikatorów w trybie pojedynczym uzyskujemy zawsze najgorsze wyniki.

W kolejnych eksperymentach wykorzystano te same klasyfikatory, jednak tym razem zastosowano strategię alertów i tryb progowania w celu automatycznego aktualizowania profilu. Porównanie wyników bez i ze wsparciem strategią alertów (oznaczonych indeksem A) możemy również znaleźć w Tabeli 3.

Z punktu widzenia bezpieczeństwa, weryfikacja użytkowników na podstawie biometrycznego profilu aktywności jest lepsza, gdy używane są klasyfikatory z kompetencjami. Wskazują na to wyniki eksperymentów zawarte w Tabeli 3. Analiza porównawcza wyników potwierdza, że najlepszą skuteczność (ACC) uzyskuje strategia uzupełniona o alerty i aktualizację profilu, co pozwala na korzystanie z systemu przez użytkowników, którzy nie mają stabilnych schematów behawioralnych podczas długotrwałej pracy.

Jest to zaleta proponowanego w autoreferacie rozwiązania.

Ostatecznie porównano wyniki weryfikacji biometrycznego profilu użytkownika tworzonego z wykorzystaniem bazy *realKDD* oraz wyniki metod opisanych w literaturze testowanych na bazie ClarksonII/Murphy [10] najbardziej zbliżonej zawartością do bazy *realKDD*. Zestawienie prezentuje Tabela 3. Wynika z niego, że proponowane w autoreferacie autorskie rozwiązania cechują się wyższą skutecznością weryfikacji niż inne metody.

Tabela 3: Wyniki weryfikacji użytkownika z wykorzystaniem bazy *realKDD* (indeksy: 1, 2, 3) oraz bazy ClarksonII najbardziej zbliżonej zawartością do bazy *realKDD*

Klasyfikator	**ACC** [%]	**EER** [%]	**FAR** [%]	**FRR** [%]
KomitetKomp$^{A\ 1)}$	99,85 ± 0,21	0,15 ± 0,00	0,10 ± 0,00	0,22 ± 0,00
KomitetKomp $^{1)}$	99,32 ± 0,21	0,68 ± 0,01	0,53 ± 0,00	0,78 ± 0,00
KomitetMaj$^{A\ 2)}$	99,21 ± 0,16	0,79 ± 0,00	0,54 ± 0,00	0,89 ± 0,00
KomitetMaj $^{2)}$	98,89 ± 0,17	1,11 ± 0,01	0,74 ± 0,00	1,59 ± 0,01
RF$^{A\ 3)}$	93,28 ± 0,18	6,72 ± 0,01	4,40 ± 0,01	12,97 ± 0,03
Acien2021 [1]	-	2,20	-	-
Xiaofeng2018 [26]	-	2,67	-	-
Li2022 [8]	91,91	7,55	-	-
Li2021 [8]	91,9	7,70	-	-
RF $^{3)}$	89,78 ± 0,26	10,22 ± 0,02	8,64 ± 0,03	13,32 ± 0,02

[-] dane niedostępne

[1)] Komitet klasyfikatorów wspierany kompetencjami

[2)] Komitet klasyfikatorów z głosowaniem większościowym bez kompetencji

[3)] Pojedynczy klasyfikator

[A] Indeks **A** oznacza zastosowanie w metodzie strategii alertów z automatyczną aktualizacją profilu

Poprawność przyjętych rozwiązań potwierdzona została także za pomocą testów Wilcoxona i Bayesa. Testy przeprowadzono dla skuteczności ACC modelu klasyfikacji komitetowej bez i ze wsparciem strategią alertów (Tabela 3). Obliczenia przeprowadzono dla przedziału ufności 95% (α = 0,05) uzyskując wynik $p = 0.00768 < \alpha$. W związku z tym można stwierdzić, że istnieją dowody statystyczne na poziomie α = 0,05, że średnie wartości ACC w obu przypadkach istotnie się różnią. Tym samym wykazano, że wprowadzenie mechanizmu alertów i automatycznej aktualizacji profilu istotnie poprawia skuteczność weryfikacji użytkowników.

Proponowane rozwiązanie zostało również sprawdzone testem znakowanych rang Bayesa, gdzie brane są pod uwagę wszystkie elementy walidacji krzyżowej we wszystkich rundach. W tym teście można porównać dwa klasyfikatory, a test daje trzy wartości w kategoriach prawdopodobieństwa: a) pierwsza metoda jest lepsza od drugiej, b) metody są równoważne, c) pierwsza metoda jest gorsza od drugiej.

Porównano najbardziej obiecujące podejścia: **KomitetKomp**, **KomitetMaj**, **KomitetKompA** i **KomitetMajA**. Tabela 4 przedstawia wyniki porównania skuteczności ACC, suma prawdopodobieństw w komórkach jest równa 1. Komitety klasyfikatorów wspierane strategią alertów (**KomitetKompA** i **KomitetMajA**) wykazują przewagę w porównaniu z pozostałymi podejściami (**KomitetKomp** i **KomitetMaj**).

Tabela 4: Porównanie skuteczności ACC klasyfikatorów w teście Bayesian signed-rank (baza *realKDD*)

Komitet	**KomitetMaj**	**KomitetKompA**	**KomitetMajA**
KomitetKomp	1,000/0,000/0,000	0,000/0,197/0,803	0,175/0,825/0,000
KomitetMaj	-	0,000/0,000/1,000	0,000/0,003/0,997
KomitetKompA	-	-	1,000/0,000/0,000

Prawdopodobieństwa w każdej komórce oznaczają:
metoda w wierszu tabeli jest lepsza / metody są równoważne / metoda w kolumnie jest lepsza.

5.4 Weryfikacja autorskich metod z wykorzystaniem bazy Bufallo

W celu zapewnienia rzetelności badań przeprowadzono walidację proponowanych metod wykorzystując publicznie dostępną bazę danych *Bufallo* [15]. Eksperymenty z wykorzystaniem bazy Bufallo również potwierdziły skuteczność biometrycznego profilowania i weryfikacji użytkowników opartej na klasyfikacji wspieranej kompetencjami i strategią alertów z automatyczną aktualizacją profilu.

Ostatecznie porównano wyniki eksperymentów z innymi metodami opisanymi w literaturze, testowanymi na tej samej bazie danych Bufallo. Zestawienie wyników prezentuje Tabela 5. Wyniki z tej tabeli wskazują, że proponowane rozwiązania autorskie cechują się w większości przypadków wyższą skutecznością weryfikacji. Jedną z metod [3] cechuje wyższa skuteczność ACC, jednak porównanie z uwzględnieniem współczynnika EER wypada na korzyść autorskiego rozwiązania.

Tabela 5: Porównanie autorskich metod weryfikacji biometrycznego profilu użytkownika z innymi metodami. Weryfikację przeprowadzono z wykorzystaniem bazy Bufallo [15]

Klasyfikator	**ACC** [%]	**EER** [%]	**FAR** [%]	**FRR** [%]
Chang2021 [3]	99,31	6,90	-	-
KomitetKomp^{A}	99,17 ± 0,23	0,83 ± 0,01	1,31 ± 0,03	2,11 ± 0,00
Li2022 [8]	98,56	0,88	-	-
KomitetKomp	98,34 ± 0,27	1,66 ± 0,02	1,59 ± 0,00	2,02 ± 0,00
KomitetMaj^{A}	98,32 ± 0,20	1,68 ± 0,02	1,37 ± 0,02	2,52 ± 0,00
KomitetMaj	97,95 ± 0,14	2,05 ± 0,01	2,06 ± 0,01	2,88 ± 0,01
Acien2021 [1]	-	2,20	-	-
Xiaofeng2018 [26]	-	2,67	-	-
Xiaofeng2019 [27] (3 cechy KDA)	-	3,04	4,12	1,95
Xiaofeng2019 [27] (cecha DT)	-	9,17	5,96	12,39

$^{-}$ dane niedostępne

6 Podsumowanie

W autoreferacie przedstawiono autorski algorytm tworzenia profilu biometrycznego oraz nowatorską metodę weryfikacji użytkowników opartą na klasyfikatorach wspieranych kompetencjami i progami decyzyjnymi pozwalającą na automatyczną aktualizację profilu behawioralnego.

Weryfikacja jest przeprowadzana automatycznie, w sposób ciągły, co zwiększa bezpieczeństwo systemu. Zastosowanie weryfikacji ciągłej wykorzystującej biometryczny profil aktywności użytkownika bazujący na KDA oraz strategii automatycznej aktualizacja profilu behawioralnego sterowanej progami decyzyjnymi poprawia skuteczność weryfikacji użytkowników.
Tym samym potwierdzona została teza rozprawy.

W ramach prac zaprojektowano i zaimplementowano oprogramowanie do ciągłej rejestracji aktywności użytkownika. Przeprowadzono proces akwizycji danych w rzeczywistych warunkach pracy użytkowników i na podstawie zarejestrowanych zdarzeń utworzono bazę danych do testów. Pozwoliło to na opracowanie autorskiego algorytmu biometrycznego profilowania użytkowników wykorzystującego KDA oraz metody weryfikacji użytkowników na podstawie profilu behawioralnego. Zaproponowana metoda weryfikacji została rozszerzona o strategię alertów z automatyczną aktualizacją profilu behawioralnego sterowaną progami decyzyjnymi co poprawiło skuteczność weryfikacji.
Opisane w autoreferacie autorskie strategie profilowania i weryfikacji były testowane na danych rzeczywistych i porównane z innymi metodami walidowanymi na tym samym zestawie danych testowych.
Tym samym zrealizowane zostały wszystkie cele określone we wstępie autoreferatu.

Autoreferat prezentuje nowe podejście do weryfikacji użytkowników na podstawie profilu biometrycznego. Badania potwierdziły, że klasyfikatory działające w komitecie oraz wspierane kompetencjami zapewniają najwyższą skuteczność metody.

Przedstawiona metoda może być przydatna w praktycznych zastosowaniach: uzyskane

wyniki numeryczne pokazują lepszą skuteczność proponowanej strategii w porównaniu z istniejącymi metodami state-of-the-art.

Dodatkowo zaproponowano modyfikację wprowadzającą nowatorską metodę wspierania weryfikacji alertami wraz z automatyczną aktualizacją profilu behawioralnego użytkownika. Strategia ta pozwala uwzględnić naturalne zmiany w zachowaniu użytkowników (np. na skutek choroby lub podnoszenia umiejętności).

Należy również zauważyć, że metoda może być stosowana, gdy można zarejestrować odpowiednio długą aktywność użytkownika. Wymaga to utworzenia wektora cech $\mathbf{F}$. W przypadku, gdy aktywność jest krótka i naciśnięto tylko kilka klawiszy, wektor $\mathbf{F}$ nie może zostać zbudowany. Można to traktować jako ograniczenie metody.

Autor prac był stypendystą projektu „DoktoRIS – Program stypendialny na rzecz innowacyjnego Śląska" współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.

Badania dotyczące profilowania i weryfikacji użytkowników wykorzystujące wnioskowanie rozmyte zostały częściowo wsparte przez Narodowe Centrum Nauki w ramach grantu nr DEC-2013/09/B/ST6/02264.

7 Publikacje autora dotyczące tematyki autoreferatu

Wyniki badań zawartych w autoreferacie zostały przez autora częściowo opublikowane w czasopismach o międzynarodowym zasięgu (*Applied Soft Computing, Applied Artificial Intelligence* oraz *Soft Computing*) jak i w materiałach międzynarodowych konferencji. Tabela 6 zawiera wykaz prac autora z uwzględnieniem ich tematyki poruszonej w autoreferacie.

Tabela 6: Opublikowane prace wraz z poruszaną w autoreferacie tematyką

Tematyka pracy	Publikacje
Weryfikacja i profilowanie oparte na analizie poleceń	[7, 18]
Analiza aktywności związanej z wykorzystaniem manipulatorów	[12, 16, 21]
Hybrydowe (multimodalne) metody weryfikacji	[14, 17, 19, 24]
Autorska metoda profilowania użytkowników oparta na analizie zdarzeń klawiatury	[13, 14, 17, 20, 22, 23, 24]
Weryfikacja przy użyciu komitetów klasyfikatorów	[13, 20, 22, 23]
Klasyfikatory z kompetencjami	[13]

Najbardziej znaczące publikacje autora związane z tematyką autoreferatu

1. 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 (Punktacja MEiN: **200**, **IF 8,7**)

2. 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 (Punktacja MNiSW: **15**, **IF 0,527**)

3. 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 (Punktacja MNiSW: **25**, **IF 1,271**)

Bibliografia

[1] Acien A., Morales A., Monaco J.V., Vera-Rodriguez R., Fierrez J., *Typenet: Deep learning keystroke biometrics*, IEEE Transactions on Biometrics, Behavior, and Identity Science, 4(1), 57–70, 2021, URL `http://dx.doi.org/10.1109/TBIOM.2021.3112540`.

[2] Alsultan A., Warwick K., *Keystroke dynamics authentication: a survey of free-text methods*, International Journal of Computer Science Issues, 10(4), 1–10, 2013.

[3] Chang H.C., Li J., Stamp M., *Machine learning-based analysis of free-text keystroke dynamics*, arXiv e-prints, arXiv–2107, 2021.

[4] Cooper W.E., Cognitive aspects of skilled typewriting, Springer Science & Business Media, 2012.

[5] Cybersecurity Ventures, *2019 official annual cybercrime report*, `https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report`, 2019, [online, dostęp 21.07.2020].

[6] Doroz R., Wrobel K., Porwik P., *An accurate fingerprint reference point determination method based on curvature estimation of separated ridges*, International Journal of Applied Mathematics and Computer Science, 28(1), 2018.

[7] Kudłacik P., Porwik P., Wesołowski T., *Fuzzy approach for intrusion detection based on user's commands*, Soft Computing, 20(7), 2705–2719, 2016, ISSN 1433-7479, URL `http://dx.doi.org/10.1007/s00500-015-1669-6`.

[8] Li J., Chang H.C., Stamp M., *Free-text keystroke dynamics for user authentication*, Artificial Intelligence for Cybersecurity, 357–380, Springer, 2022.

[9] Monaco J.V., *Time intervals as a behavioral biometric*, PhD diss., PhD thesis, Pace University, 2015.

[10] Murphy C., Huang J., Hou D., Schuckers S., *Shared dataset on natural human-computer interaction to support continuous authentication research*, 2017 IEEE International Joint Conference on Biometrics (IJCB), 525–530, IEEE, 2017.

[11] Neacsu T., Poncu T., Ruseti S., Dascalu M., *Doublestrokenet: Bigram-level keystroke authentication*, Electronics, 12(20), 4309, 2023.

[12] Palys M., Wesołowski T.E., *Features reduction for computer user profiling based on mouse activity*, Journal of MIT, 24, 45–51, 2015, ISSN 1642–6037.

[13] Porwik P., Doroz R., Wesołowski T.E., *Dynamic keystroke pattern analysis and classifiers with competence for user recognition*, Applied Soft Computing, 99(106902), 2021, ISSN 1568-4946, URL http://dx.doi.org/https://doi.org/10.1016/j.asoc.2020.106902.

[14] Safaverdi H., Wesolowski T.E., Doroz R., Wrobel K., Porwik P., *Computer user verification based on typing habits and finger-knuckle analysis*, N.T. Nguyen, G.A. Papadopoulos, P. Jędrzejowicz, B. Trawiński, G. Vossen (red.), Computational Collective Intelligence, 161–170, Springer International Publishing, 2017, ISBN 978-3-319-67077-5, URL http://dx.doi.org/10.1007/978-3-319-67077-5_16.

[15] Sun Y., Ceker H., Upadhyaya S., *Shared keystroke dataset for continuous authentication*, 2016 IEEE International Workshop on Information Forensics and Security (WIFS), 1–6, IEEE, 2016.

[16] Wesołowski T., Palys M., Kudłacik P., *Computer user verification based on mouse activity analysis*, D. Barbucha, T.N. Nguyen, J. Batubara (red.), New Trends in Intelligent Information and Database Systems, tom 598 z serii *Studies in Computational Intelligence*, 61–70, Springer International Publishing, 2015, ISBN 978-3-319-16211-9, URL http://dx.doi.org/10.1007/978-3-319-16211-9_7.

[17] Wesołowski T.E., Doroz R., Wrobel K., Safaverdi H., *Keystroke dynamics and finger knuckle imaging fusion for continuous user verification*, K. Saeed, W. Homenda, R. Chaki (red.), Computer Information Systems and Industrial Management, 141–152, Springer International Publishing, 2017, ISBN 978-3-319-59105-6, URL http://dx.doi.org/10.1007/978-3-319-59105-6_13.

[18] Wesołowski T.E., Kudłacik P., *Data clustering for the block profile method of intruder detection*, Journal of MIT, 22, 209–216, 2013, ISSN 1642–6037.

[19] Wesołowski T.E., Kudłacik P., *User profiling based on multiple aspects of activity in a computer system*, Journal of MIT, 23, 121–129, 2014, ISSN 1642-6037.

[20] Wesołowski T.E., Porwik P., *Keystroke data classification for computer user profiling and verification*, M. Núñez, N.T. Nguyen, D. Camacho, B. Trawiński (red.), Computational Collective Intelligence, 588–597, Springer International Publishing, Cham, 2015, ISBN 978-3-319-24306-1.

[21] Wesołowski T.E., Porwik P., *User verification based on the analysis of keystrokes while using various software*, Journal of MIT, 24, 13–22, 2015, ISSN 1642–6037.

[22] Wesołowski T.E., Porwik P., *Computer user profiling based on keystroke analysis*, R. Chaki, A. Cortesi, K. Saeed, N. Chaki (red.), Advanced Computing and Systems for Security: Volume 1, tom 395, 3–13, Springer India, New Delhi, 2016, ISBN 978-81-322-2650-5, URL http://dx.doi.org/10.1007/978-81-322-2650-5_1.

[23] Wesołowski T.E., Porwik P., Doroz R., *Electronic health record security based on ensemble classification of keystroke dynamics*, Applied Artificial Intelligence, 30(6), 521–540, 2016, http://dx.doi.org/10.1080/08839514.2016.1193715, URL http://dx.doi.org/10.1080/08839514.2016.1193715.

[24] Wesołowski T.E., Safaverdi H., Doroz R., Wrobel K., *Hybrid verification method based on finger-knuckle analysis and keystroke dynamics*, Journal of MIT, 26, 26–36, 2017, ISSN 1642–6037.

[25] Wiatrak M., Figielska E., *Zastosowanie algorytmu optymalizacji rojem cząstek do znajdowania ekstremów globalnych wybranych funkcji testowych*, Zeszyty Naukowe WWSI, 13, 7–19, 2015.

[26] Xiaofeng L., Shengfei Z., Shengwei Y., *Free-text keystroke continuous authentication using cnn and rnn*, Journal of Tsinghua University (Science and Technology), 58(12), 1072–1078, 2018.

[27] Xiaofeng L., Shengfei Z., Shengwei Y., *Continuous authentication by free-text keystroke based on cnn plus rnn*, Procedia computer science, 147, 314–318, 2019.

[28] Zhong Y., Deng Y., Jain A.K., *Keystroke dynamics for user authentication*, 2012 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, 117–123, 2012, ISSN 2160-7508, URL http://dx.doi.org/10.1109/CVPRW.2012.6239225.

Dodatek A

Wykaz oznaczeń stosowanych w autoreferacie

Jeśli w tekście nie wykazano inaczej, stosowane symbole należy rozumieć jako:

uid – identyfikator użytkownika,

Φ^{uid} – profil użytkownika o identyfikatorze uid,

ω_j – identyfikator przycisku użytego w ramach zarejestrowanego j-tego zdarzenia klawiatury,

E – zbiór zdarzeń klawiatury reprezentujących aktywność użytkownika,

D – zbiór zależności czasowych zdarzeń klawiatury reprezentujących aktywność użytkownika,

G – grupa zależności czasowych zdarzeń klawiatury związanych z rodzajem użytego klawisza / użytych klawiszy,

g – rozmiar kontenerów G^k, maksymalna liczba elementów w kontenerze, parametr profilowania,

f_k – k-ta cecha wektora cech,

$\mathbf{F}$ – wektor cech,

r – liczba wektorów cech tworzących profil użytkownika Φ,

τ – próg zaufania (decyzji, akceptacji),

C – przestrzeń klas,

c – etykieta klasy,

$p(c|\mathbf{x})$ – prawdopodobieństwo warunkowe *a posteriori*.