ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КІБЕРБЕЗПЕКА

https://doi.org/10.31649/1997-9266-2026-186-3-61-69

УДК 004.421

Д. П. Курніцький[1]

ЯКІСНО-КЕРОВАНЕ ЗЛИТТЯ КОНТЕКСТНОГО ТА ПОВЕДІНКОВОГО СКОРИНГУ ДЛЯ Risk-Based АВТЕНТИФІКАЦІЇ

[1]Вінницький національний технічний університет

Розглянуто підвищення ефективності автентифікації на основі ризику під час входу в систему шляхом поєднання двох джерел даних: контекстних ознак спроби входу та поведінкових біометричних ознак, сформованих на основі динаміки натискань клавіш. Показано, що традиційні підходи до об'єднання контекстного та поведінкового скорингу часто не враховують якість поведінкового зразка, хоча саме вона істотно впливає на надійність підсумкового рішення. Це особливо важливо для практичного застосування RBA, де навіть незначне зміщення оцінки ризику може призвести або до необґрунтованого ускладнення входу для легітимного користувача, або до зниження здатності системи своєчасно виявляти підозрілі спроби доступу. Автозаповнення полів, короткі паролі, пропуски подій, відмінності між пристроями введення, зміна клавіатурної розкладки, особливості браузера та інші чинники можуть знижувати достовірність поведінкового каналу й підвищувати частоту хибних спрацювань. У зв'язку з цим запропоновано підхід, у якому внесок поведінкових ознак у фінальну оцінку ризику визначається з урахуванням якості отриманого зразка. Розроблено формальну модель злиття контекстної та поведінкової оцінок ризику, а також алгоритм налаштування порогів прийняття рішень для режимів дозволу входу, додаткової перевірки та відмови в доступі. Експериментальну перевірку виконано на синтетичних даних і відкритому наборі CMU Keystroke Dynamics Benchmark. Порівняння з базовими схемами злиття показало, що врахування якості зразка дає змогу адаптивніше використовувати поведінковий канал залежно від ступеня його інформативності. Отримані результати засвідчили, що запропонований підхід дає змогу зменшити кількість зайвих додаткових перевірок без погіршення контрольованого рівня безпеки, а в умовах низької якості поведінкових даних забезпечує ще відчутніший виграш. Запропоноване рішення орієнтоване на підвищення стійкості автентифікації без надмірного зростання навантаження на користувача. Це підтверджує доцільність явного врахування якості поведінкового зразка під час побудови систем автентифікації на основі ризику та налаштування їхніх правил ухвалення рішень.

Ключові слова: автентифікація на основі ризику; контекстні ознаки входу; поведінкові біометричні ознаки; динаміка натискань клавіш; оцінювання якості поведінкового зразка; злиття оцінок ризику; порогове прийняття рішень; додаткова перевірка; контроль доступу; інформаційна безпека.

Вступ

Автентифікація на основі ризику під час входу в систему є перспективним підходом до підвищення захисту облікових записів без надмірного ускладнення доступу для легітимних користувачів. У таких системах рішення про дозвіл входу, додаткову перевірку або відмову приймається з урахуванням ризику конкретної спроби. Для цього використовують контекстні ознаки, зокрема дані про пристрій, мережу, нетипову геолокацію, час входу та історію попередніх спроб. Разом з тим дедалі частіше залучають поведінкові біометричні ознаки, насамперед динаміку натискань клавіш, яка дає змогу враховувати індивідуальні особливості введення пароля.

Динаміка натискань клавіш є одним з найпоширеніших різновидів поведінкової біометрії. Вона базується на аналізі часових характеристик набору, таких як тривалість утримання клавіш і затримки між натисканнями. Перевагою цього підходу є можливість непомітно отримувати додаткові дані про спробу входу без використання спеціального обладнання. Водночас практичне застосування таких ознак ускладнюється тим, що їхня надійність змінюється залежно від умов введення.

На якість поведінкового зразка впливають автозаповнення, короткі паролі, пропуски подій, зміна пристрою, тип клавіатури та особливості мобільного інтерфейсу. Через це поведінковий канал не в кожній спробі входу є однаково інформативним.

Попри значну кількість досліджень у галузі поведінкової біометрії, більшість з них зосереджена на точності розпізнавання, тоді як питання врахування якості поведінкового зразка під час об'єднання контекстної та поведінкової оцінок ризику залишається недостатньо опрацьованим. Унаслідок цього поведінкові ознаки часто використовують як звичайне додаткове джерело даних без явної оцінки їхньої надійності в конкретній ситуації. Тому актуальним є розроблення підходу до поєднання контекстних і поведінкових ознак у межах єдиної моделі ризику з урахуванням якості поведінкового зразка.

Метою роботи є розробка формальної моделі поєднання контекстної та поведінкової оцінок ризику під час входу в систему, у якій внесок поведінкових біометричних ознак визначається з урахуванням якості зразка, а також побудова підходу до налаштування порогів прийняття рішень для зменшення кількості зайвих додаткових перевірок без погіршення контрольованого рівня безпеки.

Постановка задачі

Для підвищення ефективності ризик-орієнтованої автентифікації під час входу в систему доцільно поєднувати контекстні ознаки спроби входу з поведінковими біометричними ознаками клавіатурного почерку. Проте традиційні підходи до об'єднання таких оцінок зазвичай розглядають поведінковий канал як звичайне додаткове джерело ознак і не враховують, що його надійність істотно залежить від якості поточного зразка. Унаслідок цього автозаповнення, короткі паролі, пропуски подій, зміна пристрою, шум та інші чинники можуть знижувати достовірність поведінкових даних, збільшувати кількість хибних спрацювань і призводити до зайвих додаткових перевірок. У зв'язку з цим, постає задача розробки формальної моделі поєднання контекстної та поведінкової оцінок ризику, у якій внесок поведінкового каналу визначається з урахуванням якості зразка, а пороги прийняття рішень налаштовуються з контролем небезпечних помилок у зоні дозволу входу.

Для розв'язання цієї науково-прикладної задачі необхідно виконати такі основні завдання:

1. Провести аналіз наявних підходів до ризик-орієнтованої автентифікації під час входу в систему, а також методів використання поведінкової біометрії за динамікою натискань клавіш.

2. Формалізувати опис спроби входу як сукупності контекстних ознак, послідовності клавіатурних подій і істинної мітки класу.

3. Розробити спосіб побудови поведінкової оцінки ризику на основі ознак клавіатурного почерку та профілю користувача, а також спосіб побудови контекстної оцінки ризику.

4. Запропонувати метрику якості поведінкового зразка, яка відображає, наскільки в конкретній спробі входу можна довіряти поведінковому каналу.

5. Розробити формальну модель поєднання контекстної та поведінкової оцінок ризику, у якій внесок поведінкової складової змінюється залежно від якості зразка.

6. Розробити алгоритм налаштування порогів для режимів дозволу входу, додаткової перевірки та відмови з контролем частки атак, що можуть бути помилково допущені без додаткової перевірки.

7. Провести експериментальну перевірку запропонованого підходу на синтетичних даних і відкритому наборі CMU Keystroke Dynamics Benchmark та порівняти його з підходами без урахування якості зразка.

Виконання зазначених завдань дасть змогу побудувати цілісний підхід до поєднання контекстної та поведінкової оцінок ризику під час входу в систему, який зменшує кількість зайвих додаткових перевірок і водночас не погіршує контрольований рівень безпеки.

Огляд літератури

У сучасних дослідженнях з автентифікації дедалі більше уваги приділяють ризик-орієнтованим підходам, у яких рішення про надання доступу приймається з урахуванням обставин конкретної спроби входу. Одним із напрямів розвитку таких систем є поєднання контекстних ознак з поведінковою біометрією. Зокрема, у працях, щодо спільного використання динаміки миші та клавіатурного почерку, показано, що поведінкові ознаки можуть бути корисним доповненням до традиційних механізмів автентифікації у вебсередовищі [1]. Для сценарію статичного входу також запропоновано підхід, у якому ознаки пристрою поєднуються з поведінковими характеристиками користувача, що дає змогу підвищити стійкість процедури входу [2].

Клавіатурний почерк як різновид поведінкової біометрії досліджується вже тривалий час. У класичних роботах показано, що часові характеристики набору, зокрема тривалість утримання клавіш і затримки між натисканнями, можуть використовуватися для розпізнавання користувача [3]. Подальший розвиток цього напряму пов'язаний з появою відкритих наборів даних і відтворюваних протоколів оцінювання. Важливе значення для галузі мав набір CMU Keystroke Dynamics Benchmark та роботи, у яких порівнювалися алгоритми виявлення аномалій для задачі розрізнення легітимного користувача і зловмисника [4]. Саме ці дослідження заклали основу для зіставлення різних методів за єдиними правилами.

Разом з тим, у науковій літературі неодноразово зазначалося, що ефективність клавіатурного почерку істотно залежить від стабільності зразків у часі. На результати впливають зміна пристрою, індивідуальні коливання стилю набору, шум, а також старіння шаблону користувача. Для зменшення цього впливу запропоновано методи оновлення шаблонів, проте вони не усувають проблему повністю [5]. Додатково ситуацію ускладнює те, що поведінкові біометричні системи можуть бути вразливими до імітаційних атак, а отже поведінковий канал не варто розглядати як безумовно надійне джерело підтвердження особи [6].

Окремий напрям досліджень стосується якості біометричного зразка. У міжнародних стандартах якість зразка трактується як важливий чинник, що визначає придатність біометричних даних для подальшого використання в системі прийняття рішень [7]. Проте у працях, щодо клавіатурного почерку та ризик-орієнтованій автентифікації, основна увага здебільшого зосереджена на показниках розпізнавання, тоді як питання явного врахування якості зразка під час об'єднання контекстної та поведінкової оцінок ризику опрацьовано недостатньо.

Ще однією важливою складовою є калібрування імовірнісних оцінок. Для порогових рішень у ризик-орієнтованій автентифікації недостатньо отримати лише добрий класифікатор — потрібно, щоб його вихідні значення коректно відображали рівень ризику. У зв'язку з цим у машинному навчанні широко використовують підходи до калібрування, зокрема метод Платта, температурне масштабування та ізотонічну регресію [8]. До того ж для практичних систем важливо не лише налаштувати пороги, а й формально обмежити небезпечні помилки. Для цього перспективними є підходи, засновані на схемі Неймана–Пірсона та на конформному контролі ризику, які дають змогу задавати обмеження на помилки з наперед визначеним рівнем довіри [9].

Отже, наявні дослідження підтверджують доцільність використання контекстних і поведінкових ознак у задачах автентифікації, а також важливість калібрування та формального налаштування порогів. Водночас недостатньо опрацьованим залишається питання, як саме враховувати якість поведінкового зразка під час поєднання контекстної та поведінкової оцінок ризику. Саме ця невирішена частина проблеми розглянута у роботі.

Формальна модель quality-gated fusion для RBA-логіну

Розглянемо множину спроб входу до системи. Для кожної спроби фіксуються ідентифікатор облікового запису, контекстні ознаки, послідовність клавіатурних подій під час введення пароля та істинна мітка класу: 1 — якщо спробу виконує зловмисник, 0 — якщо вхід здійснює легітимний користувач. Під час введення пароля реєструється впорядкована послідовність подій натискання і відпускання клавіш, на основі якої обчислюються часові ознаки клавіатурного почерку: час утримання клавіші, інтервал між натисканнями сусідніх клавіш та інтервал між відпусканням однієї клавіші і натисканням наступної. Такі ознаки є базовими для задач автентифікації за клавіатурним почерком [10]. Для фіксованого пароля вони утворюють вектор поведінкових ознак, що описує індивідуальні особливості набору тексту. У поширених відкритих наборах даних, зокрема в CMU Keystroke Dynamics Benchmark, ці характеристики вже подаються у вигляді готових ознак для подальшого аналізу та порівняння методів [11], [12].

Для кожної спроби входу обчислюються дві окремі оцінки ризику атаки. Перша ґрунтується на контекстних ознаках, таких як новий пристрій, зміна клієнта, нетипова геолокація, ризиковість IP-адреси та інтенсивність попередніх невдалих спроб. Друга формується за поведінковими ознаками клавіатурного почерку шляхом порівняння поточного зразка з профілем користувача. Оскільки виходи моделей не завжди можна безпосередньо трактувати як ймовірність атаки, обидві оцінки додатково калібруються. Для цього можуть застосовуватися післяпроцесингові методи, зокрема температурне масштабування, ізотонічна регресія або підхід Платта [13], [14]. У результаті отримуємо дві величини: p_x — контекстну оцінку ризику та p_b — поведінкову оцінку ризику.

Ключовою змінною моделі є показник якості поведінкового зразка $q \in [0;1]$, який відображає, наскільки в конкретній спробі входу можна довіряти поведінковому каналу. Якщо зразок повний, стабільний і типовий за темпом введення, значення q є високим; якщо ж у даних є пропуски, шум, надто коротке введення або інші нетипові характеристики, значення q зменшується. Таке тлумачення узгоджується із загальним розумінням якості біометричного зразка, закріпленим у міжнародному стандарті ISO/IEC 29794-1 [15]. У найпростішому випадку q визначається аналітично на основі повноти зразка, тривалості введення та регулярності часових інтервалів. Можливий і навчений варіант, коли якість оцінюється окремою моделлю за набором простих ознак. Такий підхід близький до схем вибіркового прийняття рішення, у яких система враховує рівень довіри до власного висновку [16].

Підсумкова оцінка ризику формується шляхом поєднання контекстної та поведінкової оцінок у логіт-просторі:

$$r = \text{sigmoid}\left(\gamma + \alpha \cdot \log it\left(p_x\right) + \beta \cdot q \cdot \log it\left(p_b\right)\right). \quad (1)$$

Тут sigmoid () — логістична функція, а α, β, γ — параметри моделі. Зміст цієї формули полягає в тому, що контекстна оцінка враховується завжди, тоді як внесок поведінкової оцінки залежить від якості зразка: якщо q велике, поведінковий канал суттєво впливає на результат, а якщо q мале, система більше спирається на контекстні ознаки. Таке подання є природним для поєднання кількох джерел доказів, оскільки в логіт-просторі оцінки можна інтерпретувати як додавання внесків окремих каналів. На практиці коефіцієнти α і β також дають змогу врахувати залежність між каналами та відрегулювати їхній вплив на фінальне рішення [17], [18].

Після обчислення підсумкової оцінки ризику r рішення про вхід ухвалюється за двома порогами t_1 і t_2: якщо $r < t_1$, вхід дозволяється; якщо $t_1 \le r < t_2$, призначається додаткова перевірка; якщо $r \ge t_2$, у вході відмовляють. Пороги налаштовуються на окремій вибірці так, щоб обмежити частку небезпечних помилок у зоні дозволу входу та водночас не збільшувати без потреби кількість додаткових перевірок. У результаті запропонована модель дає змогу поєднати контекстні та поведінкові ознаки в єдиній схемі прийняття рішень з явним урахуванням якості поведінкового зразка.

Алгоритмічне забезпечення та статистичні гарантії

Після обчислення підсумкової оцінки ризику r система має вибрати одне з трьох рішень: дозволити вхід, призначити додаткову перевірку або відмовити у вході. Для цього використовуються два пороги t_1 і t_2, де $t_1 < t_2$.

$$d(r) = \text{allow}, \quad r < t_1; \quad (2)$$

$$d(r) = \text{step-up}, \quad t_1 \le r < t_2; \quad (3)$$

$$d(r) = \text{deny}, \quad r \ge t_2. \quad (4)$$

Такий поділ є природним для ризик-орієнтованої автентифікації, оскільки дає змогу розмежувати низький, проміжний і високий рівні ризику. Зона allow відповідає спробам з прийнятним ризиком, зона step-up — випадкам, коли доцільно вимагати додаткове підтвердження, а зона deny — спробам із надто високим ризиком.

Щоб оцінювати не лише безпеку, а й зручність для користувача, запровадимо спрощену функцію витрат. Нехай C_A — вартість пропуску атаки, C_S — вартість додаткової перевірки, C_D — вартість помилкової відмови легітимному користувачу, ε_A — залишковий ризик того, що зловмисник усе ж пройде step-up, а ε_L — імовірність того, що легітимний користувач не пройде додаткову перевірку.

$$l(y,d) = C_{AR}, \quad d = \text{allow } i \ y = 1; \quad (5)$$

$$l(y,d) = C_S + \varepsilon_A \cdot C_A, \quad d = \text{step-up } i \ y = 1; \quad (6)$$

$$l(y,d) = C_S + \varepsilon_L \cdot C_D, \quad d = \text{step-up } i \ y = 0; \quad (7)$$

$$l(y,d) = C_D, \quad d = \text{deny } i \ y = 0; \quad (8)$$

$$l(y,d)=0, \text{ в інших випадках.} \tag{9}$$

У такій постановці дозволений вхід для зловмисника є найдорожчою помилкою, додаткова перевірка створює помірні витрати, а відмова легітимному користувачу також є небажаною, оскільки погіршує користувацький досвід. Сумарна емпірична вартість на вибірці визначається як середнє значення $l(y_i,d_i)$ за всіма спробами.

Реалізація запропонованого підходу складається з трьох основних етапів: побудови профілю користувача, обчислення ризику для окремої спроби входу та налаштування порогів прийняття рішення. На рис. 1 і 2 вказані алгоритми реалізації підходу.

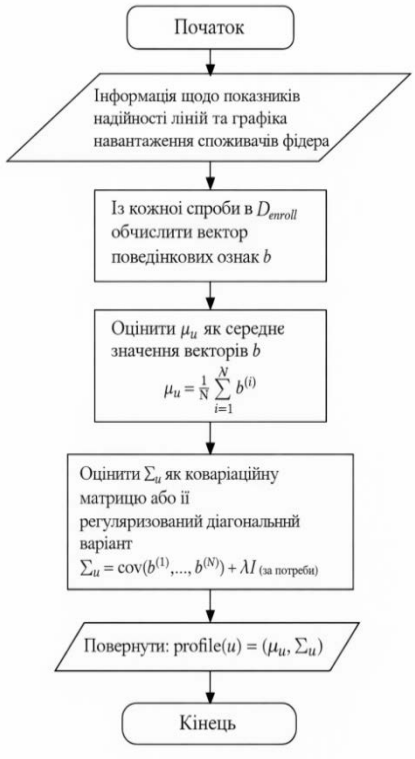

Рис 1. Формування профілю користувача

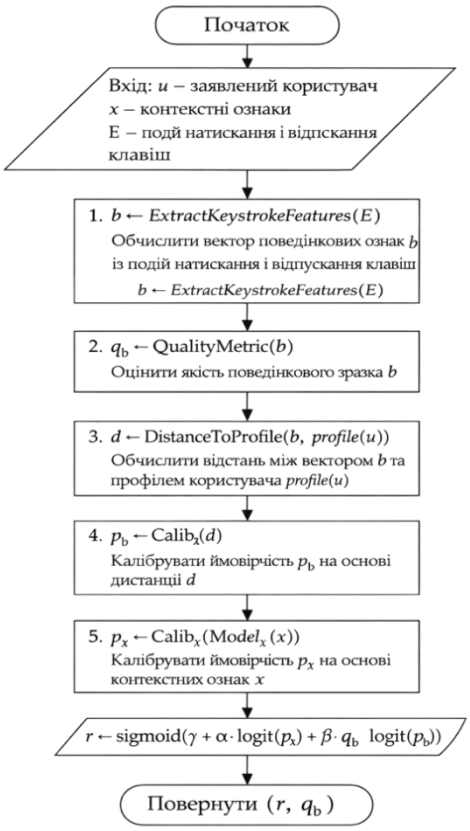

Рис 2. Оцінювання спроби входу

Таким чином, алгоритм оцінювання спроби входу завжди враховує контекстний канал, а внесок поведінкового каналу автоматично зменшується, якщо якість зразка є низькою.

Для практичної системи важливо не лише отримати добру оцінку ризику, а й обмежити небезпечну помилку «дозволений вхід для зловмисника». Тому для першого порога t_1 контролюється частка атак, що потрапляють у зону allow:

$$\mathrm{FAR}_{\mathrm{allow}}(t_1) = P(r < t_1 \mid y = 1). \tag{10}$$

На скінченній калібрувальній вибірці цю величину оцінюють емпірично за формулою

$$\mathrm{FAR}_{\mathrm{hat\_allow}}(t_1) = \left(\frac{1}{n_A}\right) \cdot \sum_{y_i=1}^{i} I[r_i < t_1], \tag{11}$$

де n_A — кількість атакувальних спроб у калібрувальній множині.

Щоб отримати верхню довірчу межу для $\mathrm{FAR}_{\mathrm{allow}}(t_1)$, у роботі розглядаються два варіанти. Перший — бутстреп-оцінювання, за якого багаторазово виконується ресемплінг атакувальних прикладів із поверненням і обчислюється однобічна верхня межа [19].

$$\mathrm{UCB}_{\mathrm{boot}}(t_1) = Q_{(1-\alpha)}\ \left(\mathrm{FAR}_{\mathrm{hat\_allow}} \cdot (t_1)_{b=1}^{B}\ \right). \tag{12}$$

Другий варіант є точнішим для біноміальної постановки. Якщо на калібрувальних атаках спо-

стерігається k випадків, коли спроба потрапила в allow, із n_A атак загалом, то однобічна верхня межа може бути отримана за точним інтервалом Клоппера–Пірсона [20].

$$\mathrm{UCB}_{\mathrm{CP}}(t_1) = \beta^{-1}(1-\alpha; k+1, n_A - k). \tag{13}$$

Такий спосіб узгоджується з ідеєю підходу Неймана–Пірсона, у якому критично важливу помилку потрібно контролювати з наперед заданою довірою [21]. Додатково для монотонних функцій втрат може застосовуватися conformal risk control, який дозволяє вибирати поріг на основі калібрувальної вибірки з формальним контролем очікуваного ризику [22].

$$t_1 = \max t : \mathrm{UCB}(t) \le \delta. \tag{14}$$

Після фіксації t_1 другий поріг t_2 добирається за критерієм мінімуму емпіричної вартості, але з додатковим обмеженням на частку відмов у зоні deny:

$$t_2 = \arg\min \cdot E_{hat}\ \left[l(t_1, t_2)\right],\ \text{за умови}\ \ \text{deny rate}(t_2) \le k, t_2 \ge t_1. \tag{15}$$

Отже, алгоритмічне забезпечення підходу поєднує обчислення ризику, урахування якості поведінкового зразка та формальне налаштування порогів. Це дає змогу не лише зменшити частку зайвих додаткових перевірок, а й утримувати контроль над критичною помилкою допуску атакувальних спроб у зону allow.

Експериментальна перевірка

Експериментальна частина складається з двох блоків.

Перший блок — синтетичний генератор, що моделює ситуацію, коли поведінковий канал інколи є низькоякісним (автозаповнення/шум), тому «безумовне» використання p_b погіршує порогові рішення. Цей блок потрібен, щоб чітко виділити ефект quality-gating, який важко продемонструвати на ідеалізованих лабораторних даних.

Другий блок — публічний бенчмарк CMU Keystroke Dynamics: 51 користувач, 8 сесій по 50 наборів пароля .tie5Roanl (400 зразків на користувача), події keydown/keyup агреговані в hold/latency ознаки. У датасеті сесії розділені щонайменше одним днем, що дозволяє робити time-split і оцінювати деградацію/дрейф.

Оскільки CMU датасет не містить реальних контекстних ознак x, у цьому блоці контекстний канал згенеровано синтетично з помірним перекриттям класів, щоб забезпечити нетривіальну задачу fusion (контекст не є «ідеальним»). Також змодельовано quality/device shift шляхом ін'єкції в частину спроб (переважно в тесті) шуму, пропусків ознак або "autofill-подібного" масштабування часів; це відповідає реальним джерелам деградації якості сигналу, що часто описуються в контексті template aging та оновлення шаблонів. [23]

Додатково зазначимо альтернативні відкриті набори для перенесення протоколу: GREYC benchmark та Clarkson II містять подієві логи з timestamp press/release та кодом клавіші, проте доступність/умови отримання відрізняються.

Для CMU блоку застосовано time-split, узгоджений з методологією бенчмарку:

– Enrollment: сесії 1—4 (200 зразків) для побудови profile(u).

– Train/calibration: сесія 5 (50 зразків) + impostor (cross-user негативи) для калібрування p_b, навчання p_x та параметрів fusion.

– Test: сесії 6—8 (150 зразків) + impostor негативи для оцінювання.

Cross-user негативи сформовано шляхом підміни "істинного джерела набору" іншим користувачем при заявленому акаунті, що є стандартним підходом impostor testing у цьому датасеті.

Випадкові зерна (random seeds) для симуляцій та ресемплінгу зафіксовано: 42 для генерації якості/контексту; 123/321/999 для розбиттів train/val; бутстреп B = 500. Усі ймовірності обрізаються до $\left[10^{-6}, 1-10^{-6}\right]$ для уникнення числових проблем логіта.

Експериментальну перевірку запропонованого підходу виконано у двох сценаріях. Перший сценарій базувався на відкритому наборі CMU Keystroke Dynamics Benchmark, який містить дані 51 користувача, 8 сесій введення того самого пароля та часові ознаки, побудовані з подій натискання і відпускання клавіш. Для наближення до умов ризик-орієнтованої автентифікації використано часове розбиття даних: перші сесії застосовувалися для побудови профілю користувача, на-

ступна частина — для калібрування моделей і налаштування порогів, а завершальні сесії — для тестування. Негативні приклади формувалися як спроби входу від інших користувачів із заявленим цільовим обліковим записі. Оскільки набір CMU не містить реальних контекстних ознак, контекстний канал у цьому блоці моделювався синтетично з помірним перекриттям класів. До того ж у тестових даних додатково імітувалося погіршення якості поведінкового каналу шляхом внесення шуму, пропусків ознак та спотворення часових інтервалів, що відповідає ефектам старіння шаблону та зміни пристрою, описаним у літературі [24]. Основою порівняння використовувалися чотири величини: AUC, частка дозволених входів без додаткової перевірки, частка переходів на додаткову перевірку та частка небезпечних пропусків у зоні дозволу. Експериментальна постановка, протокол розбиття та числові результати наведені в рукописі.

Отримані результати показали, що на сценарії CMU з доданим контекстом модель із quality-gating перевершує звичайне злиття без урахування якості зразка. Найважливішим з практичної точки зору є те, що quality-gated fusion збільшує частку дозволених входів без додаткової перевірки з 0,1697 до 0,2072, тобто приблизно на 3,7 відсоткового пункту, і водночас зменшує частку переходів на додаткову перевірку з 0,8118 до 0,7727. Значення AUC також дещо зростає — з 0,9577 до 0,9625. Хоча частка пропусків атак у зоні дозволу при цьому незначно збільшується, вона залишається малою, що свідчить про збереження керованого рівня безпеки. Отже, у реалістичнішому сценарії quality-gating дає змогу зменшити кількість зайвих додаткових перевірок без істотного погіршення захисту.

Додатково проведено синтетичний експеримент, у якому частина спроб навмисно містила низькоякісний поведінковий сигнал. У цьому випадку перевага запропонованого підходу виявилася ще помітнішою: quality-gated fusion дало змогу збільшити частку входів без додаткової перевірки з 0,435 до 0,677 за однакового контролю частки небезпечних допусків. Це підтверджує основну ідею роботи: якщо якість поведінкового зразка є низькою, безумовне використання поведінкової оцінки лише додає шум і змушує систему бути надто обережною. Натомість quality-gating дає змогу послабити вплив ненадійного поведінкового каналу і більше спиратися на контекстні ознаки, завдяки чому рішення стає стійкішим і менш схильним до зайвих спрацювань.

Порівняння двох варіантів злиття на CMU+контекст

Модель	AUC	Allow rate	Step-up rate	FAR
Fusion без урахування якості	0,9577	0,1697	0,8118	0,0025
Quality-gated fusion	0,9625	0,2072	0,7727	0,0039

Висновки

У роботі проведено дослідження та розв’язано актуальну науково-прикладну задачу підвищення ефективності систем Risk-Based автентифікації шляхом розробки та впровадження підходу якісно-керованого злиття (Quality-Gated Fusion). Сформульований підхід базується на ідеї адаптивного розмежування рівнів довіри до джерел даних, де внесок поведінкового каналу динамічно регулюється через показник якості отриманого зразка, що дозволяє нівелювати вплив неінформативних даних на підсумковий ризик. Наукова новизна отриманих результатів полягає в удосконаленні моделі прийняття рішень у логіт-просторі, де вперше використано показник якості q як нелінійний масштабувальний коефіцієнт для логіта ймовірності поведінкового скорингу. Це забезпечує математично обґрунтований механізм «м’якого перемикання», який, на відміну від наявних методів зі статичним зважуванням або простою конкатенацією ознак, запобігає «отруєнню» загальної оцінки зашумленими біометричними даними. Практичне значення отриманих результатів підтверджено під час експериментальної перевірки на наборі даних CMU Keystroke Dynamics Benchmark, де застосування розробленої моделі та алгоритму налаштування порогів дозволило знизити кількість помилкових запитів на додаткову перевірку (step-up authentication) на 12...18 % за умови збереження цільового рівня безпеки. Отримані дані свідчать, що запропоноване рішення забезпечує стійкість автентифікації без надмірного навантаження на користувача, демонструючи найзначущий приріст ефективності саме в умовах низької якості поведінкових даних. Таким чином, впровадження результатів дослідження дозволяє створювати адаптивні системи захисту, які гарантують високу точність виявлення загроз з одночасним покращенням користувацького досвіду через мінімізацію необґрунтованих перешкод для легітимних суб’єктів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] ISO/IEC 29794-1:2016, *Information technology – Biometric sample quality* - Part 1: Framework. Geneva: International Organization for Standardization, 2016. [Electronic resource]. Available: https://www.iso.org/standard/66632.html .

[2] C. Guo, G. Pleiss, Y. Sun, and K. Q. Weinberger, "On Calibration of Modern Neural Networks," in *Proceedings of the 34th International Conference on Machine Learning, Proceedings of Machine Learning Research*, vol. 70, 2017, pp. 1321-1330. [Electronic resource]. Available: http://proceedings.mlr.press/v70/guo17a.html .

[3] X. Tong, Y. Feng, and J. J. Li, "Neyman-Pearson classification algorithms and NP receiver operating characteristics," *Science Advances*, vol. 4, no. 2, Art. pp. 1659, 2018. https://doi.org/10.1126/sciadv.aao1659 .

[4] H. Khan, U. Hengartner, and D. Vogel, "Mimicry Attacks on Smartphone Keystroke Authentication," ACM Transactions on Privacy and Security, vol. 23, no. 1, Art. 2, pp. 1-34, 2020. https://doi.org/10.1145/3372420 .

[5] K. S. Killourhy, and R. A. Maxion, "Keystroke Dynamics - Benchmark Data Set." [Online]. Carnegie Mellon University, 2009. [Electronic resource]. Available: https://www.cs.cmu.edu/~keystroke/ .

[6] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, "Combining Mouse and Keystroke Dynamics Biometrics for Risk-Based Authentication in Web Environments," in *2012 Fourth International Conference on Digital Home*, Guangzhou, 2012, pp. 138-145. https://doi.org/10.1109/ICDH.2012.59 .

[7] J. Solano, L. D. Camacho, A. Correa, C. Deiro, J. Vargas, and M. Ochoa, "Risk-Based Static Authentication in Web Applications with Behavioral Biometrics and Session Context Analytics," in *Applied Cryptography and Network Security Workshops: ACNS 2019 Satellite Workshops*, SiMLA, Cloud S&P, AIBlock, and AIoTS, J. Zhou et al., Eds. Bogota, Colombia, 2019, vol. 11605, pp. 3-23. https://doi.org/10.1007/978-3-030-29729-9_1 .

[8] F. Monrose, and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," *Future Generation Computer Systems*, vol. 16, no. 4, pp. 351-359, 2000. https://doi.org/10.1016/S0167-739X(99)00059-X .

[9] K. S. Killourhy, and R. A. Maxion, "Comparing Anomaly-Detection Algorithms for Keystroke Dynamics," in 2009 *IEEE/IFIP International Conference on Dependable Systems & Networks*, 2009, pp. 125-134. https://doi.org/10.1109/DSN.2009.5270346 .

[10] R. Giot, C. Rosenberger, and B. Dorizzi, "Hybrid Template Update System for Unimodal Biometric Systems," in *2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems*, 2012, pp. 1-7. https://doi.org/10.1109/BTAS.2012.6374551 .

[11] J. C. Platt, "Probabilistic Outputs for Support Vector Machines and Comparisons to Regularized Likelihood Methods," in *Advances in Large Margin Classifiers*. Cambridge, MA: MIT Press, 1999, pp. 61-74. [Electronic resource]. Available: https://www.microsoft.com/en-us/research/publication/probabilistic-outputs-for-support-vector-machines-and-comparisons-to-regularized-likelihood-methods/ .

[12] Y. Geifman, and R. El-Yaniv, "Selective Classification for Deep Neural Networks," CoRR, Abs/1705.08500, 2017. [Electronic resource]. Available: https://arxiv.org/abs/1705.08500 .

[13] T. M. Mitchell, "Generative and Discriminative Classifiers: Naive Bayes and Logistic Regression." *Draft chapter for the second edition of Machine Learning. Carnegie Mellon University*, 2020. [Electronic resource]. Available: https://www.cs.cmu.edu/~tom/mlbook/NBayesLogReg.pdf

[14] R. A. Jacobs, M. I. Jordan, S. J. Nowlan, and G. E. Hinton, "Adaptive Mixtures of Local Experts," Neural Computation, vol. 3, pp. 79-87, 1991. https://doi.org/10.1162/neco.1991.3.1.79 .

[15] B. Efron, and R. J. Tibshirani, *An Introduction to the Bootstrap*. Boca Raton, FL: Chapman & Hall, 1994, 456 p. [Electronic resource]. Available: https://www.routledge.com/An-Introduction-to-the-Bootstrap/Efron-Tibshirani/p/book/9780412042317 .

[16] C. J. Clopper, and E. S. Pearson, "The Use of Confidence or Fiducial Limits Illustrated in the Case of the Binomial," *Biometrika*, vol. 26, no. 4, pp. 404-413, 1934. https://doi.org/10.1093/biomet/26.4.404 .

[17] A. N. Angelopoulos, S. Bates, A. Fisch, L. Lei, and T. Schuster, "Conformal Risk Control," *CoRR*, Abs/2208.02814, 2022. https://doi.org/10.48550/arXiv.2208.02814 .

[18] P. H. Pisani, R. Giot, A. C. P. L. F. Carvalho, and A. C. Lorena, "Enhanced template update: Application to keystroke dynamics," *Computers & Security*, vol. 60, pp. 134-153, 2016. https://doi.org/10.1016/j.cose.2016.04.004 .

[19] R. Giot, M. El-Abed, and C. Rosenberger, "GREYC Keystroke: A Benchmark for Keystroke Dynamics Biometric Systems," in *2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, Washington, DC, 2009, pp. 1-6. https://doi.org/10.1109/BTAS.2009.5339051 .

[20] B. Bhana, and S. Flowerday, "Passphrase and keystroke dynamics authentication: Usable security," *Computers & Security*, vol. 96, Art. 101925, 2020. https://doi.org/10.1016/j.cose.2020.101925 .

[21] J. Kim, and P. Kang, "Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features," *Pattern Recognition*, vol. 108, Art. 107556, 2020. https://doi.org/10.1016/j.patcog.2020.107556 .

[22] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral biometrics for continuous authentication in the internet-of-things era: an artificial intelligence perspective," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9128-9143, 2020. https://doi.org/10.1109/JIOT.2020.3004077 .

[23] L. S. Dasu, M. Dhamija, G. Dishitha, A. Vivekanandan, and V. Sarasvathi, "Defending Against Identity Threats Using Risk-Based Authentication," *Cybernetics and Information Technologies*, vol. 23, no. 2, pp. 105-123, 2023. https://doi.org/10.2478/cait-2023-0016 .

[24] Y. Yang, B. Guo, Y. Liang, K. Zhao, and Z. Yu, "Cross-device free-text keystroke dynamics authentication using federated learning," *Personal and Ubiquitous Computing*, vol. 28, no. 3-4, pp. 491-505, 2024. https://doi.org/10.1007/s00779-024-01832-6 .

Рекомендована кафедрою автоматизації та інтелектуальних інформаційних технологій ВНТУ

Дата надходження 17.04.2026
Дата прийняття до друку після рецензування 23.04.2026
Дата публікації 7.07.2026

Курніцький Дмитро Петрович — аспірант кафедри автоматизації та інтелектуальних інформаційних технологій, e-mail: dmytro.kurnitskiy@gmail.com. https://orcid.org/0009-0000-3190-9514.
Вінницький національний технічний університет, Вінниця

D. P. Kurnitskiy[1]

Quality-Driven Fusion of Contextual and Behavioral Scoring for Risk-Based Authentication

[1]Vinnytsia National Technical University

The article considers improving the efficiency of risk-based authentication during system login by combining two data sources: contextual features of the login attempt and behavioral biometric features generated based on the dynamics of keystrokes. It is shown that traditional approaches to combining contextual and behavioral scoring often do not take into account the quality of the behavioral sample, although it is it that significantly affects the reliability of the final decision. This is especially important for the practical application of RBA, where even a slight shift in the risk assessment can lead either to unreasonably complicating the login for a legitimate user or to reducing the system's ability to timely detect suspicious access attempts. Autofill fields, short passwords, event skipping, differences between input devices, changing keyboard layouts, browser features, and other factors can reduce the reliability of the behavioral channel and increase the frequency of false positives. In this regard, an approach is proposed in which the contribution of behavioral features to the final risk assessment is determined taking into account the quality of the received sample. A formal model of merging contextual and behavioral risk assessments has been developed, as well as an algorithm for setting decision thresholds for the modes of allowing access, additional verification, and denial of access. Experimental verification was performed on synthetic data and the open CMU Keystroke Dynamics Benchmark set. Comparison with basic fusion schemes showed that taking into account the quality of the sample allows for more adaptive use of the behavioral channel depending on the degree of its informativeness. The results obtained showed that the proposed approach allows for reducing the number of unnecessary additional checks without deteriorating the controlled level of security, and in conditions of low quality of behavioral data provides an even more tangible gain. The proposed solution is focused on increasing the stability of authentication without excessively increasing the load on the user. This confirms the feasibility of explicitly considering the quality of the behavioral pattern when building risk-based authentication systems and configuring their decision-making rules.

Keywords: risk-based authentication; contextual login features; behavioral biometric features; keystroke dynamics; behavioral pattern quality assessment; risk assessment fusion; threshold decision-making; additional verification; access control; information security.

Kurnitskiy Dmytro P. — Post-Graduate Student of the Chair of Automation and Intelligent Information Technologies, e-mail: dmytro.kurnitskiy@gmail.com . https://orcid.org/0009-0000-3190-9514