

АНАЛІЗ СУЧАСНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ НА ОСНОВІ ПОВЕДІНКОВИХ ХАРАКТЕРИСТИК І БІОМАРКЕРІВ

Шматко С.О., Чакрян В.Х., Андрушко Д.В.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: shmatko.sofiia@nure.ua
vadym.chakrian@nure.ua
dmytro.andrushko@nure.ua

Abstract

In the context of increasing cybersecurity threats, traditional authentication methods such as passwords and tokens are proving to be insufficient. This study presents a comparative analysis of modern authentication approaches based on behavioral characteristics and physiological biomarkers. Drawing upon ten peer-reviewed studies published between 2019 and 2024, we examine the effectiveness of various machine learning and deep learning algorithms, including Random Forest, Support Vector Machine (SVM), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM). Both unimodal and multimodal authentication systems are reviewed, with particular attention to mouse activity, keystroke dynamics, facial recognition, and EEG signals. Results indicate that ensemble models and deep neural networks achieve the highest accuracy up to 98% in multimodal contexts. Classical algorithms remain effective in low-resource environments. The findings suggest that combining behavioral and physiological data using hybrid methods can significantly enhance the robustness and usability of authentication systems.

Вступ

У сучасному цифровому середовищі традиційні методи автентифікації, як-от паролі та PIN-коди, дедалі частіше виявляються вразливими до фішингу, атак соціальної інженерії та компрометації даних. Це зумовлює зростаючий інтерес до альтернативних підходів, зокрема до автентифікації на основі поведінкових характеристик і фізіологічних біомаркерів. До таких ознак належать динаміка набору тексту, активність комп'ютерної миші (АКМ), голос, риси обличчя, електрокардіограма (ЕКГ), електроенцефалографія (ЕЕГ).

Завдяки розвитку методів машинного та глибокого навчання, обробка цих даних стала значно ефективнішою. Проте ефективність алгоритмів значною мірою залежить від типу ознак, умов збору та контексту використання. Це зумовлює потребу в системному аналізі наявних підходів і моделей.

Мета дослідження

Метою цієї роботи є здійснення огляду сучасних методів автентифікації користувачів на основі поведінкових характеристик та біомаркерів, які були описані у наукових публікаціях за період 2019–2024 років. Особливу увагу приділено аналізу використовуваних алгоритмів машинного та глибокого навчання, їх ефективності в різних сценаріях та визначенню тих методів, які показали найкращі результати в контексті реального застосування.

Методологія

Для реалізації поставленої мети було відібрано 10 наукових статей українською та англійською мовами, опублікованих у період з 2019 по 2024 роки. Основними критеріями для відбору джерел були: наявність експериментальної перевірки, застосування машинного навчання або глибокого навчання, та надання результатів точності, повноти або F1-міри. Розглядалися як поведінкові (динаміка натискання клавіш, мишкова активність, мобільна поведінка), так і фізіологічні біометричні

ознаки (голос, риси обличчя, ЕКГ, ЕЕГ). Після систематизації джерел було проведено якісний порівняльний аналіз використовуваних алгоритмів.

Аналіз методів

У проаналізованих роботах застосовувалися як класичні методи машинного навчання – наприклад, метод опорних векторів (Support Vector Machine, SVM), алгоритм випадкового лісу (Random Forest), метод k-найближчих сусідів, – так і глибокі нейронні мережі: згорткові нейронні мережі (Convolutional Neural Network, CNN), довгострокова короткочасна пам'ять (Long Short-Term Memory, LSTM), а також автоенкодера.

У дослідженні [1] вивчалася динаміка натискання клавіш із використанням Random Forest; точність моделі перевищувала 95%. У статті [2] мобільна поведінка аналізувалася за допомогою SVM, що дало близько 91% точності. У публікації [3] CNN застосовувалися для розпізнавання зображень обличчя і досягли 97% точності. У статті [4] використано LSTM для аналізу мобільної біометрії (жести, натискання, рухи) – результат становив 94%.

У роботі [5] автоенкодера використовувалися для виявлення відхилень у звичній поведінці користувача в режимі реального часу, і точність моделі досягала 92%. Щодо українських досліджень, у [6] була запропонована мультимодальна система автентифікації, що включала АКМ, динаміку клавіш і голос. При застосуванні ансамблевого підходу (Random Forest + XGBoost) система досягла 98% точності [6]. У дослідженні [7] аналіз АКМ за допомогою методу k-найближчих сусідів забезпечив точність 89%.

Порівняльний аналіз результатів

Результати аналізу демонструють, що глибокі нейронні мережі, зокрема CNN і LSTM, показують найвищу точність (94–97%) при роботі з біометричними ознаками – обличчя, ЕКГ, ЕЕГ [3; 4]. Вони здатні обробляти просторово-часові патерни, проте потребують великих обсягів даних і ресурсів, що обмежує їх застосування в системах із невисокою обчислювальною потужністю.

Класичні алгоритми, такі як SVM, Random Forest і метод k-найближчих сусідів, продемонстрували стабільні результати – точність 89–95% [1; 2; 7]. Їх переваги – невисокі вимоги до даних, швидке навчання, простота реалізації. Вони добре працюють із такими типами даних, як динаміка клавіш і АКМ, що часто зустрічаються в практичних додатках.

Ансамблеві методи (наприклад, поєднання Random Forest і XGBoost) виявилися найточнішими (до 98%) у мультимодальних системах, де використовується кілька типів біометричних ознак [6]. Їх ефективність пояснюється тим, що слабкі сторони однієї моделі можуть бути компенсовані перевагами іншої.

Також варто відзначити потенціал автоенкодерів [5] – хоча вони рідше використовуються для первинної автентифікації, вони ідеально підходять для безперервного контролю та виявлення підозрілих змін у поведінці користувача, що важливо для забезпечення стійкості системи до компрометації.

Висновки

Методи машинного та глибокого навчання мають значний потенціал у сфері біометричної та поведінкової автентифікації. Глибокі моделі є найефективнішими у випадках, коли доступна велика кількість даних і обчислювальні ресурси, а класичні алгоритми краще підходять для систем з обмеженим функціоналом.

Найбільш перспективними залишаються мультимодальні підходи, які комбінують різні джерела даних, а також ансамблеві моделі, здатні забезпечити баланс між точністю, швидкістю та надійністю. Важливою тенденцією є також розвиток безперервної автентифікації – зокрема на основі АКМ або інших поведінкових сигналів.

Література

1. Jain R., Gupta A., Sharma V. Keystroke dynamics authentication using Random Forest // Journal of Cybersecurity. 2021. Vol. 7, № 2. P. 115–122. DOI: <https://doi.org/10.1093/cybsec/tyaa023>.

2. Khan M., Asghar S., Hayat K., Ali S. Mobile behavioral biometrics using SVM // IEEE Access. 2020. Vol. 8. P. 196250–196260. DOI: <https://doi.org/10.1109/ACCESS.2020.3034465>.
3. Liu Y., Zhang H., Wu X. EEG-based biometric authentication via CNN // Pattern Recognition Letters. 2022. Vol. 155. P. 27–35. DOI: <https://doi.org/10.1016/j.patrec.2022.01.010>.
4. Singh P., Arora S., Gupta R. Deep learning in behavioral biometrics // Computers & Security. 2023. Vol. 124. Article № 102936. DOI: <https://doi.org/10.1016/j.cose.2022.102936>.
5. Lee S., Kim H., Choi J. Anomaly detection via autoencoders in user behavior // Neurocomputing. 2020. Vol. 417. P. 58–65. DOI: <https://doi.org/10.1016/j.neucom.2020.07.071>.
6. Іваненко Д. В. Мультимодальні методи автентифікації користувачів // Кібербезпека: наука і практика. 2023. № 2. С. 33–41.
7. Петренко Л. М. Мишкова активність як фактор автентифікації // Інформаційні технології і безпека. 2021. № 4. С. 25–30.
8. Zhang T., Li M., Wang Y. Voiceprint recognition with CNN-LSTM // Speech Communication. 2021. Vol. 131. P. 78–87. DOI: <https://doi.org/10.1016/j.specom.2021.07.004>.
9. Al-Bakri S., Liu X., Wu Z. Behavioral biometrics in cybersecurity: trends and challenges // Computers & Security. 2022. Vol. 114. Article № 102578. DOI: <https://doi.org/10.1016/j.cose.2021.102578>.
10. Діденко С. О. Аналіз точності методів біометричної автентифікації // Вісник НТУУ «КПІ». 2024. № 1. С. 49–54.