УДК 004.4
В. Ящук; Г. Цуприк, к. т. н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АРХІТЕКТУРНІ ПІДХОДИ ДО ПРОЄКТУВАННЯ ПРОГРАМНИХ СИСТЕМ ДЛЯ БЕЗПЕЧНОГО КЕРУВАННЯ АВТЕНТИФІКАЦІЙНИМИ ДАНИМИ

UDC 004.4
V. Yashchuk; H. Tsupryk, PhD., Assoc. Prof.

ARCHITECTURAL APPROACHES TO DESIGNING SOFTWARE SYSTEMS FOR SECURE MANAGEMENT OF AUTHENTICATION DATA

У сучасних умовах розвитку цифрових технологій питання безпечного керування автентифікаційними даними стає особливо актуальним. Значне зростання кількості кібератак, пов'язаних із компрометацією користувацьких паролів, підкреслює необхідність створення систем, які забезпечують високий рівень захисту та надійності [1]. Дослідження у сфері програмної інженерії та прикладної криптографії демонструють, що більшість порушень безпеки виникає через недоліки архітектури та слабкі механізми перевірки автентифікаційних даних [2].

Архітектура програмних систем для керування автентифікаційними даними включає низку компонентів, що забезпечують зберігання, обробку та перевірку паролів у захищеному середовищі. Одним із ключових елементів є модуль шифрування, який відповідає за криптографічні перетворення даних. Сучасні підходи передбачають використання симетричних алгоритмів AES, а також асиметричних алгоритмів для розмежування прав доступу [3]. Застосування надійних алгоритмів дозволяє суттєво зменшити ризики несанкціонованого доступу навіть у випадку часткової компрометації системи.

Модуль зберігання автентифікаційних даних базується на зашифрованих сховищах, які унеможливлюють доступ до інформації у відкритому вигляді. Особлива увага приділяється структурі сховища, яка повинна бути оптимізована для швидкого доступу до записів та захищена від атак на метадані. У сучасних дослідженнях підкреслюється, що добре структурована архітектура програмної системи дозволяє мінімізувати площину атаки та зменшити вплив внутрішньої складності на загальну стійкість до загроз [4].

Дослідження трансформерних моделей у контексті Industry 4.0 демонструють їх здатність адаптивно працювати з великими потоками даних, що може бути використано й для оптимізації процесів обробки автентифікаційної інформації [5].

Надзвичайно важливим компонентом архітектури є модуль виявлення слабких та скомпрометованих паролів. Серед сучасних методів особливе місце займає фільтр Блума – ймовірнісна структура даних, що дозволяє ефективно визначати належність пароля до великої множини хешів з мінімальними ресурсними витратами [6]. Перевагою цього підходу є можливість локальної перевірки без передавання даних на сторонні сервери, що значно підвищує рівень конфіденційності. Показано, що моделі Transformer можуть ефективно виявляти структурні залежності та витягувати патерни зі складних неструктурованих даних, що робить їх перспективними для аналізу поведінкових характеристик користувачів у системах автентифікації [7].

Сучасні програмні системи для керування автентифікаційними даними також включають інструменти генерації надійних паролів, системи контролю повторного використання, механізми моніторингу спроб доступу та захисту від автоматизованих атак. Поєднання цих механізмів у рамках єдиної архітектури сприяє підвищенню рівня безпеки користувачів та зменшенню ризиків витоку інформації. У роботах, присвячених data mining, підкреслюється, що трансформерні моделі здатні забезпечувати високу якість аналізу великих масивів даних, що є важливим для локальних систем перевірки автентифікації без значного навантаження на мережеву інфраструктуру [8].

Перспективи розвитку таких систем пов’язані з інтеграцією адаптивних алгоритмів машинного навчання, здатних аналізувати поведінкові характеристики користувача, а також з розширенням можливостей локальної обробки великих наборів даних. Використання цих технологій дозволить підвищити точність виявлення небезпечних дій, оптимізувати процес автентифікації та зменшити навантаження на центральні сервери [9].

Практичні результати застосування LLM-моделей свідчать про їх здатність виконувати обробку чутливих даних локально, забезпечуючи точне вилучення релевантних ознак, що може бути корисним для автономних модулів автентифікації [10].

Таким чином, архітектурні підходи до проєктування систем керування автентифікаційними даними відіграють важливу роль у забезпеченні загальної безпеки інформаційних систем. Використання поєднання криптографічних алгоритмів, структур даних та модульних архітектурних рішень дає змогу створювати ефективні, стійкі та масштабовані програмні засоби, здатні протидіяти сучасним кіберзагрозам.

Література

1. Verizon. Data Breach Investigations Report 2023. Verizon Enterprise Solutions, 2023. URL: https://www.verizon.com/business/resources/reports/dbir/
2. National Institute of Standards and Technology. NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management. U.S. Department of Commerce, 2017 (update 2023). URL: https://pages.nist.gov/800-63-3/sp800-63b.html
3. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson, 2023. С. 157–160.
4. Anderson R. Security Engineering. 3rd ed. Wiley, 2020. С. 118.
5. Олянін, Д., Цуприк, Г. (2025) Transformer Neural Networks in Industry 4.0 / Д. Олянін, Г. Цуприк, Т. Говорущенко, О. Багрій-Заяць, І. Андрущак // Computer Information Technologies in Industry 4.0: proceedings of the 3rd International Workshop (CITI-2025), Ternopil, Ukraine, 11–12 June 2025. – Ternopil : Ternopil Ivan Puluj National Technical University, 2025 (Scopus).
6. Ke Y., Liang Y., Sha Z., Shi Z., Song Z. DPBloomfilter: Securing Bloom Filters with Differential Privacy. arXiv, 2025. URL: https://arxiv.org/abs/2502.00693
7. Tsupryk, H., Olianin, D. (2025). Vydobuvannia danyh z tekstu vykorystovuiuchy transformerni neironni merezhi [Data extraction from text using Transformer Neural Networks]. Information Technology: Computer Science, Software Engineering and Cyber Security, 125–130, DOI: https://doi.org/10.32782/IT/2025-2-13
8. Tsupryk, H., Olianin, D. (2025). Overview of transformers role indata mining from unstructured data. International Scientific-technical journal «Measuring and computing devices in technological processes» 2025, Issue 2, 125–130, DOI: https://doi.org/10.31891/2219-9365-2025-82-52
9. Naldi M., Flamini M. Cybersecurity and behavioral authentication models. Journal of Information Security, 2023.
10. Tsupryk H. LLM-based Extraction from Resumes / D. Olianin, H. Tsupryk // Advanced Technologies in Scientific Research: collection of scientific papers with proceedings of the 1st International Scientific and Practical Conference, Rotterdam, Netherlands, 20–22 August 2025. – International Scientific Unity, 2025. – 72–76.