Модуль інкапсуляції ключів відповідає за шифрування згенерованого сеансового ключа отриманим від сервера відкритим ключем RSA.

Емулятор подій СКД генерує тестові послідовності даних, що імітують зчитування RFID-карток (наприклад, UID картки у форматі HEX) або спрацьовування датчиків проходу.

Мережевий клієнт забезпечує встановлення з'єднання із сервером та двосторонню маршрутизацію пакетів.

Взаємодія між контролером та сервером відбувається за строго визначеним протоколом, який складається з фази встановлення захищеного з'єднання та фази захищеного обміну даними, контролер ініціює TCP-з'єднання з сервером. Сервер приймає з'єднання і виділяє для нього окремий сокет [2].

Формування чіткого переліку функціональних вимог дозволяє визначити архітектурні межі системи, необхідні програмні модулі та механізми забезпечення конфіденційності, цілісності та автентичності інформаційного обміну між апаратними контролерами та центральним сервером.

1. Yevseiev, S. Modeling of security systems for critical infrastructure facilities : monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych [et al.]. – Kharkiv : PC TECHNOLOGY CENTER, 2022. – 196 p
2. Rashid, N. N. A Comprehensive Framework for Harnessing IoT and 5G for Enhanced Disaster Response / N. N. Rashid, Z. Ghanim Ali, A. Hussein Ali, N. Adnan Taher, S. Khdhaer Mukhlif, I. V. Muliar, H. Muthanna Noori // Proceeding of the 36th Conference of FRUCT Association. – 2024. – P. 655–663. – ISSN 2305-7254.

Інтеграція приватного блокчейну та сліпих підписів Чаума для забезпечення анонімності й цілісності збору даних у платформі OwlView

УДК 004.056.55 (043.2)

Анастасія Начинка[1], Валерій Трушевський[2]

Львівський національний університет імені Івана Франка,
[1]anastasiia.nachynka@lnu.edu.ua, [2]valeriy.trushevskyy@lnu.edu.ua

Платформи онлайн-опитувань акумулюють дані спеціальних категорій (ст. 9 GDPR) [4]: політичні погляди, релігія, здоров'я. Провідні сервіси (Google Forms, SurveyMonkey, Typeform) не забезпечують ані шифрування на рівні полів (field-level encryption), ані криптографічної перевірки цілісності відповідей. Виникає суперечність між необхідністю ідентифікації респондента для запобігання повторному голосуванню та забезпеченням приватності.

Мета роботи — спроєктувати й реалізувати у складі OwlView підсистему збору відповідей, що одночасно гарантує: 1) анонімність респондента; 2) неможливість повторного голосування; 3) перевірену цілісність агрегату; 4) індивідуальну верифікацію голосу без розкриття його змісту.

Наукова новизна — поєднання приватного блокчейну з консенсусом Proof-of-Work і деревами Меркла з протоколом сліпих підписів Чаума у єдиному

контурі, інтегрованому з ієрархічним KMS (MK→KEK→DEK) [3] та восьмирівневою RBAC. На відміну від [1, 2], схема дозволяє респонденту локально побудувати Merkle-квитанцію [5] для незалежної перевірки включення голосу без розкриття відповіді.

Розв'язок. Респондент засліплює авторизаційний токен m і надсилає $\tilde{m}$ серверу, який повертає $\tilde{\sigma}$; після зняття засліплення отримуємо валідний підпис σ за відкритим ключем сервера (1):

$$\tilde{m} = m \cdot r^{e} \bmod n; \quad \tilde{\sigma} = \tilde{m}^{d} \bmod n; \quad \sigma = \tilde{\sigma} \cdot r^{-1} \bmod n. \tag{1}$$

де (e, n) — публічний ключ сервера, d — приватний показник, r — випадковий фактор засліплення. Сервер не бачить m і не може зіставити підпис із користувачем. Зашифрована AES-256-GCM відповідь разом із σ потрапляє у пул транзакцій, з якого формується блок (2):

$$B = \langle idx, ts, hprev, rootM, nonce, \{txi\} \rangle, \tag{2}$$

де root_M — корінь дерева Меркла транзакцій блока. Респондент отримує квитанцію (3), яка за час O(log n) дозволяє переконатися у включенні голосу до підтвердженого блока:

$$receipt = \langle h(tx), \{hi\}, h(B) \rangle. \tag{3}$$

Серед провідних комерційних платформ (Google Forms, SurveyMonkey, Typeform) жодна не реалізує одночасно шифрування на рівні полів AES-256-GCM, ієрархічного KMS, сліпих підписів Чаума, Merkle-квитанції та блокчейн-аудиту — усі ці властивості одночасно забезпечує лише OwlView.

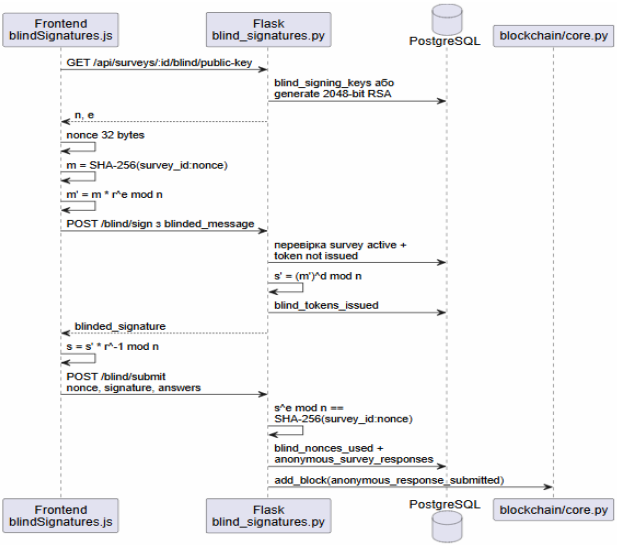

Рис. 1. Протокол сліпого підпису Чаума для анонімного голосування в OwlView

Реалізація. Підсистема — частина мікросервісної архітектури OwlView (12 Docker-контейнерів, Flask, React 18, PostgreSQL 15, Redis, Vault). Криптографія — на бібліотеках cryptography і pycryptodome; блокчейн і Merkle-перевірка — у back/blockchain. Працездатність підтверджена 312 автоматизованими тестами (167 pytest + 145 vitest, усі passed) та статичним аналізом SonarQube.

Реалізовано інтегрований механізм, який одночасно забезпечує анонімність респондента, неможливість повторного голосування, верифіковану цілісність агрегату й індивідуальну Merkle-перевірку голосу за O(log n). Схема відсутня у комерційних аналогах і відповідає ст. 25 GDPR «Privacy by Design». Перспективи — zk-SNARK і формальна верифікація в Tamarin Prover.

1. Chaum D. Blind Signatures for Untraceable Payments. Advances in Cryptology: Proceedings of CRYPTO ’82. New York: Plenum Press, 1983. P. 199–203.
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 10.05.2026).
3. Barker E. Recommendation for Key Management: Part 1 – General. NIST SP 800-57 Pt. 1, Rev. 5. Gaithersburg: NIST, 2020. 171 p.
4. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 (GDPR). Official Journal of the EU. 2016. L 119. P. 1–88.
5. Merkle R. C. A Digital Signature Based on a Conventional Encryption Function. Advances in Cryptology — CRYPTO’87. LNCS, vol. 293. Berlin: Springer, 1988. P. 369–378.

Аутентифікація користувача на основі тактильних параметрів динаміки натискань клавіш

УДК 004.056

Недвига Є.В., Сиропятов О.А.

Національний університет «Одеська політехніка», 10328108@stud.op.edu.ua, o.a.syropiatov@op.edu.ua

Вступ. Зростання кібератак (session hijacking, credential stuffing) виявило вразливість традиційних парольних механізмів та статичних методів біометрії. Безперервна поведінкова біометрія на основі динаміки натискань клавіш (keystroke dynamics) набуває значення. Класичні підходи із часовими характеристиками (dwell time, flight time) мають обмежену стійкість до імітації та replay-атак. Інтеграція тактильних параметрів (keystroke pressure, pressure profile) підвищує розрізнювальну здатність, оскільки силові показники менш підвладні свідомому контролю. Поширення сенсорних інтерфейсів (Force Touch, Android Pressure API) відкриває нові можливості для пасивної верифікації. Вимоги GDPR та Закону України «Про захист персональних даних» вимагають необоротних перетворень біометричних даних.

Мета роботи. Проєктування та програмна реалізація веб-застосунку для безперервної аутентифікації користувачів, що поєднує часові та тактильні параметри динаміки натискань з метою підвищення точності розпізнавання,