

«Методи організації безпеки даних під час автоматичних платежів»

Вінницький національний технічний університет

Анотація

Дана наукова стаття розглядає методи організації безпеки даних під час автоматичних платежів, які широко використовуються в підпискових сервісах та регулярних транзакціях. Особливу увагу приділено технічним методам забезпечення захисту даних, таким як токенизація, шифрування даних, двофакторна автентифікація та виявлення аномальних транзакцій за допомогою машинного навчання.

Ключові слова: автоматичні платежі, токенизація, шифрування, PCI DSS, 2FA, машинне навчання

Abstract

This scientific article examines methods for organizing data security during automatic payments, which are widely used in subscription services and regular transactions. Particular attention is paid to technical methods for ensuring data protection, such as tokenization, data encryption, two-factor authentication, and detection of anomalous transactions using machine learning.

Keywords: automatic payments, tokenization, encryption, PCI DSS, 2FA, machine learning

Вступ

Автоматичні платежі забезпечують зручність і автоматизацію фінансових операцій для мільйонів користувачів по всьому світу. Вони використовуються в різних сферах — від підписок на сервіси до регулярних рахунків за комунальні послуги. Однак, широке використання цієї технології вимагає дотримання високих стандартів захисту даних, оскільки будь-яка вразливість може призвести до значних фінансових і репутаційних втрат. У даній роботі розглядаються основні аспекти забезпечення захисту даних під час рекурентних платежів з технічної точки зору.

Основна частина

Автоматичні платежі — це періодичні транзакції, які автоматично списують кошти з рахунків клієнтів. Для цього використовується збережена інформація про платіжні картки, яка є надзвичайно чутливою. У зв'язку з цим розробка систем автоматичних платежів зобов'язана містити в собі безпечну передачу даних.

Однією з найважливіших вимог для захисту даних є відповідність стандарту PCI DSS (Payment Card Industry Data Security Standard). PCI DSS — це глобальний стандарт для всіх організацій, які зберігають, обробляють та передають дані платіжних карток або іншу конфіденційну інформацію, пов'язану з автентифікацією користувачів/платежів. Тобто будь-яка організація, яка приймає або опрацьовує платіжні картки, повинна проходити сертифікацію на відповідність загальноприйнятим вимогам індустрії.

Сам стандарт — це досить об'ємний документ на понад 1000 сторінок. У ньому описані 300+ критеріїв відповідності, які стосуються різних аспектів інформаційної безпеки. Усі вони згруповані за 12 основними пунктами вимог, що зображені на рисунку 1 [1].

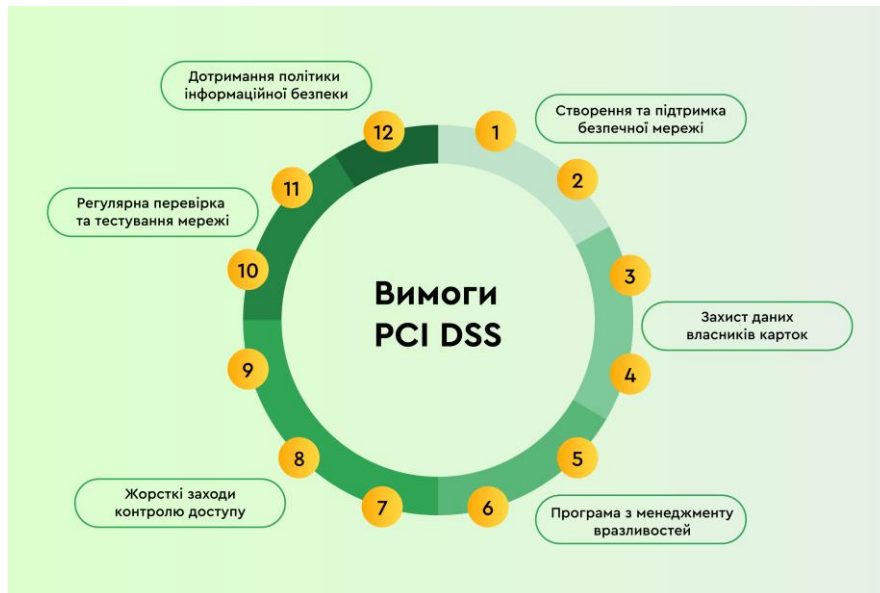


Рисунок 1 — Дванадцять основних пунктів вимог стандарту PCI DSS

Одним із методів дотримання стандартів є метод токенизації, що широко впроваджується для передачі платіжної інформації під час автоматичних списань. Цей процес полягає у заміні реальних реквізитів платіжної картки унікальними цифровими ключами, які називаються токенами. Використання таких ключів дозволяє значно підвищити рівень безпеки, мінімізуючи ризики компрометації даних.

Токени не містять жодної реальної платіжної інформації, тому їх неможливо застосувати поза межами конкретної транзакції. Наприклад, якщо цифровий ключ буде перехоплений під час передачі, зломисники не зможуть скористатися ним для інших платежів. Така властивість робить токенизацію одним із найнадійніших способів захисту даних.

Процес токенизації включає кілька етапів. Спочатку платіжні реквізити передаються до процесингового центру, який генерує унікальний токен. Реальна інформація зберігається на захищених серверах цього центру, тоді як цифровий ключ використовується для обробки подальших транзакцій. Такий підхід дозволяє уникнути зберігання чутливих даних на стороні продавця [2].

На жаль, слабкою стороною даного методу захисту даних є залежність від централізованих серверів, які зберігають відповідність між токенами та реальними даними. У разі компрометації цих серверів або токенизуючої системи вся система безпеки може бути під загрозою.

Окрім токенизації, яка забезпечує високий рівень безпеки платіжних даних, важливою складовою захисту є впровадження двофакторної автентифікації (2FA). Цей метод додає ще один рівень захисту, вимагаючи від користувачів підтверджувати свої фінансові операції через додатковий механізм, що робить несанкціонований доступ майже неможливим. Зазвичай 2FA реалізується за допомогою одноразового пароля (OTP), який генерується в реальному часі та надсилається на мобільний телефон або електронну пошту користувача [3].

Основна ідея двофакторної автентифікації полягає у використанні двох незалежних факторів для підтвердження особи. Перший фактор — це знання користувачем певної інформації (наприклад, пароля), а другий — це володіння чимось унікальним, як-от мобільним пристроєм для отримання OTP. Такий підхід забезпечує, що навіть у разі компрометації одного з факторів, зломисник не зможе завершити транзакцію без доступу до другого.

Однак цей метод має свої недоліки, які можуть вплинути на зручність і прийнятність для широкого застосування. Наприклад, для підтвердження транзакції або входу в обліковий запис користувачі часто повинні вводити одноразовий пароль, отриманий через SMS, електронну пошту або спеціальний додаток. Цей додатковий крок може створювати незручності, особливо коли користувачі не мають доступу до свого телефону або до мережі, необхідної для отримання пароля.

Крім того, якщо двофакторна автентифікація реалізована неналежним чином, вона може викликати складнощі у користувачів, наприклад, у разі затримки повідомлень з кодами або їх ненадходження взагалі.

Окрім двофакторної автентифікації, надзвичайно важливо впроваджувати шифрування, щоб гарантувати захист конфіденційної інформації під час її обробки та зберігання. Ця технологія перетворює дані у зашифрований формат, роблячи їх недоступними для злоумисників навіть у разі перехоплення.

Процес шифрування стартує з моменту, коли користувач вводить дані, і триває до завершення транзакції. Завдяки цьому створюється безпечний канал, який використовується для передачі інформації між учасниками транзакції, такими як клієнт, продавець і платіжна система. Реалізація цього процесу базується на сучасних технологіях, серед яких ключове місце займає протокол TLS (Transport Layer Security), що є загальноприйнятим стандартом для захищеної передачі через Інтернет[4].

Додатковим рівнем безпеки стає застосування алгоритму AES-256 (Advanced Encryption Standard). Цей метод, який належить до симетричних способів шифрування, використовує 256-бітний ключ, забезпечуючи надійний захист даних. Злам такого механізму надзвичайно складний навіть для сучасних обчислювальних ресурсів. Популярність AES-256 пояснюється його ефективністю, високою швидкістю роботи та універсальністю у фінансових і банківських системах.

Незважаючи на свою ефективність, вищеописаний метод вимагає значних обчислювальних ресурсів, особливо під час обробки великих обсягів даних. Це може впливати на швидкість транзакцій і створювати додаткові навантаження на сервери, що стає викликом для компаній, які обробляють значну кількість інформації в режимі реального часу. Тому впровадження шифрування потребує ретельного планування та оптимізації, щоб балансувати між високим рівнем безпеки та продуктивністю системи.

Шифрування є важливим інструментом для забезпечення конфіденційності даних, але воно не може повністю виключити ризики, пов'язані з шахрайством чи несанкціонованим використанням. Для додаткового захисту фінансових транзакцій активно використовуються алгоритми машинного навчання та штучного інтелекту, які спеціалізуються на аналізі поведінки користувачів і виявленні аномалій у їхніх діях. Такі системи є важливим доповненням до шифрування, оскільки дозволяють ідентифікувати підозрілі операції навіть у захищених мережах.

Алгоритми машинного навчання аналізують великі обсяги даних про транзакції, включаючи історію покупок, місцезнаходження, частоту операцій і звичну поведінку користувачів. На основі цього створюється профіль кожного клієнта, який стає еталоном для порівняння. Якщо система виявляє операцію, яка суттєво відхиляється від звичайної поведінки користувача, така транзакція позначається як підозріла.

Штучний інтелект, зокрема нейронні мережі, грає ключову роль у вдосконаленні цих систем. Вони можуть не лише ідентифікувати аномалії, але й передбачати потенційно ризиковані дії. Наприклад, якщо користувач зазвичай здійснює покупки лише у своїй країні, але раптово виконує велику транзакцію за кордоном, система може автоматично зупинити операцію для перевірки.

Такі системи часто інтегруються з механізмами реального часу, які миттєво блокують потенційно шахрайські операції [5]. Після цього користувач отримує сповіщення про проблему, і йому пропонується підтвердити або скасувати транзакцію. Це не лише знижує ризик фінансових втрат, але й підвищує довіру клієнтів до платіжного сервісу.

Ефективність алгоритмів машинного навчання значною мірою залежить від якості даних, на яких вони навчаються. Якщо вхідні дані є неповними, нерелевантними або містять помилки, система може генерувати хибнопозитивні або хибнонегативні результати. Це може призвести до блокування легітимних транзакцій або пропуску шахрайських дій, що впливає як на безпеку, так і на зручність користувачів.

Висновки

У роботі описано та проаналізовано ключові методи забезпечення безпеки даних у системах автоматичних платежів, кожен із яких має свої сильні сторони та обмеження. Токенізація ефективно замінює реальні платіжні реквізити унікальними токенами, що мінімізує ризик компрометації, хоча залежність від централізованих серверів залишається її слабкою стороною. Двофакторна автентифікація додає додатковий рівень захисту, однак інколи створює незручності через додаткові кроки підтвердження транзакції.

Шифрування забезпечує конфіденційність даних під час передачі та зберігання, але вимагає значних обчислювальних потужностей, що може впливати на швидкість обробки. Алгоритми машинного навчання дозволяють виявляти шахрайські операції навіть у складних сценаріях, проте їхня ефективність залежить від якості вхідних даних.

Оптимальним підходом до безпеки є інтеграція цих методів у комплексну систему, яка забезпечує багаторівневий захист. Це дозволяє не лише підвищити рівень безпеки, але й зміцнити довіру користувачів до платіжних сервісів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке сертифікація PCI DSS, і навіщо вона потрібна для приймання платежів [Електронний ресурс] / Interkassa – 2023. Режим доступу до ресурсу: <https://interkassa.com/blog/shcho-take-sertyfikatsiia-pci-dss>
2. Introduction to Tokenization [Електронний ресурс] / Microsoft. – 2023. Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/azure/security/fundamentals/tokenization>
3. What is Two-Factor Authentication and How Does It Work? [Електронний ресурс] / Kaspersky. – 2022. Режим доступу до ресурсу: <https://www.kaspersky.com/resource-center/definitions/what-is-2fa>
4. Guide to TLS Implementations [Електронний ресурс] / NIST. – 2021. Режим доступу до ресурсу: <https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final>
5. Machine Learning for Fraud Detection [Електронний ресурс] / IBM Security. – 2020. Режим доступу до ресурсу: <https://www.ibm.com/security/fraud-protection>

Дзюба Дар'я Анатоліївна – студентка групи 1KI-23м, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: dziuba.daria.anatolievna@gmail.com.

Томчук Микола Антонович – канд. техн. наук, доцент кафедри Безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: tomchuk@vntu.edu.ua.

Dziuba Daria A. – student of group 1KI – 23m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dziuba.daria.anatolievna@gmail.com.

Tomchuk Mykola A. – Cand. Sc. (Eng.), Assistant Professor of Life Safety and Pedagogy of Safety department, Vinnytsia National Technical University, Vinnytsia, e-mail: tomchuk@vntu.edu.ua.