

А. В. Грицак

Н.М. Марцун

Підвищення захищеності MQTT-комунікацій IoT-пристроїв на основі сертифікатів PKI, блокчейн-аудиту та електронного підписування для забезпечення цілісності

Вінницький національний технічний університет

Анотація. Робота присвячена розробці вдосконаленої моделі захисту MQTT-комунікацій у системах Інтернету речей. Запропонований підхід поєднує три ключові механізми: PKI-автентифікацію клієнтів, електронне підписування повідомлень та блокчейн-аудит подій. У роботі проведено аналіз сучасних загроз для IoT-інфраструктур, визначено основні вразливості MQTT-протоколу та розроблено алгоритм, що забезпечує цілісність, автентичність і невідмовність даних.

Ключові слова: MQTT, IoT, PKI, цифровий підпис, блокчейн, інформаційна безпека, цілісність даних.

Abstract. Thesis is devoted to the development of an enhanced security model for MQTT communications in Internet of Things (IoT) systems. The proposed approach integrates three core mechanisms: PKI-based client authentication, digital message signing, and blockchain event auditing. The study analyzes modern threats to IoT infrastructures, identifies key vulnerabilities of the MQTT protocol, and develops an algorithm that ensures data integrity, authenticity, and non-repudiation. The software implementation includes PKI authentication modules, digital signing and verification of MQTT messages, and a blockchain event log.

Keywords: MQTT, IoT, PKI, digital signature, blockchain, cybersecurity, data integrity.

Вступ

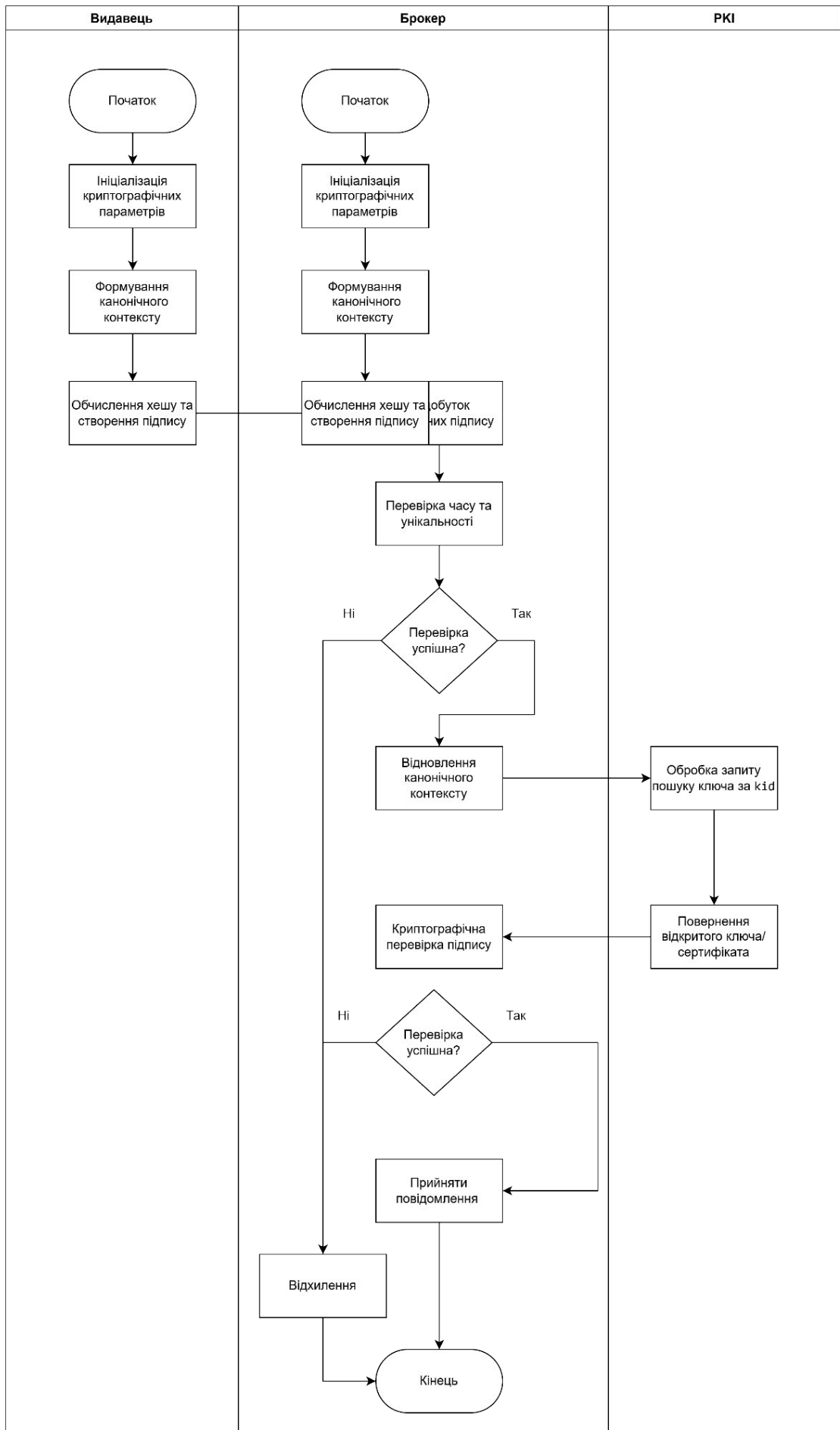
Стрімке зростання кількості IoT-пристроїв актуалізує проблему захисту комунікацій у розподілених системах. Протокол MQTT, який широко використовується для передачі телеметрії, не має вбудованих механізмів автентифікації та контролю цілісності, що створює значні ризики.

Результати дослідження

У межах розробленої моделі захисту MQTT-комунікацій ключовим елементом є механізм електронного підписування повідомлень, який забезпечує гарантовану цілісність даних, автентичність джерела та невідмовність від відправлення. На основі проведеного аналізу загроз встановлено, що саме модифікація повідомлень, інжекція підроблених пакетів та підміна пристроїв є одними з найбільш поширених атак на MQTT-інфраструктури. Тому інтеграція цифрового підпису стала необхідною складовою комплексної моделі захисту.

Розроблена діаграма електронного підписування відображає повний цикл обробки MQTT-повідомлення — від моменту його формування на пристрої-відправнику до перевірки підпису на стороні брокера та кінцевого отримувача. На етапі формування повідомлення пристрій генерує хеш вмісту за допомогою криптографічної хеш-функції SHA-256, після чого створює цифровий підпис із використанням приватного ключа, виданого в межах PKI-інфраструктури. Підпис додається до MQTT-пакета як службове поле, що дозволяє зберегти сумісність із існуючими брокерами та клієнтами.

На стороні брокера реалізовано механізм первинної перевірки підпису, який дозволяє одразу відхиляти повідомлення з некоректним або відсутнім підписом. Це не лише підвищує рівень безпеки, а й зменшує навантаження на кінцеві системи, оскільки недійсні повідомлення не передаються далі. Після цього брокер передає пакет отримувачам, які повторно виконують перевірку підпису, що забезпечує подвійний контроль цілісності та автентичності.



Розроблена діаграма враховує результати експериментального тестування, проведеного у програмній частині роботи. Зокрема, встановлено, що додавання операцій хешування та підписування збільшує затримку передачі лише на 5–7%, що є прийнятним для більшості IoT-сценаріїв. Тестування також підтвердило здатність системи виявляти спроби модифікації повідомлень, підміни пристроїв та повторного відтворення даних. Усі ці властивості були враховані під час формування логічної структури діаграми, яка відображає взаємодію між PKI-модулем, модулем цифрового підпису та блокчейн-журналом подій.

Особливу увагу приділено інтеграції механізму підписування з блокчейн-аудитом. Після успішної перевірки підпису брокер формує хеш транзакції та записує його у блокчейн-журнал, що забезпечує незмінність історії комунікацій. Таким чином, діаграма електронного підписування не лише описує процес забезпечення цілісності, а й демонструє взаємозв'язок між усіма компонентами комплексної моделі захисту.

Розроблена схема дозволяє забезпечити високий рівень довіри до даних у розподілених IoT-системах, мінімізувати ризики підміни пристроїв і спотворення повідомлень, а також створює основу для масштабованої та стійкої до атак архітектури MQTT-комунікацій. Її відповідність результатам експериментального тестування підтверджує практичну ефективність запропонованого підходу та можливість його інтеграції у реальні IoT-інфраструктури.

Висновки

У роботі розроблено вдосконалену модель захисту MQTT-комунікацій в системах Інтернету речей, що поєднує PKI-автентифікацію клієнтів, електронне підписування повідомлень та блокчейн-аудит подій. Проведений аналіз сучасних загроз MQTT підтвердив доцільність інтеграції криптографічних механізмів для забезпечення цілісності, автентичності та невідомості даних. Запропонована архітектура гарантує достовірність джерела даних, забезпечує цілісність повідомлень і неможливість їх непомітної модифікації, а також формує прозорий і незмінний журнал транзакцій, стійкий до маніпуляцій з історією комунікацій.

Програмна реалізація, що включає модулі PKI-автентифікації, цифрового підписування та блокчейн-журналу подій, показала в ході експериментів мінімальний вплив на продуктивність MQTT-комунікацій. Практичне значення роботи полягає в можливості застосування запропонованої моделі в корпоративних, промислових і критично важливих IoT-системах, де вона забезпечує високий рівень довіри до даних та захист від ключових типів атак. Унікальність роботи полягає у формалізації алгоритму взаємодії PKI, електронного підпису та блокчейн-аудиту в межах MQTT-протоколу з урахуванням обмежених ресурсів IoT-пристроїв, що дозволяє вийти за межі традиційних підходів, орієнтованих переважно на конфіденційність. Отримані результати підтверджують ефективність моделі та створюють основу для подальших досліджень, спрямованих на оптимізацію криптографічних алгоритмів і розвиток комплексних систем моніторингу та контролю доступу в IoT-інфраструктурах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Singh, S., & Gupta, P. (2025). *Unmasking Digital Deceptions: An Integrative Review of Deepfake Generation and Detection*. Journal of Digital Forensics, 12(2), 45–60.
2. Maurya, V., Rishiwal, V., Yadav, M., Shiblee, M., Yadav, P., & Agarwal, U. (2024). *Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions*. Peer-to-Peer Networking and Applications, 18(53).
3. Hsu, C., et al. (2024). *Designing a Secure and Scalable Service Model Using Blockchain and MQTT*. WACV 2024 Workshops.
4. Khordadpour, P., & Ahmadi, S. (2024). *Security and Privacy Enhancing in Blockchain-based IoT Environments via Anonymous Auditing*. arXiv preprint arXiv:2403.01356.
5. Zhang, Y., Ma, Z., & Meng, J. (2025). *Auditing in the Blockchain: A Literature Review*. Frontiers in Blockchain, 8.
6. *Cybersecurity for Blockchain-Based IoT Systems: A Review*. Applied Sciences, 13(13), 7432 (2025).
7. Zeghida, H., Boulaiche, M., & Chikh, R. (2025). *Security of MQTT Protocol: A Brief Overview*. CEUR Workshop Proceedings, Vol. 3973.

Марцун Назар Миколайович – студент групи КІТС-24м, факультет менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: martsun03@gmail.com

Науковий керівник: Грицак Анатолій Васильович – доцент каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: grytsak.a.v@gmail.com

Martsun Nazar M. – student of the KITS-24m group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: martsun03@gmail.com

Supervisor: Hrytsak Anatolii Vasyliovych – docent of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: grytsak.a.v@gmail.com