Архітектура самосуверенних цифрових двійників для приватного управління даними IoT-пристроїв

УДК 04.056:004.738.5

[1]Овсянко Дмитро, [2]Нємкова Олена

Національний університет Львівська Політехніка,
[1]dmytro.o.ovsianko@lpnu.ua, [2]olena.a.niemkova@lpnu.ua

Стрімке поширення IoT-систем супроводжується зростанням обсягів даних, кількості підключених пристроїв та вимог до безпеки їхньої взаємодії. Традиційні цифрові двійники зазвичай функціонують у межах централізованих хмарних платформ, де контроль над ідентичністю пристрою, політиками доступу та зберіганням даних фактично належить провайдеру системи. Такий підхід створює ризики єдиної точки відмови, ускладнює масштабування та обмежує автономію власника пристрою щодо управління власними даними [1]. Актуальність дослідження зумовлена необхідністю забезпечення приватності, цілісності та незалежного контролю над даними IoT-пристроїв в умовах активного впровадження концепцій Industry 4.0 та розумних середовищ, де користувач має зберігати суверенітет над власними цифровими активами.

Метою роботи є розроблення архітектури самосуверенного цифрового двійника (Self-Sovereign Digital Twin, SSDT) для приватного управління даними IoT-пристроїв на основі принципів децентралізованої ідентичності, верифікованих облікових даних та незмінного аудиту. Самосуверенний цифровий двійник розглядається як цифрове представлення фізичного об'єкта, яке має власну децентралізовану ідентичність, криптографічні ключі, набір атрибутів, поточний стан, історію змін та політики доступу [2]. Наукова новизна роботи полягає у тому, що, на відміну від відомих підходів, запропонована архітектура поєднує концепцію цифрового двійника з моделлю самосуверенної ідентичності, переносить функції управління ідентифікаторами та політиками доступу на периферійний рівень, а блокчейн-реєстр використовує виключно для криптографічних зобов'язань і службових записів, без зберігання первинних IoT-даних, що дозволяє забезпечити баланс між приватністю, прозорістю аудиту та продуктивністю системи.

Для досягнення поставленої мети запропоновано трирівневу архітектуру SSDT. Перший рівень (фізичний) представлений IoT-пристроями, які здійснюють збір телеметрії, формують повідомлення з часовими мітками та номерами послідовності, а також підписують дані за допомогою криптографічних ключів. Це дає змогу підтвердити автентичність джерела даних і виявляти спроби повторного використання повідомлень.

Другий рівень (рівень цифрового двійника) розміщується на периферійному обчислювальному шлюзі. Він відповідає за управління децентралізованими ідентифікаторами, зберігання верифікованих облікових даних, агрегацію телеметрії, підтримку поточного стану цифрового двійника та виконання політик доступу. Розміщення цього функціоналу на периферії дозволяє зменшити залежність від хмарної інфраструктури, скоротити затримки та забезпечити локальну обробку чутливих даних.

Третій рівень (блокчейн-рівень) виконує функцію розподіленого реєстру довіри. У ньому фіксуються операції реєстрації та оновлення децентралізованих ідентифікаторів, статуси облікових даних, факти відкликання повноважень і критичні події доступу. Використання приватного блокчейну дозволяє забезпечити незмінність журналу аудиту без необхідності зберігати повні набори IoT-даних у реєстрі. Замість цього до блокчейну можуть записуватися криптографічні зобов'язання, хеші або службові записи, необхідні для перевірки цілісності [3].

Окрему роль у запропонованій архітектурі відіграють механізми приватності. Для зменшення обсягу розкритих даних може застосовуватися селективне розкриття атрибутів та докази з нульовим розголошенням. Це дозволяє підтверджувати певні твердження про стан пристрою без передавання повного набору первинних даних. Наприклад, цифровий двійник може довести, що параметр перебуває в допустимому діапазоні, не розкриваючи його точного значення.

Для оцінювання безпеки системи доцільно використовувати модель загроз STRIDE. Основними загрозами для SSDT-системи є атаки типу Man-in-the-Middle, replay-атаки, підміна IoT-пристрою або цифрового двійника, підробка облікових даних, обхід політик доступу, масовані спроби несанкціонованого доступу та компрометація приватних ключів. Як контрзаходи можуть використовуватися взаємна автентифікація на рівні mTLS, підписання повідомлень на рівні застосунку, перевірка часових міток і номерів послідовності, реєстрація DID у блокчейн-реєстрі, перевірка статусу відкликання облікових даних, обмеження частоти запитів та зберігання ключів в апаратних модулях безпеки.

Висновки. У результаті дослідження запропоновано трирівневу архітектуру SSDT, яка поєднує функціональність цифрових двійників із принципами самосуверенної ідентичності, приватності за проєктуванням та незмінного аудиту. Отримані результати показують, що запропонований підхід забезпечує контроль власника пристрою над ідентичністю та даними, надає зовнішнім сервісам лише той обсяг інформації, який необхідний для конкретної взаємодії, та дозволяє верифікувати цілісність взаємодій без розкриття змісту IoT-даних. Перспективними напрямами подальших досліджень є оптимізація генерації доказів з нульовим розголошенням для ресурсно обмежених пристроїв, розроблення прототипу SSDT та експериментальна оцінка продуктивності запропонованої архітектури.

1. Tao F., Zhang M., Nee A. Y. C. Digital Twin Driven Smart Manufacturing. Academic Press, 2019. 340 p.
2. Mühle A., Grüner A., Gayvoronskaya T., Meinel C. A survey on essential components of a self-sovereign identity // Computer Science Review. 2018. Vol. 30. P. 80–86.
3. Androulaki E., Barger A., Bortnikov V. et al. Hyperledger Fabric: A distributed operating system for permissioned blockchains // Proceedings of the Thirteenth EuroSys Conference. 2018. P. 1–15.