УДК 004.056.5, 004.7

ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ REST API

Безвугляк М. С., Курдеча В. В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: maximbezvugliak@gmail.com

Security of information on the Internet of Things based on REST API

Overview, problems of protection of information in the Internet of Things. Consideration of proposed solutions at the moment and their comparison. A modified method is proposed that improves the level of protection of information on the Internet of Things.

Огляд, проблеми захисту інформації в Інтернеті речей. Розгляд запропонованих рішень на даний момент та їх порівняння. Запропонування модифікованого методу, який покращує рівень захисту інформації в Інтернеті речей.

Інтернет речей з'єднує комп'ютерні пристрої інтегровані у повсякденні об’єкти через Інтернет, що дозволяє їм надсилати та отримувати дані. Є дві переваги, які надають комп’ютерам можливість збирати інформацію про оточення, незалежно від людини і від обробки зібраної інформації зменшуються втрати та вартість.

На сьогоднішній день запропоновані методи в захисті інформації в мережі інтернету речей мають багато недоліків в таких аспектах як:

- Інфраструктура відкритих ключів не підходить для IoT середовища, так як це стає обчислювально важким завданням обчислення шифрованого тексту через великий розмір ключа.

- Після того, як система потрапить під загрозу, її буде важко оновити. Крім того, потенційно відключення скомпрометовані системи, перевстановлюють або перезапускають програмне забезпечення або замінюють компоненти або підсистема не підходить для всіх систем IOT.

Усі пристрої пов’язані в одну систему повинні мати довірчу відносини одне до одного. Програмне забезпечення IoT має керувати довірчими відносинами пристроїв, щоб ці пристрої могли бути аутентифіковані та авторизовані для обміну даними. Для цього потрібно застосувати автентифікацію для комунікації з будь-яким пристроєм, що може підтвердити походження даних.

В даній роботі розглянуто захист інформації в мережі інтернету речей використовуючи REST API для безпечного з'єднання між пристроями в мережі та використання Еліптично Кривої Криптографії для безпечної авторизації пристроїв.

REST API дозволяють відкрити підключений пристрій користувачам у програмі безпечним способом.

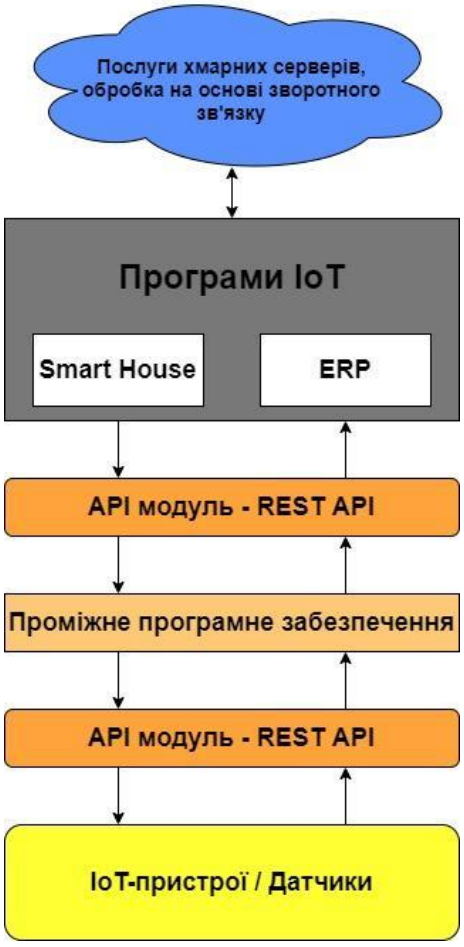

Рис. 1. Модель архітектури Проміжного програмного забезпечення в мережі інтернету речей.

RESTful API широко використовуються в сучасній мережі. Передача даних зазвичай здійснюється за допомогою JSON або XML через HTTP. Це гарна модель для неоднорідних систем. REST API робить інформацію про пристрій легкодоступною. Вони можуть стандартизувати спосіб створення, читання, оновлення та видалення даних. Усі ці операції включені до REST-запиту. API REST дозволяють делегувати та керувати авторизацією. API може автентифікуватись на сервері і сервер можуть аутентифікувати API, щоб запобігти атаки в середині.

На рис. 1 представлена загальна картина ролі проміжного програмного забезпечення в IoT. У загальномі сенсі маємо чотири категорії основних компонентів системи IoT - датчики, локальна мережа, яка може включати шлюз, проміжне програмне забезпечення, хмарне сховище.

Доступно багато протоколів авторизації. Наприклад, OAuth - це відкритий протокол авторизації, який може надати доступ до ресурсу через програмне забезпечення, використовуючи ім'я користувача, пароль та токени.

Крок 1: - Для реєстрації пристрою потрібен авторизований користувач, який вже створив онлайн-аккаунт через проміжне програмне забезпечення.

Крок 2: - Щоразу, коли запит на аутентифікацію надходить від пристрою IoT, шлюз перевіряє запит пристроїв, включаючи корисне навантаження пристрою, отримуючи доступ до відкритого REST API. Далі шлюз, у свою чергу, робить запит на доступ до відкритого API з власними обліковими даними. Запит буде містити ідентифікатор шлюзу та секретний ключ як вхідні параметри. API буде ідентифікувати та авторизувати шлюз, і підтверджувати запит. Усі методи в API REST вимагають аутентифікації. Після того, як шлюз буде авторизований, відповідь у зашифрованій формі, що містить деталі пристрою, надсилається назад до шлюзу. Тепер після перевірки шлюз надає маркер доступу до пристрою, і пристрій може надсилати дані в реальному часі на шлюз. Безпечні рішення реалізуються таким чином, щоб виявити небажані вторгнення та запобігати зловмисним атакам на комунікаційному шарі. Крім забезпечення від атак типа атак Replay, відсутній ідентифікатор відгадування атак, заборонений вхід, анонімність користувача та анонімність датчика вузла.

На рис. 2 наведено огляд вимоги безпеки для різних ступенів системи IoT.

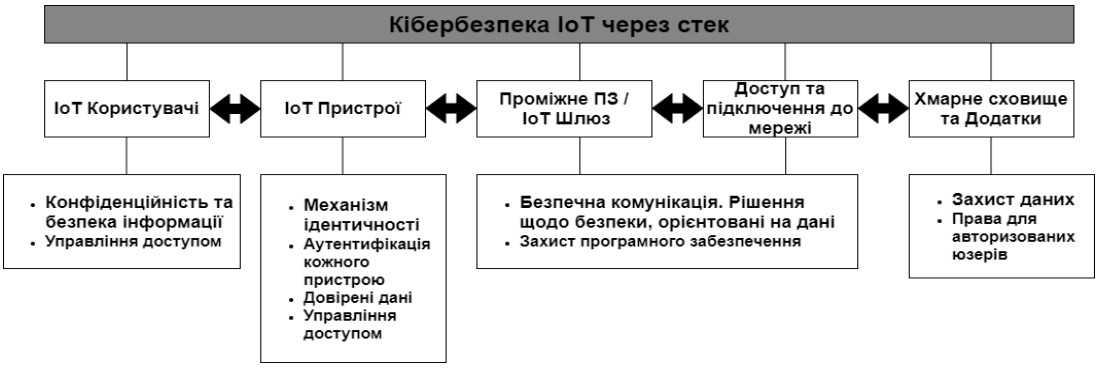

Рис. 2. Модель захисту для системи інтернету речей.

Запропоновані особливості застосування REST API дозволяють підвищити безпеку інформаційного обміну IoT :

- Пристрої IoT ізольовані і не мають взаємодії із зовнішнім світом. Вони підключені до шлюзу і цей шлюз діє як інтерфейс до Інтернету для пристроїв IoT. Тому що розумні пристрої шлюзу можуть бути заховані в підприємстві за декількома брандмауерами і не потребуватимуть вхідних даних порта.

- Зв'язок між шлюзом IoT та проміжним програмним забезпеченням захищене традиційними криптографічними алгоритмами. Не потрібно використовувати легковісні алгоритми, оскільки дві сторони не є ресурсообмеженими.

- Про автентифікацію та авторизацію піклується REST API, що робить весь процес менш складним та сумісним з індустріальними стандартами.

В даній роботі розглянуто архітектуру проміжного програмного забезпечення, яка забезпечує рішення безпеки для учасників, і сформовано особливості застосування REST API для шифрування даних. У запропонованому рішенні проміжного програмного забезпечення всі обмеження системи IoT приймаються до розгляду. REST API використовується для зв'язку та обміну даними. Проміжне програмне забезпечення успішно допомагає IoT в розробці шляхом викриття API REST та надання інтерфейсу для користувача, щоб зареєструвати пристрої в мережі IoT, а потім надання безпечного доступу до даних, зібраних пристроєм. Такий підхід має підвищити безпеку IoT мережі.

Література

1. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.
2. “REST API for Oracle Internet of Things Cloud Service”, docs.oracle.com/en/cloud/paas/iot-cloud/iotrq/QuickStart.html.
3. Wu, F., Xu, L., Kumari, S., & Li, X. (2017). “A privacy-preserving and provable user authentication scheme for wireless sensor networks.
4. Ayoade, G., El-Ghamry, A., Karande, V., Khan, L., Alrahmawy, M., & Rashad, M. Z. (2018). Secure data processing for IoT middleware systems. The Journal of Supercomputing, 1-26.