УДК 004.7, 004.4

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ДАНИХ В МЕРЕЖІ INTERNET OF THINGS

Петров О.С., Курдеча В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kyiv12@bigmir.net

ANALYSIS OF DATA PROTECTION METHODS ON THE INTERNET OF THINGS

With the constant increase in the number of "smart" devices, the vulnerability of data also increases. There are a number of vulnerabilities between them on the Internet of Things that can be exploited by attackers. The paper considers various methods of solving these weaknesses. An effective IoT connection with Blockchain is presented. As a result, a complete or partial solution to the existing problems of the Internet of Things.

При постійному зрості кількості «смарт» приладів зростає і вразливість даних. В Інтернеті речей існує низка вразливих точок, якими можуть скористуватися зловмисники. В роботі розглядаються методи протидії атакам на мережу IoT та захисту інформації. Запропоновано метод захисту інформації, що базується на технології Blockchain.

Є низка критичних аспектів, які прямо або вторинно впливають на інформаційну безпеку в IoT. Найперше – це організаційні заходи, такі як: створення і впровадження єдиної політики інформаційної безпеки підприємства з урахуванням всіх додатків і систем, розробка правил безпечного використання IoT-приладів і мереж, вдосконалення законодавчого забезпечення недоторканності приватного життя та особистої, державної та інших таємниць, державна і приватна стандартизація і сертифікація пристроїв, каналів передачі, сховищ інформації та прикладного ПО з обробки та аналізу даних.

Технічні інструменти захисту даних від витоків, втрат і перехоплення, управління, використання також потребують переконфігурації, де це необхідно. Має бути реалізація шифрування та/або інших криптографічних методів, персоналізація IoT-пристроїв з використанням унікальних ідентифікаторів ID, MAC-адрес, ключів і сертифікатів, що забезпечують досить високий рівень кібербезпеки без додаткових витрат, гнучкі політики управління доступом з багатофакторною авторизацією, резервування, реплікація, організація захищеного периметра і інші засоби інформаційної безпеки.[1]

Обладнання, яке використовується в IoT мережах не завжди відповідає необхідним критеріям. Виробник повинен нести відповідальність зі своєї сторони за продукцію та її цілеспрямованість. Для повної відповідності вимогам мають використовуватись сучасні і надійні інструменти програмної розробки (API, бібліотеки, фреймворки, протоколи…) і апаратні рішення (плати, контролери та ін.). Бажано скоротити кількість компонентів, необхідних для роботи обладнання, оскільки кожен додатковий елемент є потенційним джерелом вразливостей і фізичних поломок. Девайси мають реалізувати безпечну аутентифікацію, узгодження зашифрованих сеансів і перевірку автентичності користувачів. Для того, щоб як найдовше зберігати надійність і актуальність складових систем виробник повинен

забезпечити регулярний випуск оновлень ПО для усунення знайдених і потенційно можливих вразливостей.

Незважаючи на те, що дана область діяльності непідконтрольна окремому користувачеві IoT-системи, а регулюється галузевими гігантами або цілими державами, вона дуже важлива для кінцевого клієнта - підприємства або фізичної особи. Тому необхідно повноцінно ввести стандарт, адже він регулює довіреність інформаційної та фізичної компонентів IoT-систем: надійність, функціональну безпеку, інформаційну безпеку, безпеку персональних даних, стійке функціонування в умовах атаки.[2] Тому за останні роки державні і міжнародні організації провели низку заходів для стандартизації і регламентування. Однак, питання кібербезпеки інтернету речей хвилюють не тільки державних чиновників. Питаннями сертифікації IoT-систем займаються і приватні компанії, а також незалежні експертні співтовариства. На жаль, сьогодні сертифікація ще не діє повноцінно.

Для підтримки тенденції захищеності даних в мережі Інтернету речей, відносно нової технології, не достатньо розглянути її зі сторони самостійної концепції та методів її реалізації. Ефективним буде використання симбіозу недавно створених технологій та реалізація нових на основі існуючих.

Цікава зв’язка Інтернету речей з технологією блокчейну. Вони можуть забезпечити високий рівень перевірки довіри для даних, що передаються. Основна ідея полягає у наданні пристроям ідентичності, яка може бути перевірена під час першої ініціалізації та протягом всього життєвого циклу. Можливості технологій блокчейну, які покладаються на протоколи ідентифікації пристроїв та системи репутації, мають великий потенціал для систем IoT. За допомогою протоколу ідентифікації пристрою кожен з них може мати власний відкритий ключ блокчейну та надсилати зашифровані повідомлення про виклики та відповіді на інші, тим самим активний девайс залишається під контролем своєї ідентичності. Крім того, вузол з ідентифікацією може розвинути репутацію або історію, які відстежуються блокчейном.

На відміну від бази даних, яка має одного адміністратора, блокчейн дозволяє набору різноманітних адміністраторів "реферувати" дані, так що жоден адміністратор не може зловмисно або випадково змінити або видалити дані. І як тільки адміністратори досягнуть консенсусу, дані захищаються блоками, які «прикуті» один до одного криптографічно, формуючи книгу, стійку до фальсифікації [3].

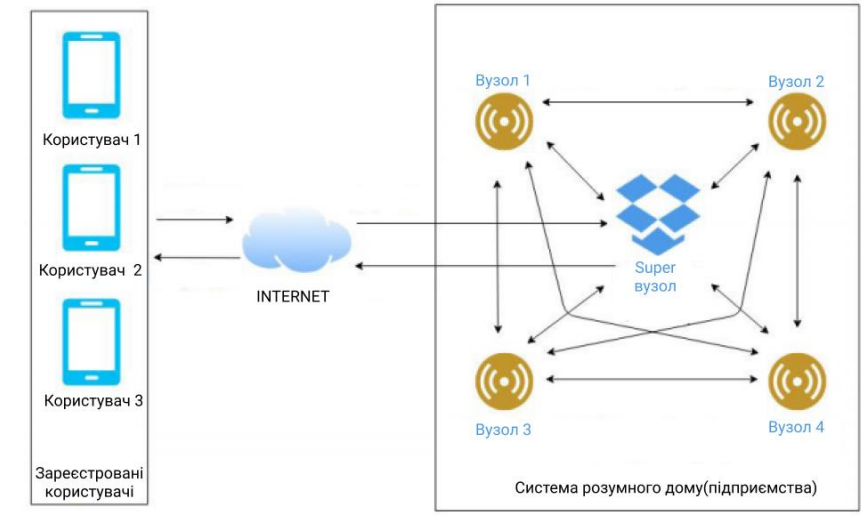

Рис 1. Архітектура розумного будинку з використанням IoT-Blockchain.

Пристрої IoT часто є легкою мішенню для розподілених атак DDoS. Під час DDoS-атак багато компрометованих комп'ютерних систем «бомбардують» ціль, таку як центральний сервер, величезним обсягом одночасних запитів, викликаючи цим відмову в обслуговуванні користувачів цільової системи.

Інша проблема сучасних мереж IoT - це масштабованість. Зі збільшенням кількості пристроїв, підключених через мережу IoT, сучасні централізовані системи для автентифікації, авторизації та підключення різних вузлів у мережі перетворюються на вузьке місце. Це вимагає величезних інвестицій у сервери, які можуть обмінюватись великими обсягами інформації. Більше того, вся мережа може занепасти, якщо сервер стане недоступним.

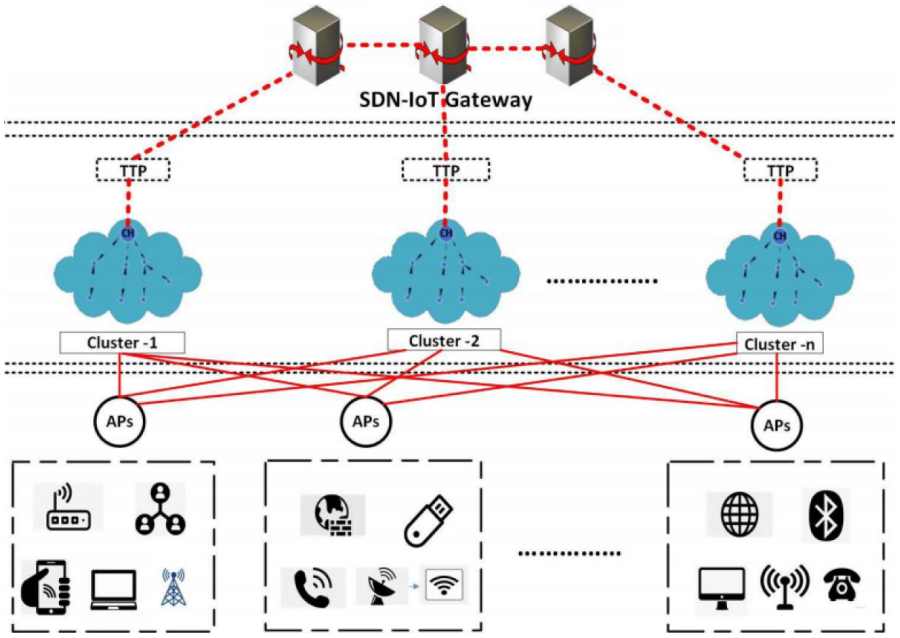

Рис. 2. Структура розподіленої системи Blockchain-IoT (рівень приладів, кластерний рівень, шлюзи хмарного рівня).

Таким чином, система складається з розподіленого цифрового реєстру, який ділиться між учасниками системи, який знаходиться в Інтернеті: транзакції або події перевіряються та реєструються в книзі, і їх не можна згодом змінити чи видалити. Це забезпечує спосіб запису інформації та спільного використання спільнотою користувачів. У межах цієї спільноти вибрані члени зберігають свою копію книги та повинні перевірити будь-які нові транзакції колективно через процес консенсусу, перш ніж їх прийматимуть до книги. Через розподіленість системи відпадають складнощі щодо масштабування та стійкості до DDoS-атак.

Література

1. Protecting Privacy and Data in the Internet of Things. Considerations and techniques for big data, machine learning and analytics / The Walbrook Building, London EC4N 8AF/ 2019 y.
2. Personal data protection for internet of things deployments: lessons learned from the European large-scale pilots of internet of things/ V.8.5 , Create-IoT, Horizon 2020/ February 2020.
3. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network/Saurabh Singh A., S. M. Sanwar Hosen , Byungun Yoon// presented at the IEEE January 14, 2021.