

УДОСКОНАЛЕНА АРХІТЕКТУРА МЕРЕЖІ ДЛЯ ХМАРНОГО ІНТЕРНЕТУ РЕЧЕЙ

Пороло Є.О., Курдеча В.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: jeykeuwork@gmail.com

Improved architecture of the cloud-IoT network

This article proposes the use of Data Bank technology in cloud-based IoT architecture. This structure aims to protect the personal data of users, allowing them to control what type of data is being transmitted and provides supportive tools for transaction visualization and privacy compromise.

В даній статті запропоновано застосування технології Data Bank в хмарній архітектурі IoT мережі. Дана структура спрямована на захист персональних даних користувачів, дозволяючи їм контролювати який тип даних передається та надає допоміжні інструменти для візуалізації транзакцій та компрометації конфіденційності.

На даний час отримав розвитку спосіб надання безкоштовних послуг в обмін на дані користувачів. Технології Інтернету речей приносять багато переваг користувачам, але також викликають занепокоєння щодо безпеки та конфіденційності. Більшість пристроїв можуть передавати особисті дані третім особам. Внаслідок цього, існує явна потреба в розробці хмарної інфраструктури Інтернету речей, щоб дозволити користувачам контролювати свої дані. Для цього пропонується хмарна архітектура Інтернету речей, названу Data Bank, яка дозволяє користувачам налаштовувати збір даних і політики контролю доступу.

Концепція Data Bank пропонується в якості настанови для постачальників послуг. Запропонована структура спрямована на управління даними, що виходять з пристроїв Інтернету речей, шляхом надання політики збору даних на рівні пристроїв і політики обміну даними на хмарному рівні.

Основні особливості цієї архітектури

- сховище(repository);
- механізм конфіденційність-корисність;
- забезпечення контролю доступу.

«Сховище» даних дозволяє користувачам зберігати свої особисті дані в безпеці. Дані тимчасово зберігаються в Data Pocket перед перенесенням в «Сховище» даних в хмарі. Data Pocket (який є локальним і знаходиться під контролем користувача) зберігає встановлену політику конфіденційності і фільтрує дані користувачів перед завантаженням до хмарного сховища. Механізм «конфіденційність-корисність» спрямований на пошук правильного балансу між отриманими перевагами та втратою конфіденційності і пропонує послуги користувачам на основі заздалегідь визначених критеріїв конфіденційності користувачів. «Забезпечення контролю доступу» обмежує постачальників послуг в доступі до даних користувачів. Постачальники послуг надають послуги користувачеві

безкоштовно в обмін на особисті дані та / або збір даних про використання сервісів від користувачів. Data Bank обмежуватиме доступ до даних на основі політики контролю доступу. Запропоновано модифікувати архітектуру Інтернету речей за рахунок зміни специфіки застосування технології Data Bank - пропонується 4-х рівнева архітектура збереження конфіденційності в процесі збору та обміну даними для хмарних платформ Інтернету речей (рис.1).

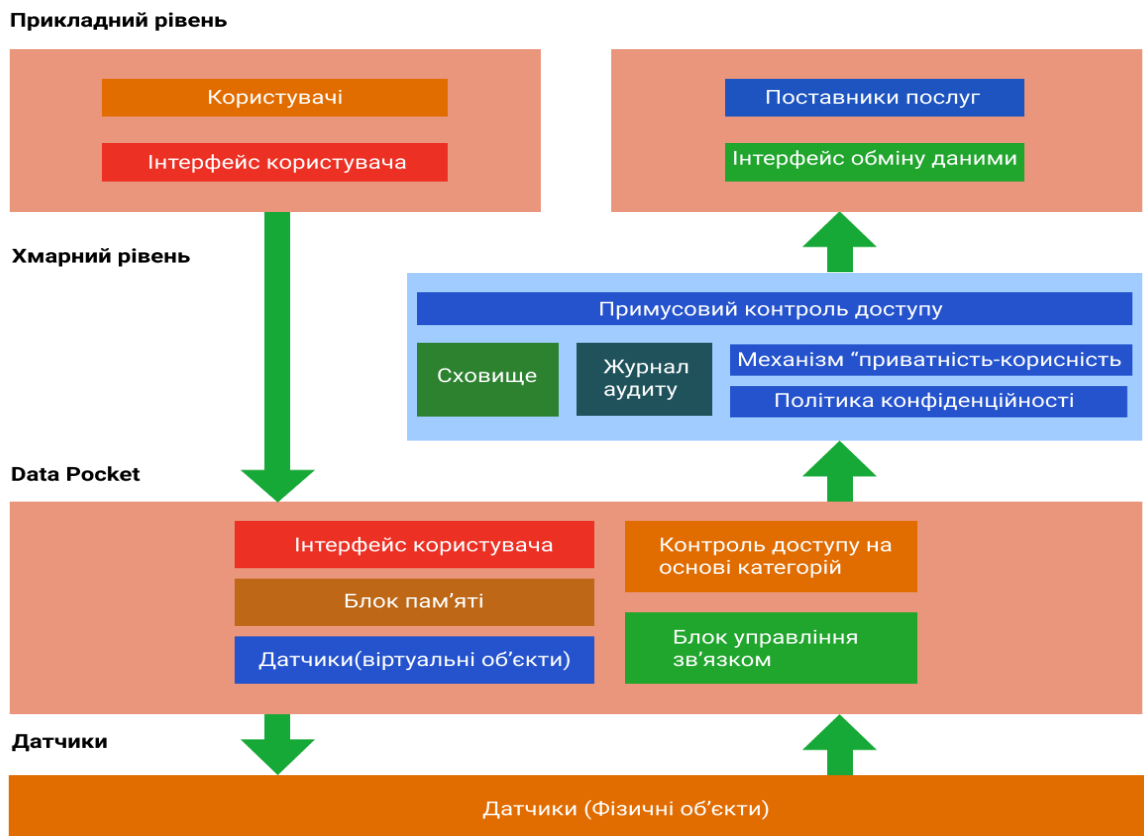


Рис. 1. Модифікована архітектура IoT з використанням Data Bank

Прикладний Шар - це верхній шар, який має справу з користувачами, службами, інтерфейсом користувача та інтерфейсом обміну даними/менеджером компонентів. Інтерфейс визначає: як користувачі повинні взаємодіяти з Data Bank.

Хмарний шар - цей шар містить п'ять основних компонентів, включаючи модуль забезпечення контролю доступу, сховище(геро), журнал аудиту, механізм конфіденційність-корисність і політику конфіденційності.

Data Pocket Layer - цей шар містить інтерфейс користувача, блок пам'яті, датчики, модуль примусового збору даних на рівні пристрою і блок управління зв'язком. Метою даного інтерфейсу є захоплення улюблених користувачів.

Шар датчиків (фізичні об'єкти) - цей шар містить пристрої Інтернету речей, підключені через Інтернет або локальну мережу. Зв'язок між об'єктами в цьому шарі заборонено. Це дозволено тільки через віртуальні об'єкти, які керуються блоком управління зв'язку в Data Pocket.

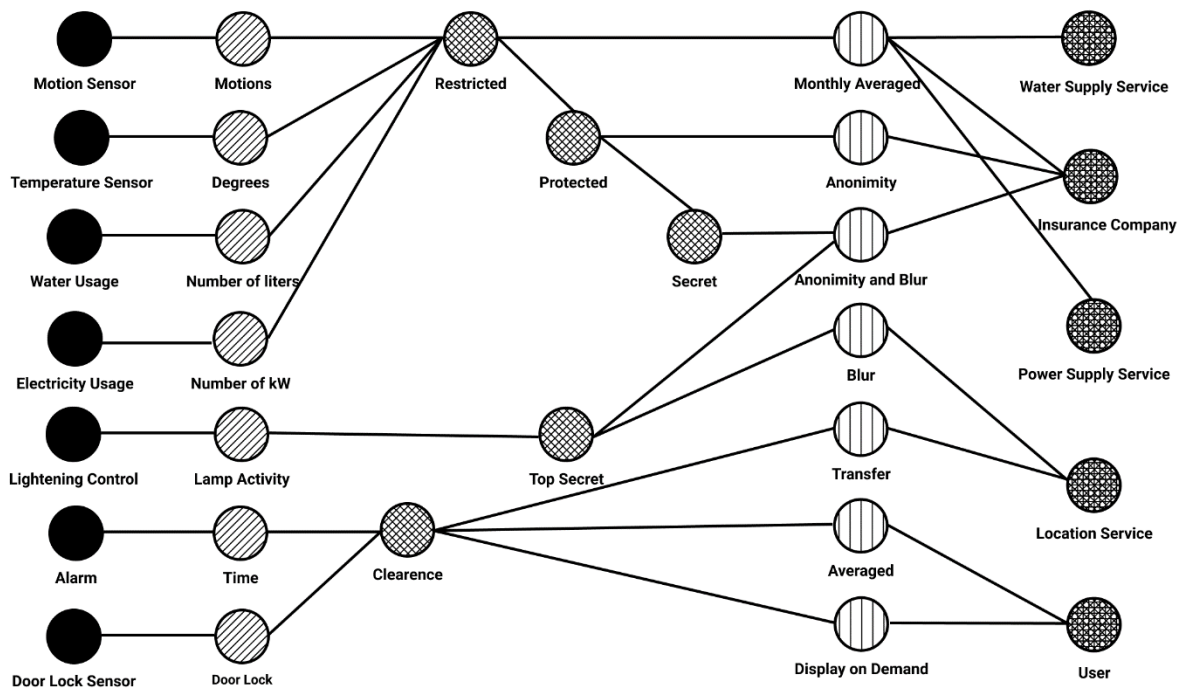


Рис. 2. Приклад політики та шляху даних в системі розумний дім.

Розроблено прототип розумного дому (рис.2), для показу концепції Data Bank.

Існує декілька подібних підходів, що вирішують питання конфіденційності, два з яких близькі до даного: [1] DataBox та [3] Personal Data Vault. Концепцію запропоновану в цій статті можна розглядати як уточнення ідеї Data Vault шляхом додавання елемента управління на рівні збору даних так, що користувачі можуть вибирати, які дані зберігаються в сховищі.

В даній статті було розглянуто багаторівневу архітектуру мережі для хмарного-ІоТ, названу Data Bank, для зберігання та керування особистими даними. Це дає користувачам детальний контроль над їхніми даними і дозволяє їм ділитися інформацією з поставниками послуг відповідно до визначеної користувачем політики. Сервіси можуть отримувати доступ до даних лише в тому випадку, якщо вони уповноважені робити це за допомогою визначеної користувачем політики обміну даними.

Література

1. H. Haddadi, H. Howard, A. Chaudhry, J. Crowcroft, A. Madhavapeddy, and R. Mortier. Personal Data: Thinking Inside the Box. ArXiv e-prints, January 2015.
2. "Access control models for virtual object communication in cloud-enabled IoT," in IEEE International Conference on Information Reuse and Integration (IRI), 2017, pp. 16–25.
3. Min Mun, Shuai Hao, Nilesh Mishra, Katie Shilton, Jeff Burke, Deborah Estrin, Mark Hansen, and Ramesh Govindan. Personal data vaults: A locus of control for personal data streams. In Proceedings of the 6th International Conference, Co-NEXT '10, pages 17:1–17:12, New York, NY, USA, 2010. ACM.
4. S. Barker, "The next 700 access control models or a unifying meta-model?" in Proceedings of the 14th ACM Symposium on Access Control Models and Technologies, ser. SACMAT '09. New York, NY, USA: ACM, 2009, pp. 187–196.