Blokklánc alapú biztonsági keretrendszer IoT eszközökre

Nagy Csaba Norbert

2023.09.20.

DECRYPT
UNIVERSITY OF DEBRECEN

Motiváció

- **Internet of Things** (IoT)
  - Egymással összekapcsolt, egyedi azonosítókkal rendelkező számítástechnikai eszközök (dolgok) rendszere, melyek képesek az adatok hálózaton keresztüli továbbítására anélkül, hogy ember-ember vagy ember-számítógép közötti interakció szükséges lenne.
  - Előnyei – Olcsó és egyszerű eszközök; Nagymennyiségű adatgyűjtésre képesek;
  - Hátrányai – Korlátozott számítási erőforrások; Nehéz átláthatóság;
- Aktuális problémák
  - Felhasználói mulasztások, gyártói és biztonsági funkciók hiányosságok
  - **Incidensek** mint például Mirai, Gafgyt, Hajime, Tsunami
  - Az eszközök számának éves exponenciális növekedése
- **Blokklánc** technológia alkalmazása lehetséges megoldás

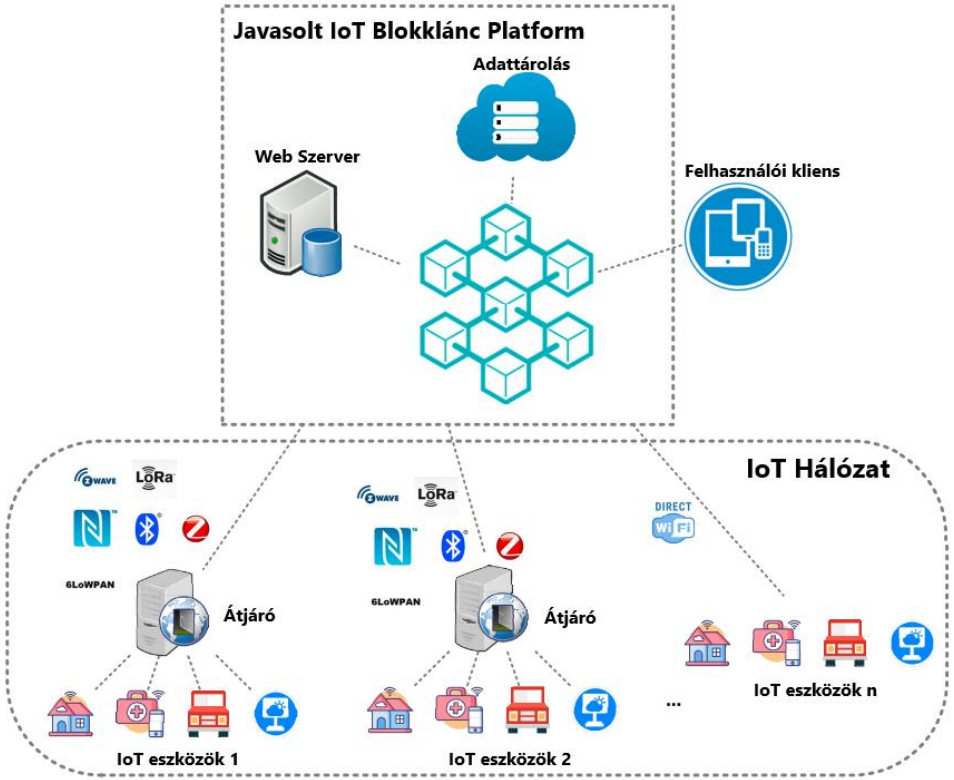
Javasolt keretrendszer általánosan

- **Blokklánc**
  - Egy **peer-to-peer**, **elosztott főkönyv**, amely **kriptográfiailag biztonságos**, csak **hozzáfűzéssel(append-only)** használható, **megváltoztathatatlan**, és csak a résztvevők közötti konszenzus vagy megállapodás révén frissíthető.
- **Blokklánc alapú biztonsági keretrendszer IoT eszközökre**
  - IoT eszközök különböző attribútumait titkosítva egy **privát** blokkláncon elosztott módon tárolja (név, szoftver/firmware azonosító, MAC cím, konfigurációs fájl, napló fájl)
  - Felhasználó figyelmeztetése **alapértelmezett jelszó** változtatásáról ÉS **szoftver/firmware azonosító** frissítése különböző támadások (például ransomware) elhárítása érdekében
- **Elosztott tárolás**
  - Kompromitálás esetén egyszerű visszaállíthatóság
- **Fő célok**
  - A biztonság szintjének növelése a keretrendszert alkalmazó IoT eszközök számára (jelszócsere, eszközök szoftveres karbantartása)
  - Felhasználóbarát platform kialakítása

DECRYPT
UNIVERSITY OF DEBRECEN

Javasolt keretrendszer elemei

- **IoT környezet**
  - Átjáró és alkalmazott protokollok
- **Privát blokklánc**
  - Szenzitív adatok titkosított elosztott tárolása, kezelése, továbbítása
  - Elosztott alkalmazás
- **Web Szerver**
  - Eszközkezelő szolgáltatására
- **Felhasználói kliens**
  - Blokklánc tagja
  - Biztonsági mentés funkció megvalósítása



Biztonsági követelmények és azok vizsgálata a rendszerben

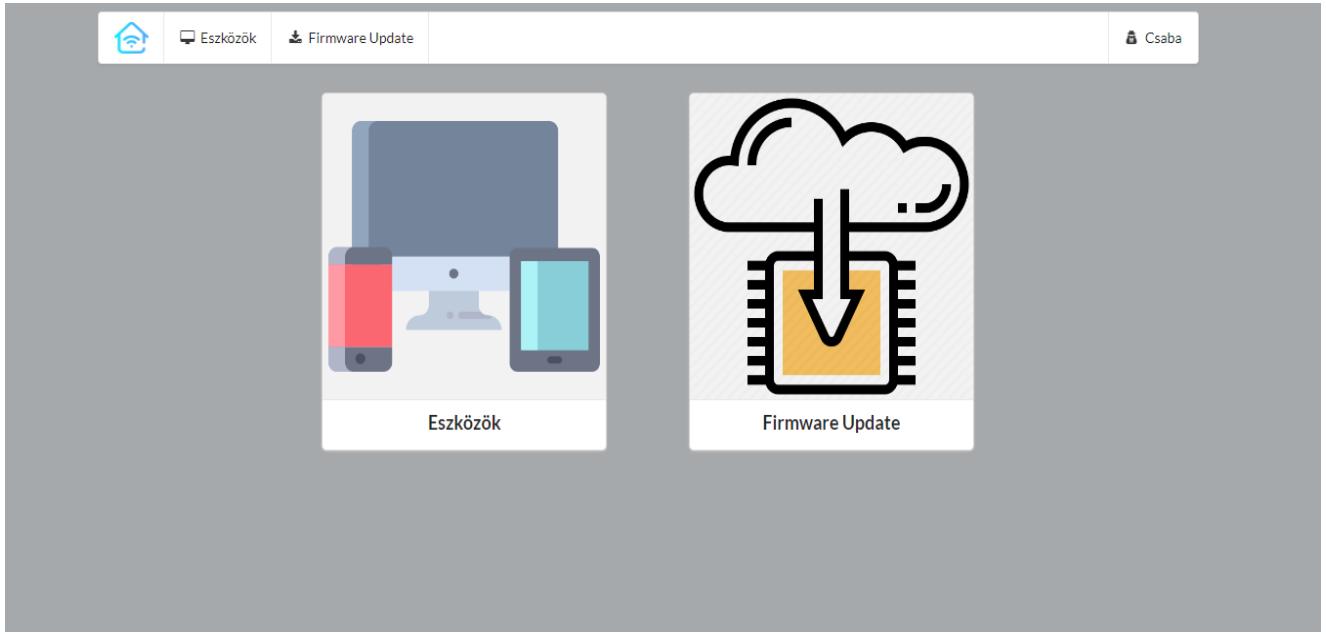
- **Bizalmasság**
  - Felhasználó, webszerver és blokklánc közötti kommunikáción **TLS** protokoll alkalmazása
  - Érzékeny adatok **AES-GCM** blokktitkosítási algoritmussal való alkalmazása
- **Integritás**
  - Blokklánc biztosítja az adatok integritását
  - **Digitális aláírás, SHA-256** hash függvény használata (hash lánc)
- **Rendelkezésre állás**
  - Eszközök és hálózatok redundanciája és a keret skálázhatósága teszi lehetővé
  - Elosztott tárolás és alkalmazás

Biztonsági követelmények és azok vizsgálata a rendszerben

- **Hitelesítés**
  - Felhasználónak a blokklánc tagjának kell lennie
  - Egyszer használatos jelszó alkalmazása
- **Letagadhatatlanság**
  - Eszközök és felhasználók interakcióinak nyomon követése
  - Blokklánc lehetővé teszi a megváltoztathatatlanság teljesülését

Implementáció

- **Backend Javascript nyelvet használ**
- **Frontend React nyelvet használ**
- **Okosszerződések Solidity nyelven íródnak**
- **Metamask fiók alkalmazása Blokklánchoz**
- **Sepolia teszt láncot alkalmazunk**
- **Eszközkezelő**
  - Alkalmazás IoT eszközök menedzselésére
- **Konszenzusmechanizmus**
  - Jelenleg: Proof-of-Work
  - Javaslat: Federated Byzantine Agreement



Köszönöm a figyelmet!