IoT ökoszisztémák biztonsági kérdései

Oláh Norbert

2022. november 4.

UNIVERSITY of DEBRECEN

Debreceni Egyetem Informatikai Kar

Internet of Things

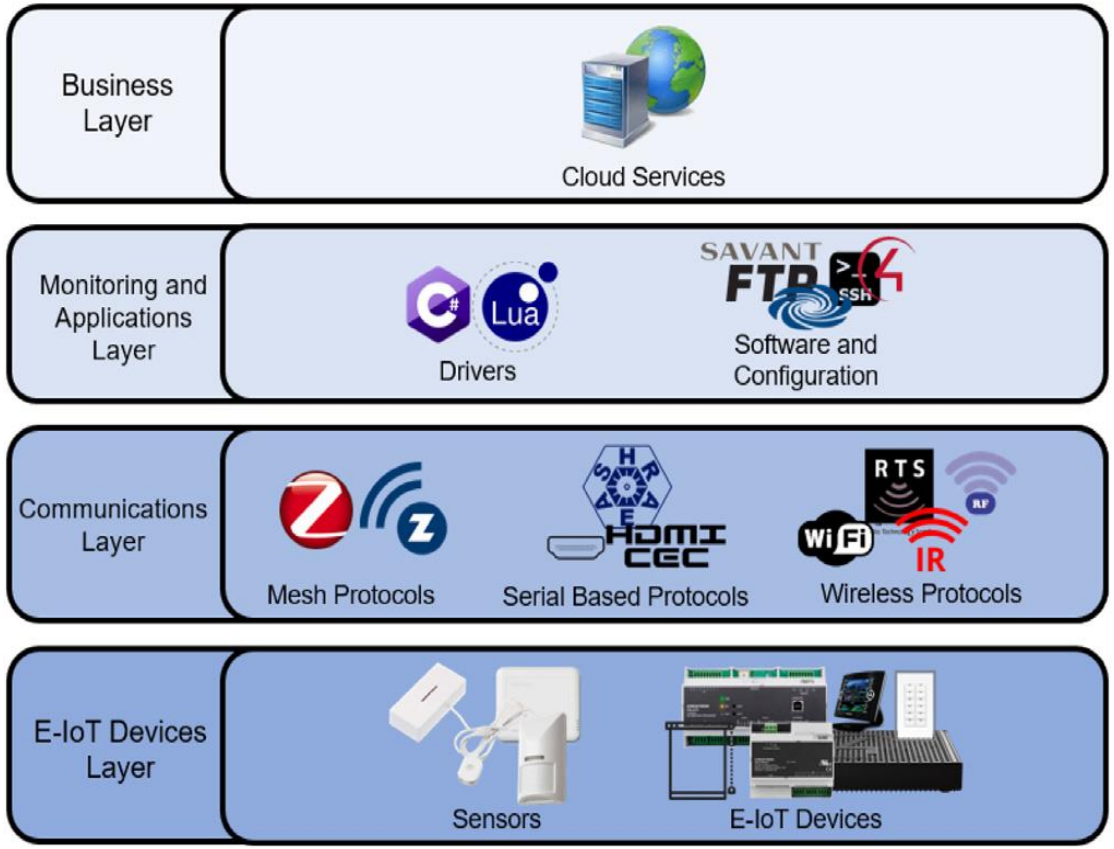
- IoT kiterjesztése:
  - Internet of Space
  - Internet of Ships (IoS)
  - Internet of Mission-Critical Things
  - Internet of Mobile Things
  - IoT ökoszisztémák:
    - A dolgok Internetének (IoT) ökoszisztémája - egy adott cél megvalósítása érdekében Internet hálózat segítségével összekapcsolt és egymástól függő, meghatározott funkcionalitású eszközök és technológiák együttese.
    - Smart Cities
    - Smart Homes
    - Smart Hospitals
    - Smart Grids
    - Smart Airports
    - Smart Transport

UNIVERSITY of DEBRECEN

Debreceni Egyetem Informatikai Kar

IoT eszközök

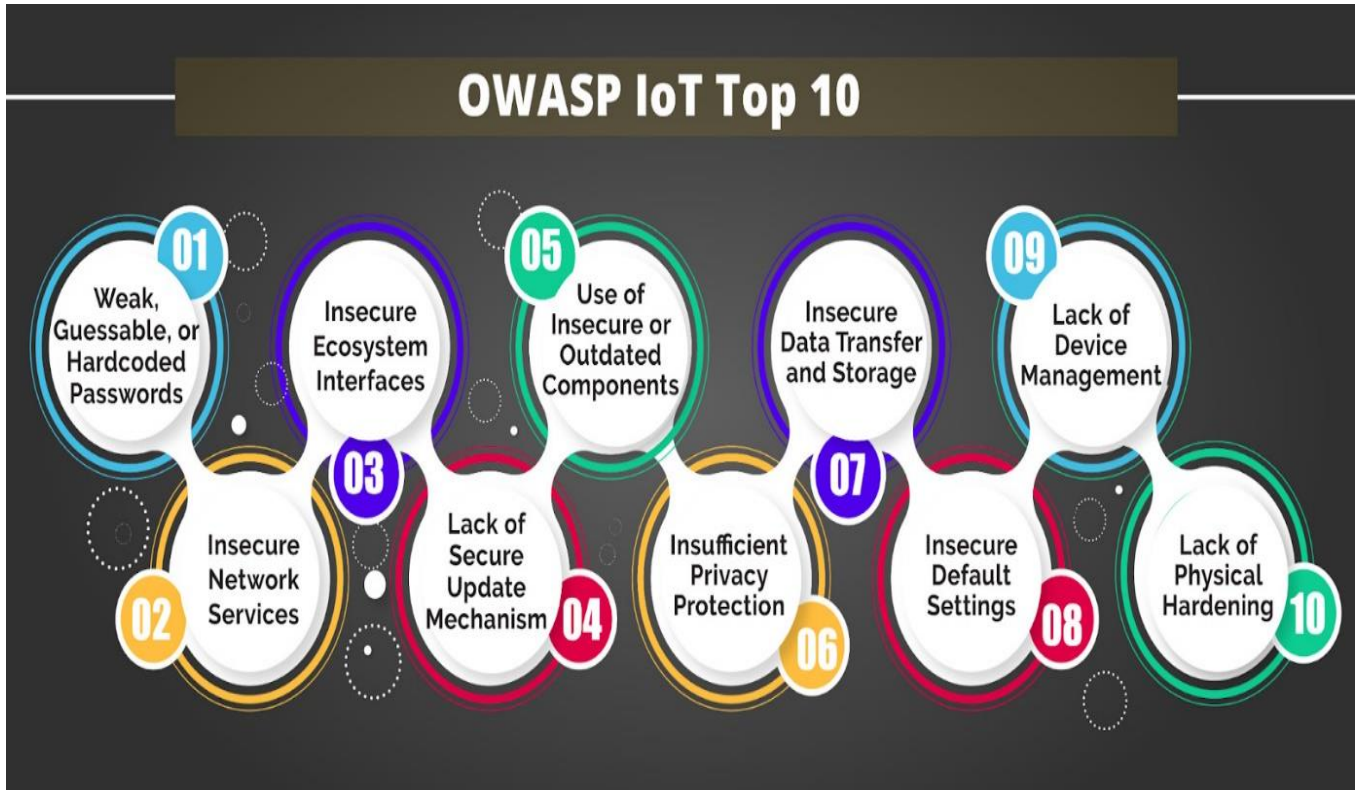
- Érzékelők és beavatkozók
- IoT eszközök gyűjtik az adatokat
  - Biztonságos kommunikáció
  - Adatok tárolása és kezelése
- Kihívások:
  - Korlátozott erőforrással rendelkező eszközök
  - Áramellátási problémák



UNIVERSITY of DEBRECEN

Biztonsági követelmények

- Bizalmasság
- Adatok integritása
- Rendelkezésre állás
- Letagadhatatlanság
- Entitások közötti hitelesítés
- Kulcsok generálása és kezelése

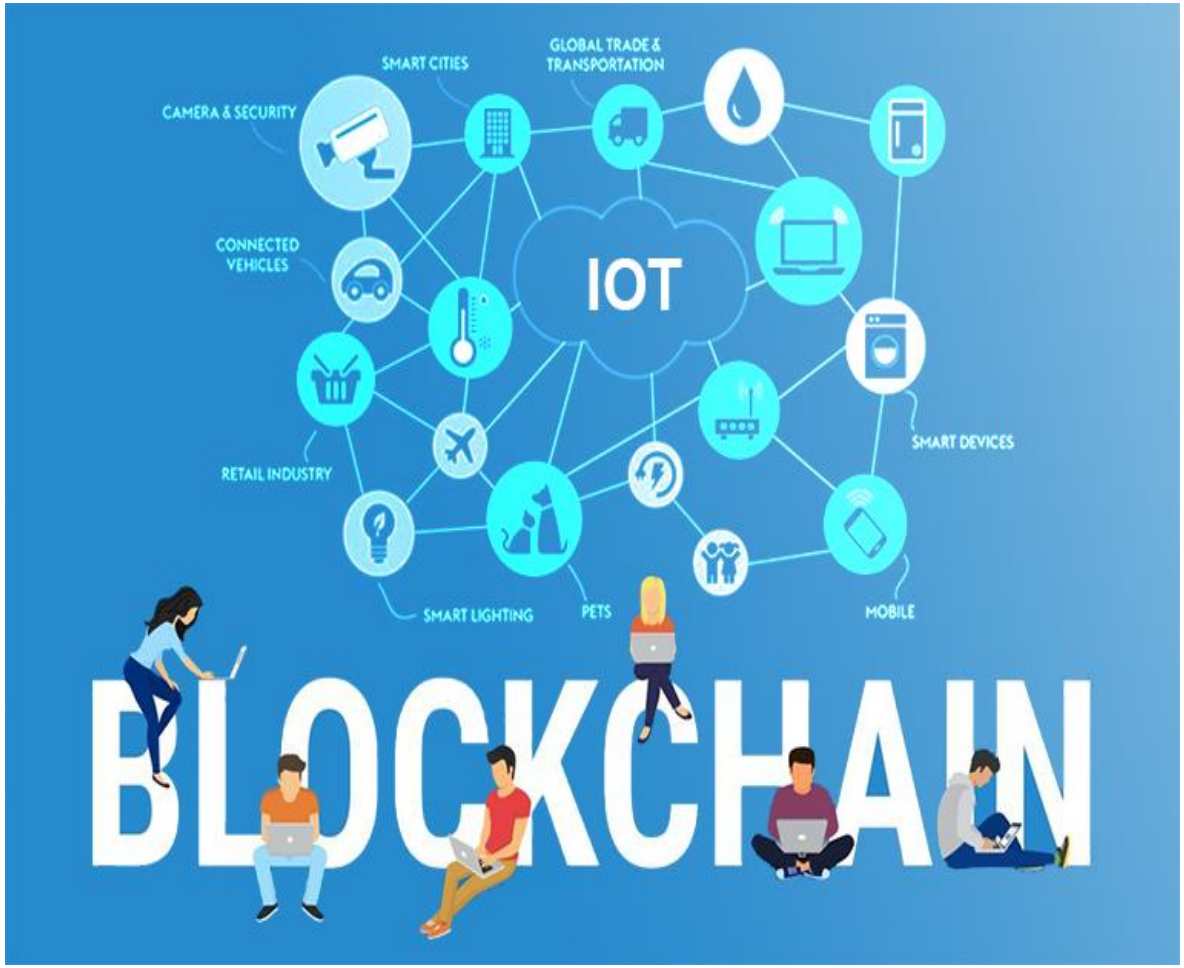


UNIVERSITY of DEBRECEN

DECRYPT
UNIVERSITY OF DEBRECEN

Lehetséges biztonsági megoldások

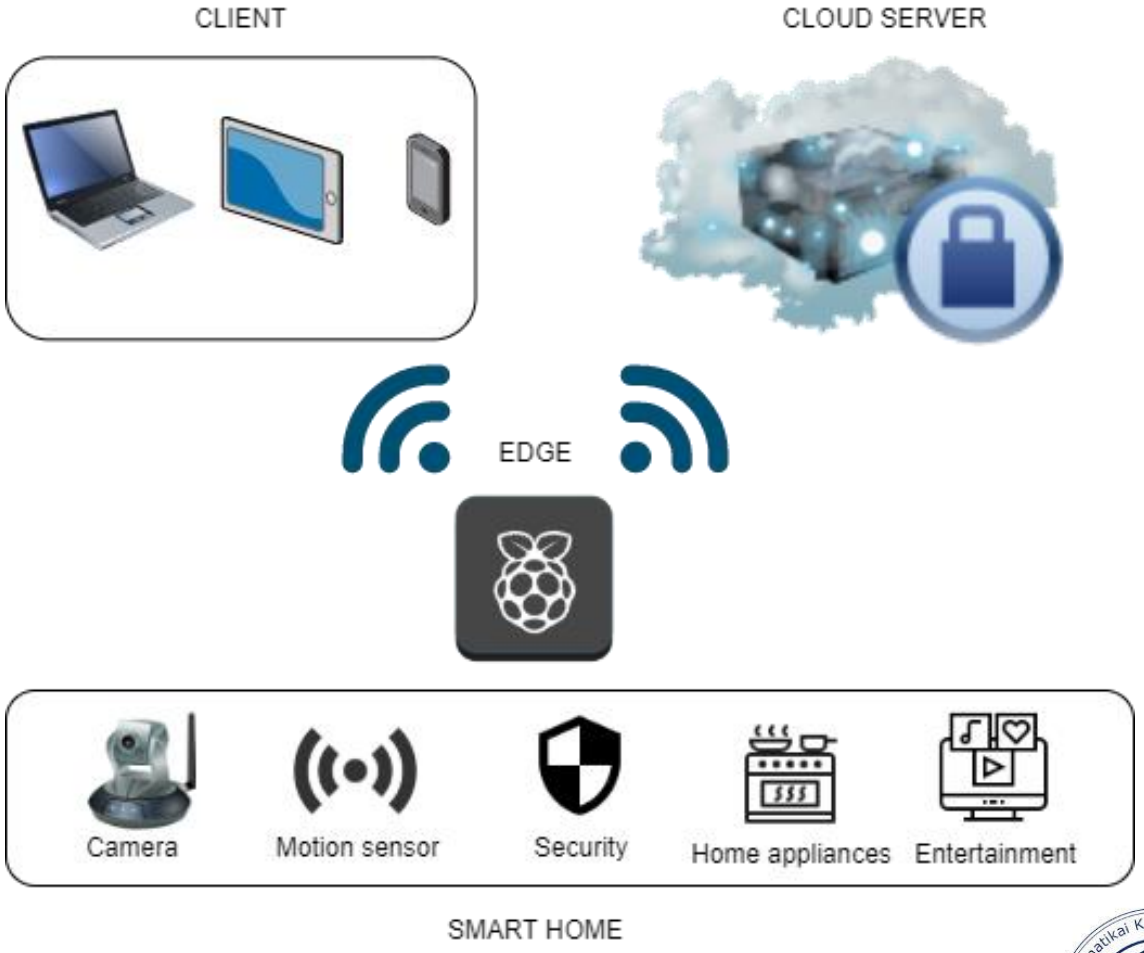
- Elosztott rendszerek és protokollok:
  - Blokklánc biztosítja:
    - Adatintegritás
    - Elérhetőséget
    - Ellenőrizhetőséget
    - Letagadásmentesség
    - elosztott tárolás -> védelem a zsarolóprogramok ellen
- Lightweight kriptográfiai protokollok tervezése
  - Bizalmasság
  - Entitás-hitelesítés
  - Kulcselosztás és -kezelés
  - Posztkvantum algoritmusok (AES 256, hash függvények)



UNIVERSITY of DEBRECEN

Okos otthon autentikáció

- Elosztott - Küszöbértéken alapuló
- Skálázhatóság
- Használható biztonság - jelszó alapú



UNIVERSITY of DEBRECEN

Hiteles és anonim incidens információ küldés

- Feltételes anonimitás
- Üzenetek összeköthetetlensége
- Üzenetek letagadhatatlansága

UNIVERSITY of DEBRECEN

Debreceni Egyetem Informatikai Kar

Köszönöm a figyelmet!