Gradus Vol 10, No 1 (2023)
ISSN 2064-8014

IOT RENDSZEREKET FENYEGETŐ TÁMADÁSOK

IOT SECURITY CHALLENGES

Johanyák Zsolt Csaba[*], *Pásztor Attila*

Informatika Tanszék, GAMF Műszaki és Informatikai Kar, Neumann János Egyetem, Magyarország
https://doi.org/10.47833/2023.1.CSC.001

Kulcsszavak:
IoT
biztonság
támadás
megelőzés

Keywords:
IoT
security
attack
prevention

Cikktörténet:
Beérkezett 2023. január 22.
Átdolgozva 2023. január 25.
Elfogadva 2023. február 28.

Összefoglalás

Az IoT rendszerek az élet szinte minden területén jelen vannak kényelmi funkciókat nyújtva, növelve a hatékonyságot, vagy éppen megoldást kínálva korábban megoldatlan problémákra. Ezen rendszereket a heterogenitás valamint a nagy mennyiségű és sokszor kényes adat továbbítása jellemzi, aminek eredményeképpen számos fenyegetés célpontjává válnak. Cikkünk első részében áttekintjük az IoT rendszerek néhány fontosabb jellemzőjét, majd a legfontosabb biztonsági követelmények ismertetését követően az egyes fenyegetés típusokkal és a kapcsolódó megelőzési/elhárítási lehetőségekkel foglalkozunk.

Abstract

IoT systems are present in almost every aspect of life, providing convenience, increasing efficiency, or even offering solutions to previously unsolved problems. These systems are characterized by heterogeneity and transmission of large amounts of often sensitive data, which makes them targets for a variety of threats. In the first part of this article, some of the main characteristics of IoT systems are reviewed. Then, the most important security requirements will be described, followed by the presentation of different types of threats and the corresponding ways to prevent them.

1. Bevezetés

A dolgok internete (Internet of Things - IoT) elnevezés sokrétű fizikai eszközök (pl. készülékek, járművek, szenzorok, gépek, épületek, számítógépek stb.) interneten keresztüli összekapcsolására utal. Ezek az eszközök érzékelőkkel, szoftverekkel és hálózati interfészekkel vannak felszerelve, amelyek lehetővé teszik számukra, hogy adatokat gyűjtsenek és osszanak meg egymással valamint egy központi rendszerrel.

Számos területen alkalmaznak IoT rendszereket. Az egészségügyben IoT eszközök segítségével távolról is megfigyelhetők a betegek, ami hatékonyabb és olcsóbb ellátást tesz lehetővé. Az iparban az IoT rendszerek felhasználhatók a termelési folyamatok optimalizálására és az általános hatékonyság javítására. Az IoT rendszerek jelentősen hozzájárulhatnak hétköznapi komfortunkhoz is például olyan intelligens otthoni rendszerek révén, amelyek okostelefonok segítségével vezérelhetik a világítást, a hőmérsékletet és az eszközöket.

Az IoT-rendszerek egyik fő jellemzője a nagy mennyiségű adat gyűjtésének és elemzésének képessége. Ezek az adatok felhasználhatók a folyamatok optimalizálására, a döntéshozatal

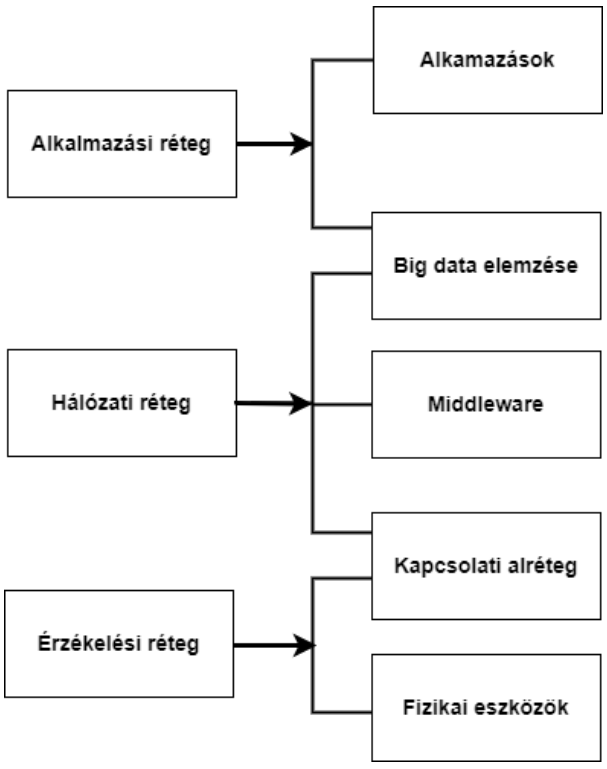
* Kapcsolattartó szerző.
E-mail cím: johanyak.csaba@gamf.uni-neumann.hu

támogatására és az ügyfelek viselkedésének elemzésére. Ezen adatok felhasználása azonban fontos adatvédelmi és biztonsági aggályokat is felvet. Az IoT-rendszerek széleskörű elterjedésével kritikus fontosságúvá vált, hogy a biztonságot szem előtt tartva tervezzék meg őket annak érdekében, hogy megelőzzék a hackertámadásokat és az adatszivárgást.

Az IoT-rendszerek által nyújtott lehetőségek kiaknázása során jelentős kihívásokkal kell szembenézni úgy a biztonság, mint a technológia terén. Sok az egyedi IoT-rendszer, ami megnehezíti a különböző gyártók eszközei közötti kommunikációt. A védelem egyik fontos eszköze a támadások érzékelése, amiben nagy szerepet játszhatnak a mesterséges intelligencia algoritmusokon/eljárásokon alapuló megoldások. A cikk második szakaszában röviden áttekintjük az IoT rendszerek fontosabb jellemzőit, majd ezt követően a harmadik szakaszban a potenciális támadástípusok bemutatására kerül sor kitérve a védekezés lehetőségeire is.

2. IoT rendszerek

Az alábbiakban rövid áttekintést adunk az általános IoT-rendszerekről a biztonsági kockázatot potenciálisan növelő jellemzőkre összpontosítva. A dolgok internete a fizikai eszközöket intelligenssé alakítja kommunikációs technológiák, internetes protokollok és alkalmazások, valamint érzékelőhálózatok segítségével [2]. A közkedvelt intelligens város koncepció megvalósítása is az összekapcsolt intelligens eszközök gondolatán alapszik [30]. Az 1. ábra egy áttekintő képet ad az IoT architektúráról. Ez általában három rétegből áll: (1) alkalmazási réteg, (2) hálózati réteg, és (3) érzékelési réteg [19]. Emellett egyes irodalmakban négy [13], öt [19], illetve 12 réteg [7] megnevezésével is találkozhatunk. Az egyes rétegeknél egy vagy több alréteget különböztethetünk meg, amelyek az ábra jobb oldalán jelennek meg. Az alábbiakban röviden áttekintjük ezeket.

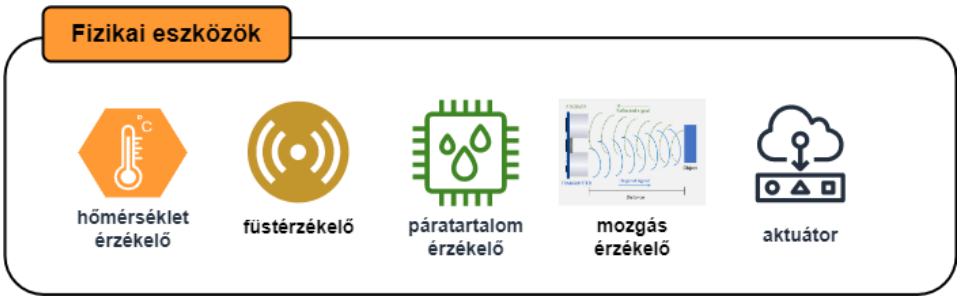


1. ábra. IoT-architektúra [3]

2.1. Fizikai eszközök alrétege

A fizikai eszközök feladata az érzékelés, adatgyűjtés és egyes estekben az adatok feldolgozása. Ez az alréteg érzékelőket (pl. hőmérséklet-, páratartalom-, mozgás- és füstérzékelőket) és aktuátorokat alkalmaz a különböző érzékelési funkciók megvalósításához. A

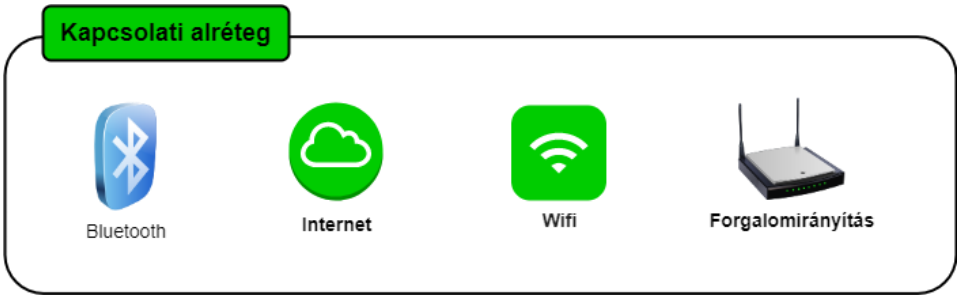
heterogén érzékelők konfigurálása a plug-and-play mechanizmuson alapszik [32]. Az IoT érzékelők erőforrásai általában korlátozottak úgy az akkumulátor-kapacitás, mint a számítási képességek vonatkozásában. Az IoT-eszközök számának növekedése az adatforgalom emelkedését is eredményezi.



2. ábra. Fizikai eszközök alrétege

2.2. Kapcsolati alréteg

Az IoT egyik fontos feladata a heterogén érzékelők együttműködésének megvalósítása, és segítségükkel intelligens szolgáltatások nyújtása. Az érzékelők veszteséges és zajos kommunikációs környezetben működnek [2]. Az IoT-eszközök telepítése során biztosítani kell az egyedi IPv6 címeket (pl. 6LoWPAN [15] használatával), valamint az alacsony fogyasztású kommunikációs technológiát az érzékelők által generált adatok továbbításához. Emellett olyan hatékony útválasztási protokollok megvalósítása szükséges, amelyek figyelembe veszik az érzékelők memóriakorlátait, és támogatják az intelligens tárgyak rugalmasságát és mobilitását. A leggyakrabban alkalmazott technológiák a 6LoWPAN, a Bluetooth, az IEEE 802.15.4, a WiFi, az ultraszéles sávszélesség, az RFID és a közeli mezőkommunikáció (NFC) [2].



3. ábra. Kapcsolati alréteg [13]

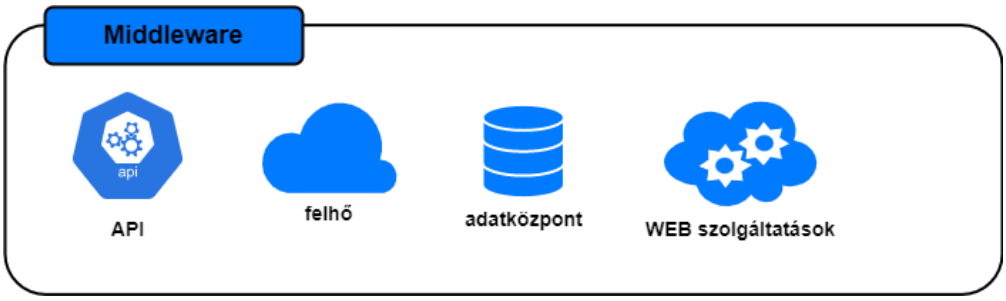
2.3. Middleware

A middleware egy olyan szoftver, amely interfészként szolgál az IoT összetevői között, lehetővé téve a kommunikációt olyan komponensek között, amelyek egyébként nem lennének képesek erre. Az IoT alapfeladata, hogy lehetővé tegye, hogy szinte bármi csatlakoztatható legyen, és biztosított legyen az adattovábbítás.

A middleware-nek biztosítania kell a skálázhatóságot, mivel várható az IoT eszközök számának jövőbeli folytonos növekedése. További feladata az eszközfelfedezés [19] és annak támogatása, hogy az objektumok ismerettel rendelkezzenek az összes környező IoT objektumról. A környezet ismerete hasznosítható az intelligens szolgáltatások nyújtása során is [38]. Emellett a middleware szerepet játszhat az IoT eszközök biztonságának és adatvédelmének biztosításában is.

2.4. A big data elemzése

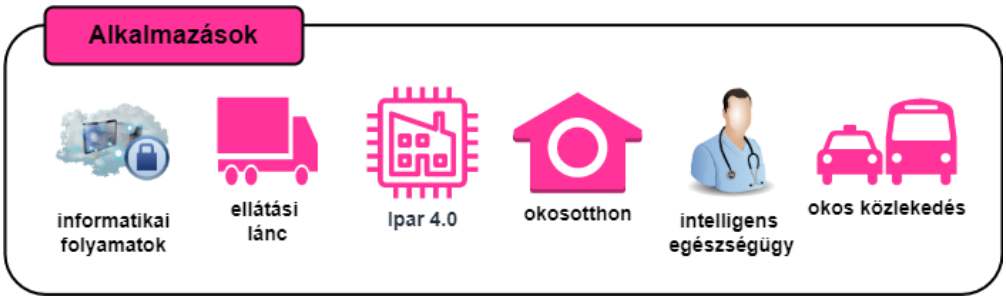
Az IoT által előállított vagy rögzített hatalmas mennyiségű adat rendkívül értékes. A ráépülő gépi tanulást alkalmazó elemzések fontos szerepet játszanak az intelligens IoT rendszerek kiépítésében [29]. A nagy mennyiségű adat feldolgozásában fontos szerepet játszanak a jellemző kiemelési és mély tanulási technikák.



4. ábra. Middleware [13]

2.5. Alkalmazások

Az IoT rendszereket és technológiákat számos területen alkalmazzák. Az alábbiakban hat területet emelünk ki ezek közül.



5. ábra. Alkalmazási réteg [13]

1. A vállalati informatikai folyamatok támogatása

Egy valós idejű adatokkal dolgozó IoT alapú biztonsági rendszer hatékonyan alkalmazható a kibertámadások felismerésére és az incidensekre adott válaszok előkészítésére. Emellett az ügyfélelemzésen alapuló döntéshozatal támogatásában is jelentős szerepet játszhat a dolgok internete által szolgáltatott hatalmas mennyiségű valós idejű adat [17].

2. IoT az ellátási lánc menedzsmentben

Az IoT-t az ellátási lánc menedzsment több szintjén is alkalmazzák. Például a szállítmányozási vállalatok a flottakezelés keretében nyomkövetőket használnak a járművek nyomon követésére. Továbbá elemzik a szállítási útvonalakat annak érdekében, hogy meghatározzák a leggyorsabb és leggazdaságosabb útvonalakat. Az IoT segítségével sok más paraméter is nyomon követhető. Például ilyen a konténerek hőmérséklete és páratartalma [17].

3. Ipari IoT

Az ipari forradalom negyedik hullámának (Ipar 4.0) központi eleme az ipari IoT (Industrial Internet of Things - IIoT). A vállalati karbantartás menedzsment rendszerek IoT érzékelőkkel való kombinálása meghosszabbíthatja a gépek élettartamát, továbbá biztosíthatja a rendelkezésre állást és a megbízhatóságot a valós idejű eszközfelügyeletnek köszönhetően. Ezeken túl az IIoT által gyűjtött adatok segíthetnek a termékfejlesztés és a minőségirányítás optimalizálásában javítva a gyártás hatékonyságát [22] is.

4. Okosotthonok megvalósítása

Az IoT egyik legnagyobb érdeklődést kiváltó alkalmazása az okosotthonok megvalósítása. Egy okosotthon érzékelőket használ a világítás, az erőforrás-kezelés és a biztonsági rendszerek vezérlésére és karbantartására [14]. Az IoT alapú okosotthon-rendszer egyik példája Mark Zuckerberg Jarvis nevű személyi asszisztense [27], ami képes a természetes nyelven megadott parancsok értelmezésére és végrehajtására. Jarvis IoT kapcsolaton keresztül vezéreli az

eszközöket. A rendszer felelős a szoba megvilágításának a foglaltság alapján történő szabályozásáért, sőt képes személyre szabott zenét is lejátszani a szobában tartózkodók számára. Jarvis biztonsági rendszere arcfelismerést alkalmaz a látogatók személyazonosságának megállapításához [17].

5. Intelligens egészségügyi ellátás megvalósítása

Az IoT-eszközöket az egészségügyi ágazatban a betegek állapotának folytonos megfigyelésére és rögzítésére használják, és szükség esetén figyelmeztetéseket küldenek az érintett egészségügyi rendszernek, hogy a betegek gyors és időben történő kezelését biztosítsák. Az egészségügyi alkalmazásoknál nagy kihívást jelent, hogy az adatvédelem követelményeinek történő megfelelés mellett vészhelyzetben hozzáférést kell biztosítani az eszközök által kezelt adatokhoz. Ha egy IoT alapú orvosi eszközzel rendelkező személy hirtelen kórházba kerül, akkor az egészségügyi személyzet könnyen hozzá kell férjen a beültetett IoT eszközhöz [8]. Az előzőekben ismertetett alkalmazási lehetőségek mellett az okostelefonokat széleskörűen használják még a napi aktivitás (lépések, gyaloglás, futás és kerékpározás mérésére), vagy az alvás megfigyelésére is.

6. Okos közlekedés

A dolgok internete (IoT) jelentős szerepet játszik az intelligens közlekedésben, mivel lehetővé teszi a különböző forrásokból (pl. járművekből, közlekedési lámpákból és közúti érzékelőkből) származó adatok gyűjtését és elemzését. Ezek eredménye felhasználható a forgalomáramlás javítására, a torlódások csökkentésére és a biztonság növelésére. Emellett az IoT arra is használható, hogy friss tájékoztatást (pl. forgalmi adatok, és útvonalfrissítések) nyújtson a járművezetőknek és a tömegközlekedéssel utazóknak. Az IoT rendszerek hozzájárulnak ahhoz, hogy a közlekedési rendszerek hatékonyabbá, fenntarthatóbbá és a felhasználók igényeihez igazodóvá váljanak [18].

3. IoT rendszereket fenyegető támadások

Az IoT-rendszerek összetettek, különböző környezetben működő sokfajta eszköz összekapcsolását valósítják meg, ami igen széleskörű támadási felületet eredményez. Az alábbiakban elsőként áttekintjük a fő biztonsági követelményeket, majd ezt követően ismertetjük a fenyegetés típusokat és a védekezési lehetőségeket.

3.1. Biztonsági követelmények

A hatékony IoT biztonsági módszerek kidolgozása során a következő főbb biztonsági követelményeket kell figyelembe venni.

Rendelkezésre állás

A rendelkezésre állás azt jelenti, hogy egy rendszer képes a tervezett módon működni és szolgáltatást nyújtani. IoT rendszerek esetében ez alapvetően két funkciót jelent: (1) az eszközök képesek legyenek csatlakozni a hálózathoz és kommunikálni más eszközökkel, (2) a rendszer képes kell legyen az adatok kezelésére és feldolgozására [24]. A magas rendelkezésre állás kulcsfontosságú az IoT rendszerek számára annak érdekében, hogy megbízható szolgáltatást tudjanak nyújtani, és megfeleljenek a felhasználók igényeinek.

Hitelesítés

A hitelesítés célja az IoT hálózathoz vagy egy adott eszközhöz hozzáférni kívánó személyek és eszközök azonosságának megerősítése. A jogosulatlan hozzáférés és a biztonsági kockázatok elkerülése érdekében alapvető fontosságú annak biztosítása, hogy a hálózathoz vagy az eszközhöz csak az arra jogosult személyek és eszközök férhessenek hozzá.

Az IoT rendszerek gyakran bonyolultak és összetettek, ezért a hitelesítési megoldások jelentősen eltérőek lehetnek. Az IoT-eszközök hitelesítési technikái közé tartozik a jelszóvédelem, a kétfaktoros hitelesítés és a digitális tanúsítványok. A tényleges megvalósítás megtervezésekor a biztonsági szempontok mellett az erőforrás-rendelkezésre állás lehetőségeit is figyelembe kell venni. Olyan hatékony hitelesítésre van szükség, amely képes egyensúlyt teremteni a rendszerkorlátok között, és robusztus biztonsági megoldást nyújt [31].

Engedélyezés

Az engedélyezés témaköre a felhasználók hozzáférési jogainak kezelését jelenti. A felhasználók lehetnek gépek, emberek vagy szolgáltatások. Például az érzékelők által gyűjtött adatokat csak az arra jogosult felhasználóknak (engedélyezett objektumok és szolgáltatásigénylők) szabad átadni, és azokhoz csak az engedéllyel rendelkezők férhetnek hozzá. Egy műveletet csak akkor szabad végrehajtani, ha az igénylő megfelelő felhatalmazással rendelkezik. Egy IoT-rendszerben az engedélykezelés fő kihívása az, hogy hogyan lehet hozzáférést biztosítani egy olyan környezetben, ahol nemcsak az embereknek, hanem a fizikai érzékelők (objektumok) számára is engedélyeket kell adni. Egy ilyen heterogén környezetben a hatalmas adatmennyiség kezelése során az adatokat az érzékelési és továbbítási folyamat során végig védeni kell, és csak az arra jogosultak számára szabad hozzáférhetővé tenni.

Bizalmas kezelés

A bizalmas kezelés azt jelenti, hogy megvédik a jogosulatlan hozzáféréstől vagy nyilvánosságra hozataltól az érzékeny adatokat (pl. orvosi, személyes, ipari és katonai adatok). Az IoT rendszerekben ezen követelmény biztosítása jellemzően titkosítással és biztonságos kommunikációs protokollok alkalmazásával történik. A bizalmas kezeléshez kapcsolódik a hozzáférés-ellenőrzés megvalósítása. A hozzáférés szabályozás és titkosítás azonban nem minden esetben biztosít elegendő védelmet. Például orvosi eszközök esetében elképzelhető, hogy a támadók érzékelhetik a fizikai eszköz létezését, és akár a tulajdonosát is nyomon követhetik [8].

Adat épség

Az IoT eszközök által előállított adatok legtöbbször vezeték nélküli kommunikáción keresztül kerülnek továbbításra. Az épségre vonatkozó elvárás azt jelenti, hogy IoT rendszer biztosítja, hogy az adatok pontosak és teljesek legyenek, azaz nem manipulálták vagy módosították őket jogosulatlanul [10]. Az integritás-ellenőrzés hiányosságai lehetővé tehetik az IoT eszközök memóriájában tárolt adatok módosítását. Az integritás biztosítása az IoT rendszerekben jellemzően titkosítási eljárások, digitális aláírás és hash-elés alkalmazásával történik. Emellett a hozzáférés-ellenőrzés és a naplózás is gyakran alkalmazott eszközök.

Letagadhatatlanság

A letagadhatatlanság arra utal, hogy egy IoT-rendszerben egy művelet vagy kommunikáció eredete visszavezethető egy adott eszközre vagy felhasználóra [9]. Ezen szolgáltatás biztosítása azt jelenti, hogy a rendszer megakadályozza azt, hogy az eszköz vagy a felhasználó letagadja egy műveletet vagy egy kommunikációs tevékenységet. A letagadhatatlanság fontos elvárás az IoT-rendszerek integritásának és biztonságának fenntartása szempontjából, mivel ezen alapul az elszámoltathatóság jogosulatlan műveletek vagy kommunikáció esetén is vagy akár egy fizetési tranzakciónál.

A felhasználók hitelességének és a kommunikáció integritásának biztosítása érdekében a dolgok internetén a letagadhatatlanság hozzáférési naplók, digitális tanúsítványok, digitális aláírások és más kriptográfiai technikák segítségével valósítható meg.

3.2. Fenyegetés típusok

Az IoT rendszereket fenyegető biztonsági kockázatok alapvetően két csoportba oszthatók, ezek a kiber- és a fizikai fenyegetések. A kiberfenyegetések passzív és aktív fenyegetéseket foglalnak magukba. A következő két alfejezetben röviden bemutatjuk ezeket.

3.2.1. Kiberfenyegetések

Passzív fenyegetések

A passzív fenyegetés általában a kommunikációs csatornákon átmenő adatforgalomhoz az IoT rendszer normál működésének megzavarása nélkül történő jogosulatlan hozzáférést jelenti. Két fő típusa a lehallgatás (eavesdropping) és a szimatolás (sniffing).

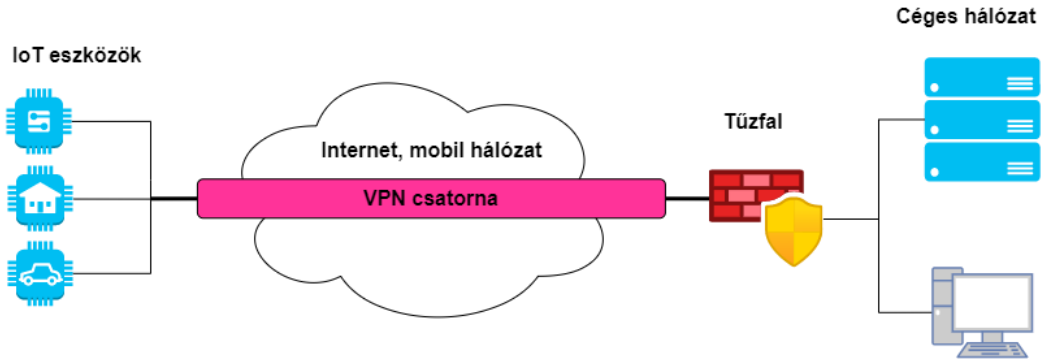
A lehallgatással a támadó információt gyűjthet az érzékelőkről, és nyomon követheti az érzékelő tulajdonosát anélkül, hogy megzavarná a rendszer működését vagy változást idézne elő a rendszerben. A személyes információk gyűjtése nagyon gyakori, mivel ezeket az adatokat rosszindulatú célokra, például személyazonosság-lopásra vagy célzott támadásokra használhatják

fel. Az egyik kiemelten veszélyeztetett terület a személyes egészségügyi adatok gyűjtésével és tárolásával foglalkozó IoT rendszerek területe [3].

A passzív fenyegetés másik formája az adatcsomagok engedély nélküli elfogása és elemzése, aminek célja lehet például a hálózati forgalmi szabályosságok és trendek vizsgálatával történő információszerzés, vagy autentikációs adatok megszerzése.

A passzív fenyegetések gyakran észrevétlenek maradnak, mivel nem zavarják a rendszer normál működését. A védekezés tipikus esközei az alábbiak:

Virtuális magánhálózat (virtual private network - VPN) *létrehozása és használata*. A VPN segítségével a nyilvános internetre csatlakoztatott IoT eszközök egy titkosított ún. VPN csatornán keresztül tudnak kommunikálni az adatokat tároló és feldolgozó szerverekkel titkosított formában továbbítva az adatokat, és elrejtve azokat a támadók elől. A mobil VPN kapcsolat ezen kívül lehetővé teszi, hogy a mobil hálózatok között mozgó IoT eszköz egyetlen logikai IP címmel rendelkezzen, és a céges hálózaton állandó jelleggel ezzel a címmel legyen elérhető amellett, hogy a tényleges IP címe minden hálózatváltáskor módosul.



6. ábra. VPN csatorna IoT rendszerben

Titkosítás használata. A megfelelő biztonsági szintet az ún. erős titkosítási protokollok segítségével érhető el. A klasszikus megoldások, mint pl. Triple DES, elliptikus görbe alapú titkosítás (Elliptical Curve Cryptography - ECC), Advanced Encryption Standard (AES), Digital Signature Algorithm (DSA), Rivest–Shamir–Adleman (RSA), Blowfish és Twofish minőségi megoldást nyújtanak a feladatra, de korlátozott erőforrások rendelkezésre állása esetén valamilyen pehelysúlyú megoldás (Lightweight Cryptography Algorithm) használata ajánlott [28].

Tűzfal használata. A tűzfal segíthet megakadályozni a hálózathoz való illetéktelen hozzáférést, és emellett bizonyos típusú forgalmak szűrhetőek segítségével.

Aktív fenyegetések

Az aktív fenyegetések esetében a támadó valamilyen változtatást kísérel meg végrehajtani az IoT rendszerben vagy az általa továbbított adatokban vagy hozzáférést igyekszik szerezni ezekhez. Leggyakoribb típusai a szolgáltatásmegtagadás, közbeékelődéses támadás, parancsinjekció, brute force-támadások

A *szolgáltatásmegtagadás* (Denial of Service - DoS) támadások célja egy IoT eszköz vagy -hálózat erőforrásainak túlterhelése annak érdekében, hogy az eszköz szolgáltatásai elérhetetlenné váljanak a jóindulatú felhasználók számára. Például ebbe a csoportba tartoznak a hálózati sávszélesség kimerítésére irányuló kísérletek, a vezeték nélküli kommunikáció zavarása, kiszolgálók túlterhelése, stb.

A DoS támadások elleni védekezés elemei lehetnek a támadások korai felismerését biztosító behatolásérzékelő rendszerek (Intrusion Detection System - IDS) [12]. Fejlesztésükben fontos szerepet játszanak a mesterséges intelligencia technikák (pl. [1][4][5][6][20][21]). Alkalmazásuk mellett megfontolandó az eszközök kikapcsolt állapotban tartása olyankor, amikor nem szükségesek (pl. munkaszüneti időszakokban); a nem igényelt funkcionalitás kikapcsolása; az alapértelmezett jelszó lecserélése; és az eszköz szoftverének rendszeres frissítése.

A *közbeékelődéses támadás* (Man-in-the-middle - MitM) során a támadó úgy módosítja két eszköz között a kommunikációt, hogy eltéríti az adatforgalmat, és mindkét fél számára a másik

félnek adja ki magát. Ez lehetővé teszi érzékeny információk ellopását vagy rosszindulatú kód bejuttatását a rendszerbe. A MitM támadások elleni védekezés egyik legfontosabb eleme a VPN alapú kommunikáció és egy megfelelő tanúsítványkezelő rendszer használata. Itt fontos szerepe van a tanúsítványok/kulcsok időszakos felülvizsgálatának/megújításának.

A *parancsinjekció* (Command Injection - CI) során a támadók kihasználhatják az IoT-eszköz szoftverének sebezhetőségeit, hogy jogosulatlan parancsokat hajtsanak végre, kártékony programokat (malware) juttassanak a rendszerbe, érzékeny információkhoz férjenek hozzá, támadásokat indíthatnak más eszközök ellen, vagy megváltoztassák a továbbított adatokat. A malware fenyegetések közül ez egyik legveszélyesebb a Mirai [26], amit arra terveztek hogy Arc processzorral rendelkező IoT eszközök (pl. forgalomirányítók, biztonsági kamerák, hűtőszekrények, stb.) felett átvéve az irányítást botnetet alakítson ki vagy más rosszindulatú programokkal fertőzze az IoT rendszert.

A parancsinjekció elleni védekezés magában foglalja a rendszeres biztonsági tesztelést (pl. Firmware Analysis Toolkit* , AWS IoT Device Defender† vagy PENIOT‡ segítségével) [26], az eszközök firmware-jének rendszeres frissítését, a rendszeres jelszócserét, biztonságos boototás (secure booting) és erős titkosítás alkalmazását.

A szótár alapú és a brute force-támadások során támadók automatizált szkriptekkel próbálkoznak különböző felhasználónév és jelszó kombinációkkal annak érdekében, hogy hozzáférjenek egy IoT-eszközhöz vagy magához az IoT hálózathoz.

A brute-force támadások elleni védekezés legfontosabb eszközei a tűzfalak és az IDS rendszerek, de használatuk mellett is be kell tartani a gyakori jelszócserére és bejelentkezési próbálkozások számának korlátozására vonatkozó általános szabályokat, ajánlott a rendszeres szoftverfrissítés, VPN és erős titkosítás alkalmazása valamint a kétfaktoros hitelesítés bevezetése [25].

3.2.2. Fizikai fenyegetések

A fizikai fenyegetés azt jelenti, hogy a támadó manipulálhatja vagy megsemmisítheti az IoT eszközöket vagy azok környezetét. Az IoT rendszereket fenyegető fizikai támadásfajták néhány jellegzetes esetét az alábbiakban mutatjuk be.

Fizikai fenyegetést jelenthetnek a *természeti katasztrófák* (pl. árvizek vagy földrengések), az emberek által okozott *katasztrófák* (pl. háború), de ide tartozik a *lopás* és *szándékos megrongálás* esete is, ahol a cél a működés megzavarása vagy az adatokhoz történő jogosulatlan hozzáférés.

Ellátási lánc elleni támadás (Supply Chain Attack - SCA) során a támadó hozzáférhet egy IoT eszközhöz még mielőtt azt leszállítanák a végfelhasználóhoz, majd a firmware vagy a hardver megváltoztatásával rosszindulatú komponenst adhat hozzá.

A hozzáférés egy különleges esete az, amikor a támadó *megvásárol cégektől leselejtezett* eszközöket és megpróbál hozzájutni az azokon korábban tárolt adatokhoz. Sok esetben ezek törlése nem történt meg vagy a korábban törölt adatok könnyen helyreállíthatók.

Visszafejtés (Reverse Engineering - RE) veszélye azt jelenti, hogy a támadó szétszerelhet egy IoT eszközt annak érdekében, hogy feltárja annak belső működését, és sebezhetőségeket találjon.

A fizikai támadásokhoz fizikai hozzáférés szükséges az eszközhöz. Ez korlátozza a lehetséges támadók számát, de egyben sebezhetőbbé is teszi az eszközt a támadással szemben, ha az hozzáférhető vagy nem biztonságos környezetben található.

4. Összefoglalás

A dolgok internetén alapuló megoldások komplex rendszerek, amelyek számos eltérő eszköz összekapcsolásából jönnek létre, és az ezek közötti kommunikáció kulcsfontosságú a rendszer működése szempontjából.

Az IoT rendszereket úgy kell megtervezni, megvalósítani, és üzemeltetni, hogy azok az alap szolgáltatás biztosítása mellett a lehető legnagyobb mértékben védettek legyenek az őket fenyegető

* https://github.com/attify/firmware-analysis-toolkit
† https://aws.amazon.com/iot-device-defender/
‡ https://github.com/yakuza8/peniot

igen nagyszámú támadástípussal szemben. Ez utóbbi elvárás azonban a rendszerek sokrétűsége, a költségek és az erőforrásigény miatt komoly kihívást jelent.

A cikk harmadik szakaszában felsoroltuk az alap biztonsági követelményeket, majd a támadástípusokat követően áttekintettük a védekezés lehetséges módjait. Ezek legfontosabb elemei az alábbi ajánlásokban foglalhatók össze:

- Vállalati tűzfal használata.
- Virtuális magánhálózat létrehozása.
- Erős titkosító algoritmusok és egy megfelelő tanúsítványkezelő rendszer használata.
- A tanúsítványok/kulcsok időszakos felülvizsgálata/megújítása.
- Behatolásérzékelő rendszerek alkalmazása.
- Az IoT eszközök kikapcsolt állapotban tartása olyankor, amikor nem szükségesek (pl. munkaszüneti időszakokban), valamint a nem igényelt funkcionalitás kikapcsolása.
- Az alapértelmezett jelszó lecserélése.
- Az IoT eszközök szoftverének rendszeres frissítése.
- Bejelentkezési próbálkozások számának korlátozása.
- A rendszer folyamatos felügyelete.

Az IoT rendszerekkel kapcsolatos további kutatásunk fő iránya egy mesterséges intelligencia technológiákon alapuló behatolásérzékelő rendszer kialakítása valamint a biztonsági kockázatok értékelése fuzzy szignatúrák [16] segítségével.

Köszönetnyilvánítás

A szerzők köszönetet mondanak a projektben résztvevő intézmények - Nádor Rendszerház Kft., Controlsoft Automatika Szolgáltató Kft., Neumann János Egyetem GAMF Műszaki és Informatikai Kar - kollégáinak. Köszönettel tartozunk a kutatás támogatásáért, amely az “Ipar 4.0 moduláris felépítésű ipari csomagológép fejlesztése integrált adatelemzéssel és mesterséges intelligenciára épülő optimalizálással, hibaelemzéssel 2020-1.1.2-PIACI-KFI-2020-00062" pályázat keretében valósult meg. A projekt a Magyar Állam és az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával, a Széchenyi 2020 program keretében valósul meg.

5. Irodalomjegyzék

[1] Andoga, R., Főző, L., Kovács, R., Beneda, K., Moravec, T., & Schreiner, M. (2019). Robust Control of Small Turbojet Engines. Machines, 7(1), 3. doi:10.3390/machines7010003

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015. doi: 10.1109/COMST.2015.2444095

[3] Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Du, X., Ali, I., & Guizani, M. (2020). A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Communications Surveys & Tutorials, 1–1. doi: 10.1109/comst.2020.2988293

[4] Babič, M., Karabegović, I., Martinčič, S.I., Varga, G. (2019). New Method of Sequences Spiral Hybrid Using Machine Learning Systems and Its Application to Engineering. In: Karabegović, I. (eds) New Technologies, Development and Application. NT 2018. Lecture Notes in Networks and Systems, vol 42. Springer, Cham. doi: 10.1007/978-3-319-90893-9_28

[5] S. Blažič, D. Dovžan, I. Škrjanc, Cloud-based identification of an evolving system with supervisory mechanisms, 2014 IEEE International Symposium on Intelligent Control, ISIC 2014, Antibes, France, art. no. 6967642, pp. 1906-1911, 2014. doi: 10.1109/ISIC.2014.6967642

[6] I.-D. Borlea, R.-E. Precup, A.-B. Borlea, and D. Iercan, A unified form of fuzzy C-means and K-means algorithms and its partitional implementation, Knowledge-Based Systems, vol. 214, paper 106731, Feb. 2021. doi:10.1016/j.knosys.2020.106731

[7] A.E. Bouaouad, A. Cherradi, S. Assoul and N. Souissi, "The key layers of IoT architecture," 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), Marrakesh, Morocco, 2020, pp. 1-4, doi: 10.1109/CloudTech49835.2020.9365919.

[8] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," Journal of biomedical informatics, vol. 55, pp. 272-289, 2015. doi: 10.1016/j.jbi.2015.04.007

[9] Chen, F., Wang, J., Li, J., Xu, Y., Zhang, C., & Xiang, T. (2022). TrustBuilder: A non-repudiation scheme for IoT cloud applications. Computers & Security, 116, 102664. doi: 10.1016/j.cose.2022.102664

[10] De Cremer, David, Bang Nguyen, and Lyndon Simkin. "The integrity challenge of the Internet-of-Things (IoT): on understanding its dark side." Journal of Marketing Management 33.1-2 (2017): 145-158. doi: 10.1080/0267257X.2016.1247517
[11] E. Georgescu, "The Complete Guide to IoT Security and What Every Business Owner Needs to Know" https://heimdalsecurity.com/blog/iot-security-for-business/ [Megtekintve: 2022.12.12.]
[12] L. Göcs, Z.C. Johanyák, S. Kovács, "Review of Anomaly-Based IDS algorithms", TEAM 2016 : Proceedings of the 8th International Scientific and Expert Conference, Trnava, Slovakia : Alumni Press (2016) 360 p. pp. 58-63.
[13] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
[14] J. Hvizdoš, J. Vaščák, and A. Březina, "Object identification and localization by smart floors," Proceedings of IEEE 19th International Conference on Intelligent Engineering Systems (INES 2015), Bratislava, Slovakia, 2015, pp. 113-117, doi: 10.1109/INES.2015.7329649.
[15] IPv6 over Low power WPAN (6lowpan) https://datatracker.ietf.org/wg/6lowpan/documents/ [Megtekintve: 2022.12.12.]
[16] Lilik, F., Bukovics, Á., Kóczy, L.T. (2023). Fuzzy Inference System-like Aggregation Operator for Fuzzy Signatures. In: Cornejo, M.E., Harmati, I.Á., Kóczy, L.T., Medina-Moreno, J. (eds) Computational Intelligence and Mathematics for Tackling Complex Problems 4. Studies in Computational Intelligence, vol 1040. Springer, Cham. doi: 10.1007/978-3-031-07707-4_12
[17] R. Mohanakrishnan, "Top 10 Applications of IoT in 2022" https://www.spiceworks.com/tech/iot/articles/top-applications-internet-of-things/ [Megtekintve: 2022.12.12.]
[18] Muthuramalingam, S., et al. "IoT based intelligent transportation system (IoT-ITS) for global perspective: A case study." Internet of Things and Big Data Analytics for Smart Generation. Springer, Cham, 2019. 279-300. https://fardapaper.ir/mohavaha/uploads/2020/02/Fardapaper-IoT-Based-Intelligent-Transportation-System-IoT-ITS-for-Global-Perspective-A-Case-Study.pdf
[19] Pallavi Sethi, Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017. doi:10.1155/2017/9324035
[20] Piller I., Vincze D., Kovács Sz.: Declarative Language for Behaviour Description. In Emergent Trends in Robotics and Intelligent Systems. Advances in Intelligent Systems and Computing, vol 316. Springer, 2015. doi: 10.1007/978-3-319-10783-7_11
[21] L. Pokorádi (2009) "Risk Assessment Based upon Fuzzy Set Theory". In: 15th Building Services, Mechanical and Building Industry Days. Debreceni Egyetem, Debrecen, pp. 311-318. ISBN 978-963-473-315-7
[22] Shrouf, F., Ordieres, J., & Miragliotta, G. (2014, December). Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm. In 2014 IEEE international conference on industrial engineering and engineering management (pp. 697-701). IEEE. 10.1109/IEEM.2014.7058728
[23] E. Staddon, V. Loscri, and N. Mitton, "Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey," Applied Sciences, vol. 11, no. 16, p. 7228, Aug. 2021, doi: 10.3390/app11167228.
[24] A. Strielkina, V. Kharchenko and D. Uzun, "Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 58-62, doi: 10.1109/DESSERT.2018.8409099.
[25] Sudha, M.N., Rajendiran, M., Specht, M. et al. A low-area design of two-factor authentication using DIES and SBI for IoT security. J Supercomput 78, 4503–4525 (2022). doi: 10.1007/s11227-021-04022-w
[26] K. Tagade, "A Comprehensive Guide to IoT Security Testing", https://www.getastra.com/blog/security-audit/iot-security-testing/ [Megtekintve: 2022.12.23.]
[27] D. Terdiman, "At Home With Mark Zuckerberg And Jarvis, The AI Assistant He Built For His Family", https://www.fastcompany.com/3066478/mark-zuckerberg-jarvis [Megtekintve: 2022.12.23.]
[28] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in IEEE Access, vol. 9, pp. 28177-28193, 2021, doi: 10.1109/ACCESS.2021.3052867.
[29] C. -W. Tsai, C. -F. Lai, M. -C. Chiang and L. T. Yang, "Data Mining for Internet of Things: A Survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 77-97, First Quarter 2014, doi: 10.1109/SURV.2013.103013.00206.
[30] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," Information Systems Frontiers, vol. 17, no. 2, pp. 261-274, 2015. doi: 10.1007/s10796-014-9489-2
[31] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," Future Generation Computer Systems, vol. 49, pp. 104-112, 2015. doi: 10.1016/j.future.2014.10.010
[32] Zhihong Yang, Yingzhao Yue, Yu Yang, Yufeng Peng, Xiaobo Wang and Wenji Liu, "Study and application on the architecture and key technologies for IOT," 2011 International Conference on Multimedia Technology, Hangzhou, 2011, pp. 747-751, doi: 10.1109/ICMT.2011.6002149.