EVALUATING THE INTEROPERABILITY OF IOT DEVICES AND CLOUD ENVIRONMENTS IN INTELLIGENT BUILDING SYSTEMS

AZ IOT-ESZKÖZÖK ÉS A FELHŐKÖRNYEZETEK INTEROPERABILITÁSÁNAK ÉRTÉKELÉSE INTELLIGENS ÉPÜLETRENDSZEREKBEN

SÁNDOR Barnabás[1] – RAJNAI Zoltán[2]

Abstract

Integrating IoT devices and cloud environments is critical to developing and designing intelligent building systems. However, ensuring interoperability poses significant challenges, including data security and standardized communication. This research assesses the interoperability of IoT devices and cloud environments in intelligent building systems. It includes a description of advanced security protocols, data protection safeguards, and standardized communication interfaces. Cloud computing for real-time processing and analysis of IoT data will be presented, facilitating intelligent decision-making and optimization of building functions.

Keywords

Smart Building, IoT Cloud Environment, Cybersecurity Framework, Building Management, Data Security and Privacy

Absztrakt

Az IoT eszközöknek és a felhő-környezeteknek az integrálása kulcsfontosságú az intelligens épület-rendszerek fejlesztéseés kialakítása szempontjából. Az interoperabilitás biztosítása azonban jelentős kihívásokat jelent, többek között az adatbiztonság és a szabványosított kommunikáció terén. Ez a kutatás az IoT-eszközök és a felhőkörnyezetek interoperabilitását értékeli az intelligens épületrendszerekben. Magában foglalja a fejlett biztonsági protokollokat, az adatvédelmet megőrző intézkedéseket és a szabványosított kommunikációs interfészek ismertetését. Bemutatásra kerül a felhőalapú számítástechnika az IoT-adatok valós idejű feldolgozásához és elemzéséhez, megkönnyítve az intelligens döntéshozatalt és az épületfunkciók optimalizálását.

Kulcsszavak

Intelligens épület, IoT felhőkörnyezet, Kiberbiztonsági keretrendszer, Épületüzemeltetés, Adatbiztonság

[1] sandor.barnabas@gmail.com | ORCID: 0000-0001-7133-8082 | PhD-student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] rajnai.zoltan@bgk.uni-obuda.hu | ORCID: 0000-0002-9139-736X | dean, professor, Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering| dékán, egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

Az IoT technológia úttörőként jelent meg, amely forradalmasította a mindennapi életünk számos aspektusát, beleértve az épületek üzemeltetését és felhasználását. Az intelligens épületrendszerek, amelyek számos IoT-eszközzel, például érzékelőkkel, működtető elemekkel és beágyazott rendszerekkel vannak felszerelve, megkönnyítik az adatok valós idejű gyűjtését, feldolgozását és elemzését, lehetővé téve az intelligens döntéshozatalt és az épületfunkciók optimalizálását. Ehhez elengedhetetlen, hogy a felhőkörnyezetek biztosítsák a szükséges infrastruktúrát az IoT-eszközök által generált hatalmas mennyiségű adat tárolásához, feldolgozásához és elemzéséhez, ezáltal fokozva az intelligens épületrendszerek képességeit.

Az IoT-eszközök és a felhőkörnyezetek intelligens épületrendszerekbe való integrálása összetett feladat, amely jelentős kihívásokat jelent informatikai, kiberbiztonsági és műszaki szempontból is. A legkritikusabb kihívás az interoperabilitás, az kiberbiztonság és az adatvédelem biztosítása. Az interoperabilitás létfontosságú a különböző IoT-eszközök és felhőkörnyezetek közötti zökkenőmentes kommunikáció és interakció lehetővé tételéhez. Ez teszi lehetővé az eszközök és rendszerek egységes működését az intelligens épületrendszerekben. Az adatbiztonság és a magánélet védelme szintén kulcsfontosságú, mivel az IoT-eszközök által gyűjtött és feldolgozott adatok érzékenyek. Az intelligens épületrendszerekbe vetett bizalom megteremtése megköveteli ezen adatok biztonságának és adatvédelmének biztosítását.

E kutatásnak célja volt az IoT-eszközök és a felhőkörnyezetek interoperabilitásának értékelése az intelligens épületrendszerekben, miközben az kiberbiztonság és az adatvédelem kritikus kihívásaira fókuszálni. Egy komplex rendszer foglalja a fejlett biztonsági protokollokat, a magánélet védelmét szolgáló mechanizmusokat és a szabványosított kommunikációs interfészeket. A tanulmány fókusza a felhőalapú számítástechnika az IoT-adatok valós idejű feldolgozása és elemzése, megkönnyítve az intelligens döntéshozatalt és az épületfunkciók optimalizálását.

INTEROPERABILITÁSI KIHÍVÁSOK AZ INTELLIGENS ÉPÜLETRENDSZEREKBEN

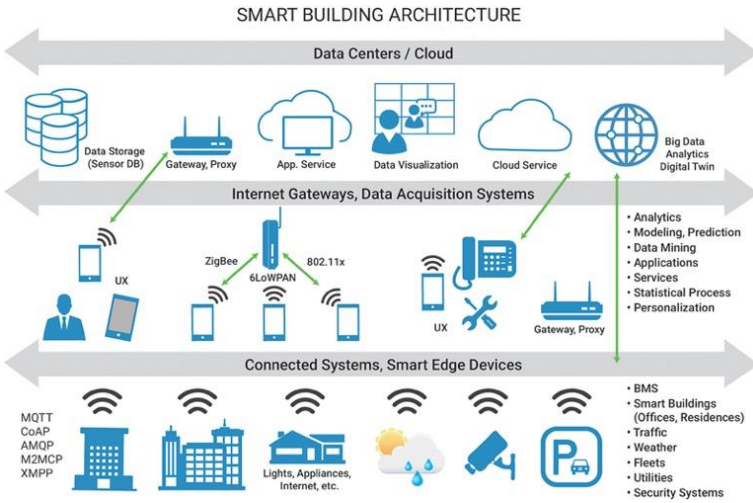
A dolgok internetétének megjelenése a különböző ágazatok kiterjedt integrációját eredményezte, ami az átalakító intelligens technológiák korszakát jelzi. Ennek a trendnek egyik jelentős haszonélvezője az építőipar. Ebben a részben Az intelligens épületek és az IoT kapcsolatának kölcsönhatását vizsgáltuk. Az intelligens épületek a modern építési gyakorlatok megtestesítői, amelyek fejlett technológiákat használnak az energiahatékonyság, a kényelem és az épület általános irányításának javítására. Működésükben központi szerepet játszik az IoT - egy olyan innovatív technológia, amely megkönnyíti az összekapcsolt eszközök közötti adatcserét. [1]

Az IoT integrálása az intelligens épületekbe a technológia és a szerkezeti tervezés érdekes keverékét kínálja, olyan intelligens szerkezeteket hozva létre, amelyek önállóan alkalmazkodnak a környezeti feltételekhez és a felhasználói igényekhez. Célünk ebben a részben megvilágítaani ezeket a fogalmakat, részletes betekintést nyújt az intelligens épületek és az IoT meghatározásába, szinergikus működésükbe, valamint a mai digitális korban rejlő forradalmi lehetőségekbe.

Az átjárhatóság az intelligens épületrendszerek egyik legfontosabb szempontja, amely lehetővé teszi a különböző eszközök és rendszerek zökkenőmentes együttműködését. Az intelligens épületrendszerek interoperabilitásának megvalósítása azonban számos kihívást jelent.

Eszközök az intelligens épületeken belül

Az intelligens épületrendszerekben különböző eszközöket, például érzékelőket, (fény, CO_2, levegőminőség), működtetőket (ablaknyitó) és vezérlőket használnak, és az egyes eszközök különböző kommunikációs protokollokat, adatformátumokat és interfészeket használhatnak. ***(1. Ábra)*** Ez a heterogenitás megnehezíti a különböző eszközök és rendszerek egységes és működőképes épületirányítási rendszerbe történő integrálását. Emellett számos gyártó saját megoldásokat kínál az intelligens épületrendszerekhez, amelyek nem feltétlenül kompatibilisek más gyártók eszközeivel és rendszereivel. Ez a gyártóspecifikus megközelítés akadályozza az interoperabilitást, mivel a gyártóhoz való kötődéshez vezet, és csökkenti az épületirányítási rendszer rugalmasságát. [2]



1. Ábra: Okos Épület IoT architecktúra, powersystemsdesign.com

Felhőkörnyezetek az intelligens épületekben

A felhőkörnyezetek kulcsfontosságúak az intelligens épületrendszerekben, mivel platformot biztosítanak az adatok tárolásához, feldolgozásához és elemzéséhez. Az IoT-eszközök felhőkörnyezetekkel való integrálása azonban számos kihívást jelent, beleértve az kiberbiztonságot, az adatvédelmet és az interoperabilitást. A felhőszolgáltatók különböző adatformátumokat, API-kat és kommunikációs protokollokat használhatnak, ami kihívás elé állítja az IoT-eszközök integrálását a felhőkörnyezetekkel. Az IoT-eszközök és a felhőkörnyezetek közötti adattovábbítás során jogi, biztonsági és adatvédelmi aggályok is felmerülhetnek. [3]

Az IoT-eszközök és a felhőkörnyezetek integrációjának kihívásai

Az IoT-eszközök és a felhőkörnyezetek intelligens épületrendszerekbe történő integrálása több problémát vet fel. Első sorban az intelligens épületrendszerek kommunikációs protokolljai és interfészei nincsenek szabványosítva. Bár több szabványügyi szervezet,

például a Nemzetközi Szabványügyi Szervezet (ISO), a Nemzetközi Elektrotechnikai Bizottság (IEC) és az épületautomatizálási és vezérlőhálózatok (BACnet) szabványokat dolgozott ki az épületautomatizálási rendszerek kommunikációjára, ezek a szabványok nincsenek általánosan elfogadva. Másodsorban a biztonság az átjárhatóság másik jelentős problémája. A különböző eszközök és rendszerek integrálása biztonsági résekkel járhat, mivel az egyes eszközök és rendszerek eltérő biztonsági jellemzőkkel és sebezhetőségekkel rendelkezhetnek.

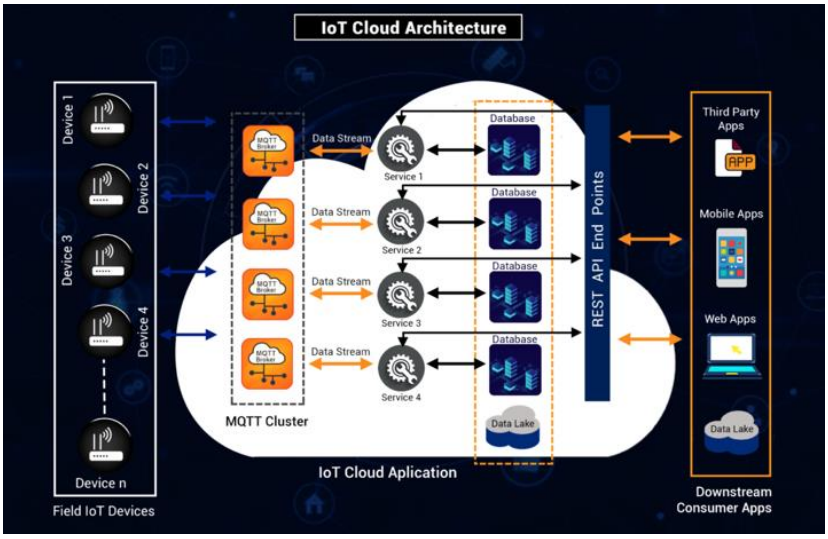
2022-ben az Európai Unióban 2022/2555 irányelvként megjelent a NIS2, melynek célja a kiberbiztonság növelése az alapvető szolgáltatók körében, a kiberbiztonság ésszerűsítése szigorúbb biztonsági követelmények és a jogsértésekért kiszabható szankciók révén, valamint az EU kibertámadásokkal szembeni felkészültségének javítása. Ebbe beletartoznak az IoT eszközök is. [4]

E kihívások kezelése érdekében ajánlott szabványosított kommunikációs protokollok és interfészek, például a BACnet, a KNX vagy a Zigbee használata, amelyek közös platformot biztosítanak a különböző eszközök és rendszerek kommunikációjához és integrálásához. Emellett fontos figyelembe venni a különböző eszközök és rendszerek integrációjának biztonsági vonatkozásait, és megfelelő biztonsági intézkedéseket kell végrehajtani az épületirányítási rendszer biztonságának és integritásának biztosítása érdekében.

AZ IOT-FELHŐKÖRNYEZET VÉDELME AZ INTELLIGENS ÉPÜLETEKBEN

Az IoT elterjedése forradalmasította az épületüzemeltetést, így a hagyományos épületeket intelligens, energiahatékony és felhasználóbarát környezetté alakította át. Az egymással összekapcsolt IoT-eszközökkel felszerelt intelligens épületek megkönnyítik a különböző épületfunkciók, például a világítás, fűtés, szellőzés, légkondicionálás (HVAC), biztonság és energiagazdálkodás valós idejű felügyeletét, vezérlését, így az energiahatékonyság optimalizálását. [5] A felhőkörnyezetek és az intelligens épületekben lévő IoT-eszközök integrálása lehetővé teszi az ezen eszközök által generált hatalmas mennyiségű adat tárolását, feldolgozását és elemzését, ezáltal javítva az épületirányítási rendszerek képességeit. [6]

Az IoT-eszközök és a felhőkörnyezetek intelligens épületekbe történő integrálása azonban jelentős kihívásokat jelent a kiberbiztonság, jog és a műszaki megvalósítások terén. Az IoT-eszközök által gyűjtött és feldolgozott adatok érzékeny jellege miatt széleskörű intézkedésekre van szükség a titkosság, integritás és rendelkezésre állás (CIA-követelmények) biztosítása érdekében. [7] A ***2. Ábrán*** látható, hogy az egyes rendszerek közötti kommunikácó és szeparáció mekkora szerepet játszik a kiberbiztonág területén. Továbbá az intelligens épületekben a különböző eszközök és rendszerek interoperabilitása aggályokat vet fel a kommunikációs interfészek és protokollok szabványosításával kapcsolatban.



2. Ábra: IoT Felhő architecktóra, www.embitel.com

E kihívások kezelése érdekében fejlett biztonsági protokollok, adatvédelem, megőrző mechanizmusokat és szabványosított kommunikációs interfészeket kerülnek bemutatásra. Továbbá kiemelésker került az adatbiztonság és az adatvédelem kritikus szerepe az intelligens épületrendszerekbe vetett bizalom kiépítésében, és kiemeli a szabványosított kommunikáció fontosságát a hatékony épületirányítás szempontjából.

Protokollok

Az IoT eszközök és az okosépületek felhőkörnyezetének integrálása adatbiztonsági szempontból megfelelő adatátviteli és titkosítási protokollokat követel meg. Tekintettel arra, hogy a feldolgozott és tárolt adatok megfeleljenek a CIA-követelményeinek. Az adatbiztonság kiemelkedő fontosságú az intelligens épületrendszerekben, mivel az IoT-eszközök által gyűjtött és feldolgozott adatok olyan érzékeny információkat tartalmazhatnak, mint például a foglaltsági minták, az energiafogyasztás és a biztonsági kamerák felvételei, felhasználók biometrikus adatai. [8] Továbbá az intelligens épületekben a különböző eszközök és rendszerek interoperabilitása aggályokat vet fel a kommunikációs interfészek és protokollok szabványosításával kapcsolatban.

- **Titkosítási protokollok**

A titkosítás az adatbiztonsági protokollok alapvető eleme. Magában foglalja az egyszerű szövegű adatok rejtjelezett szöveggé alakítását egy kriptográfiai kulcs segítségével, így azok az illetéktelen felhasználók számára értelmezhetetlenné válnak [9]. Az IoT-eszközök és a felhőkörnyezetek között továbbított adatok védelmére különböző titkosítási algoritmusok, például az Advanced Encryption Standard (AES), a Rivest Cipher (RC4) és az Data Encryption Standard (DES) alkalmazhatók. [10]

Az AES egy szimmetrikus titkosítási algoritmus, amely ugyanazt a kulcsot használja a titkosításhoz és a visszafejtéshez. Magas biztonsági szintje és számítási hatékonysága miatt széles körben használják különböző alkalmazásokban. [11] Az RC4 egy olyan folyamkódolás, amely pszeudo-véletlen bitekből álló kulcsfolyamot generál, amelyet aztán

a rejtjelezett szöveg előállítása érdekében XOR-olnak az egyszerű szöveggel. Az RC4-ről azonban kiderült, hogy számos sebezhetőséggel rendelkezik, és már nem tekinthető biztonságosnak. [12] A DES egy blokkos titkosítás, amely fix méretű blokkokban titkosítja az adatokat, de szintén nem tekinthető biztonságosnak a kis kulcsméret és a brute-force támadásokra való fogékonysága miatt. [13]

Ezért az intelligens épületekben az IoT-eszközök és a felhőkörnyezetek között továbbított adatok titkosítására az AES ajánlott. Az AES nagy biztonságot nyújt és számítási szempontból hatékony, így alkalmas az erőforrás-korlátozott IoT-eszközökhöz.

- **Hitelesítési protokollok**

A hitelesítés az adatbiztonsági protokollok másik kritikus eleme. Ez magában foglalja a felhasználó, az eszköz vagy a rendszer személyazonosságának ellenőrzését, mielőtt hozzáférést biztosítana egy erőforráshoz vagy szolgáltatáshoz. [14] Az intelligens épületek IoT-felhőkörnyezetének biztosítására különböző hitelesítési protokollok, például a PAP (Password Authentication Protocol), a CHAP (Challenge Handshake Authentication Protocol) és az EAP (Extensible Authentication Protocol) alkalmazhatók. [15]

A PAP egy egyszerű hitelesítési protokoll, amely a felhasználónevet és a jelszót egyszerű szövegben küldi a hálózaton keresztül. A PAP azonban a lehallgatási támadásokra való érzékenysége miatt nem tekinthető biztonságosnak. [15] A CHAP egy biztonságosabb hitelesítési protokoll, amely háromirányú kézfogást és kihívás-válasz mechanizmust tartalmaz. A kiszolgáló kihívást küld az ügyfélnek, aki egy egyirányú hash-függvény és egy megosztott titok segítségével kiszámított értékkel válaszol. [16] Az EAP egy rugalmas hitelesítési keretrendszer, amely különböző hitelesítési módszereket támogat, például token-kártyákat, intelligens kártyákat és digitális tanúsítványokat. [17]

Az EAP használata ajánlott az IoT-eszközök és a felhőkörnyezetek hitelesítésére az intelligens épületekben. Az EAP nagy biztonságot és rugalmasságot nyújt, így különböző alkalmazásokhoz és eszközökhöz alkalmas.

- **IoT-specifikus protokollok**

Az IoT-eszközök egyedi jellemzői, például az erőforráskorlátok, az időszakos kapcsolódás és a valós idejű követelmények speciális, az IoT-környezetre szabott biztonsági protokollokat tesznek szükségessé. Különböző IoT-specifikus biztonsági protokollokat fejlesztettek ki az IoT-eszközök és az intelligens épületekben lévő felhőkörnyezetekkel való kommunikációjuk biztosításának kihívásaira. [18]

Lightweight Cryptography

A „könnyű kriptográfia” a kriptográfia egy olyan ága, amelyet erőforrás-korlátozott eszközök, például IoT-eszközök számára terveztek. A hagyományos kriptográfiai algoritmusok, például az AES, túl számításigényesek lehetnek egyes IoT-eszközök számára, ami megnövekedett energiafogyasztáshoz és késleltetéshez vezet. [19] Könnyű kriptográfiai algoritmusokat, például a PRESENT és a SIMON-t úgy fejlesztették ki, hogy a hagyományos algoritmusokhoz hasonló szintű biztonságot nyújtsanak, de csökkentett számítási követelményekkel. [20]

A PRESENT egy erőforrás-korlátozott eszközökre tervezett, könnyű blokkos titkosítás. Blokkmérete 64 bit és 80 és 128 bit kulcsméretet támogat. A SIMON a Nemzeti Biz-

tonsági Ügynökség (NSA) által tervezett könnyűsúlyú blokkos titkosítások családja. Különböző blokkméreteket és kulcsméreteket támogat, így különböző alkalmazásokhoz alkalmas. [21]

Biztonságos kommunikációs protokollok

A biztonságos kommunikációs protokollok elengedhetetlenek az IoT-eszközök és a felhőkörnyezetek között továbbított adatok titkosságának, integritásának és rendelkezésre állásának biztosításához. Az IoT-eszközök számára különböző biztonságos kommunikációs protokollokat fejlesztettek ki, például a Datagram Transport Layer Security (DTLS), a Constrained Application Protocol (CoAP) és a Message Queuing Telemetry Transport (MQTT). [22]

A DTLS a Transport Layer Security (TLS) protokoll egy adatcsomag-alapú kommunikációra tervezett változata. A TLS-szel azonos szintű biztonságot nyújt, de alkalmas a IoT eszközöket tartalmazó alkalmazásokban általánosan használt User Datagram Protocol (UDP) protokollal való használatra. [22] A CoAP egy speciális webes átviteli protokoll korlátozott csomópontok és hálózatok számára. Könnyű és hatékony mechanizmust biztosít az IoT-eszközök és a felhőkörnyezetek közötti kommunikációhoz. Az MQTT egy könnyű üzenetküldési protokoll, amelyet kis érzékelők és mobil eszközök számára terveztek. Megbízható és hatékony mechanizmust biztosít az IoT-eszközök és a felhőkörnyezetek közötti kommunikációhoz.

Az intelligens épületek IoT-felhőkörnyezetének biztonságossá tételéhez könnyű kriptográfiai algoritmusok, például a PRESENT vagy a SIMON, valamint biztonságos kommunikációs protokollok, például a DTLS, a CoAP vagy az MQTT használata ajánlott. Ezek a protokollok magas szintű biztonságot nyújtanak, miközben alkalmasak az erőforrás-korlátozott IoT-eszközökhöz.

Adatvédelmi mechanizmusok

Az adatvédelem kiemelkedő fontosságú napjainkban, tekintettel arra, hogy az intelligens épületekben az IoT-eszközök által generált és feldolgozott adatok olyan érzékeny információkat tartalmaznak, mint a foglaltsági minták, az energiafogyasztás és a biztonsági kamerák felvételei. [23] Ezen adatok adatvédelmének biztosítása kulcsfontosságú az intelligens épületrendszerekbe vetett bizalom kiépítéséhez.

- **Az adatok anonimizálása**

Az adatok anonimizálásának célja a személyazonosításra alkalmas információk (PII) eltávolítására használnak az adathalmazokból, megnehezítve a rosszindulatú szereplők számára az adatok konkrét személyekhez való hozzárendelését. [24] Különböző adatanonimizálási technikákat, például a k-anonimitást, az L-diverzitást és a T-closeness technikát fejlesztettek ki a magánélet különböző szintű védelmének biztosítására. [25]

A K-anonimitás biztosítja, hogy az anonimizált adathalmaz minden egyes rekordja megkülönböztethetetlen legalább k-1 másik rekordtól bizonyos azonosító attribútumok tekintetében. [24] Az L-diverzitás kiterjeszti a k-anonimitást annak biztosításával, hogy az azonos azonosító attribútumokkal rendelkező rekordok minden egyes csoportja legalább l "jól reprezentált" értékkel rendelkezik az érzékeny attribútumok tekintetében. [25] A T-

closeness biztosítja, hogy egy érzékeny attribútum eloszlása az azonos azonosító attribútumokkal rendelkező rekordok bármely csoportjában közel áll a teljes adathalmazban való eloszláshoz. [26]

Ezen adatanonimizálási technikák kombinálása ajánlott az intelligens épületekben található IoT-eszközök által gyűjtött és feldolgozott adatok adatvédelmének biztosítása érdekében. Például a k-anonimitás, majd az L-diverzitás és a T-closeness alkalmazása magas szintű adatvédelmet biztosíthat, miközben megőrzi az adatok hasznosságát.

- **Biztonságos többszereplős számítás (SMPC)**

Az SMPC egy olyan kriptográfiai technika, amely lehetővé teszi, hogy több fél közösen számítson ki egy függvényt a bemeneteiken, miközben a bemeneteket titokban tartja.[27] Az SMPC különösen hasznos az intelligens épületek adatelemzésének adatvédelmére, ahol több érdekelt félnek, például az épület tulajdonosainak, bérlőinek és szolgáltatóinak együtt kell működniük az adatelemzésben anélkül, hogy felfednék egymás előtt a privát adataikat. [28]

Különböző SMPC protokollokat, például a Garbled Circuits protokollt és a Secret Sharing protokollt fejlesztettek ki, hogy különböző szintű biztonságot és hatékonyságot biztosítsanak. [27][29] A Garbled Circuits protokoll a kiszámítandó függvény torzított változatának létrehozását és a felek közötti torzított értékek cseréjét foglalja magában [27]. A Secret Sharing protokoll a bemeneteket részekre osztja és szétosztja a felek között, akik ezután részeredményeket számolnak ki a részükön, és ezeket kombinálva kapják meg a végeredményt. [29]

Az SMPC használata ajánlott az intelligens épületek adatainak adatvédelmet biztosító elemzésére. Az SMPC lehetővé teszi, hogy több érdekelt fél együttműködjön az adatelemzésben anélkül, hogy felfedné magánadatait, ezáltal növelve az intelligens épületrendszerek adatvédelmét és megbízhatóságát.

Szabványosított kommunikáció az épületüzemeltetés számára

A hatékony kommunikáció az épületirányítási rendszerek kritikus eleme, különösen az intelligens épületekben, amelyek számos IoT-eszközre támaszkodnak különböző funkciók, például az energiagazdálkodás, a biztonság és az épületet használók kényelme szempontjából. A szabványosított kommunikációs protokollok és interfészek elengedhetetlenek az épületirányítási rendszerek átjárhatóságának, biztonságának és hatékonyságának biztosításához. [30] Tekintettel arra, hogy más-más hatótávolságon és frekvencián működnek. ***(3. Ábra)*** Így a biztonságuk is más felkészültséget igénye.

Vezeték nélküli kommunikáció

A vezeték nélküli kommunikáció egyre népszerűbbé válik az épületirányítási rendszerekben a rugalmassága, a könnyű telepíthetősége és a különböző IoT-eszközökkel való integrálhatósága miatt. Az intelligens épületekben általában több vezeték nélküli kommunikációs technológiát használnak, köztük a Wi-Fi, a Bluetooth, a Zigbee, a LoRa és a KNX RF technológiákat.

- **Wi-Fi**

A Wi-Fi egy széles körben használt vezeték nélküli kommunikációs technológia, amely nagy sebességű internet- és hálózati kapcsolatokat biztosít. Általánosan használják

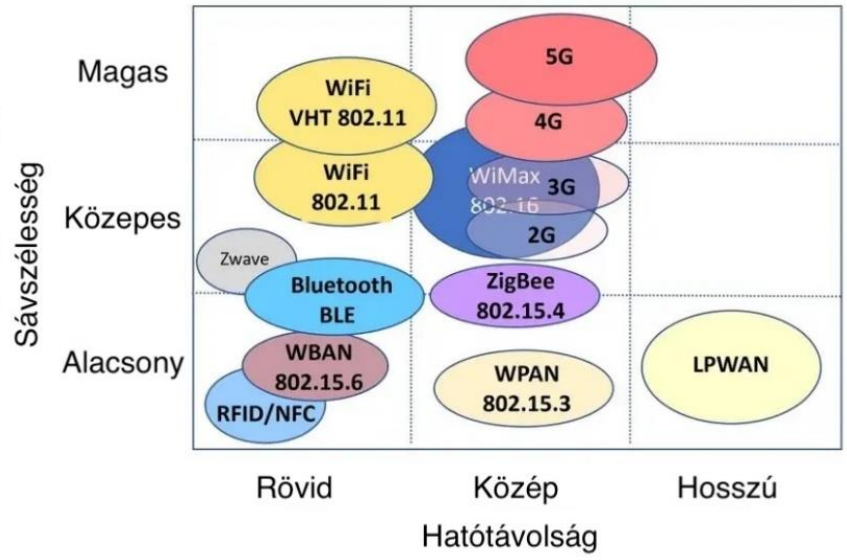
az intelligens épületekben a különböző IoT-eszközök, például érzékelők, működtetők és vezérlők épületirányítási rendszerhez való csatlakoztatására. [31]

- **Bluetooth**

A Bluetooth egy kis hatótávolságú vezeték nélküli kommunikációs technológia, amely kis területen, jellemzően legfeljebb 10 méteres körzetben csatlakoztatja az eszközöket. Általában az intelligens épületekben használják olyan eszközök, mint a termosztátok, világításvezérlők és biztonsági kamerák csatlakoztatására az épületirányítási rendszerhez. [32]

- **Zigbee**

A Zigbee egy alacsony fogyasztású, alacsony adatátviteli sebességű vezeték nélküli kommunikációs technológia, amelyet az eszközök hálós hálózatba kapcsolására terveztek. Általában intelligens épületekben használják érzékelők, működtetők és vezérlők hálós hálózatba kapcsolására, ami redundanciát biztosít és növeli a kommunikáció megbízhatóságát.[30]



3. Ábra: Vezeték nélküli kapcsolatok összehasonlítása, saját készítésű

- **LoRa**

A LoRa (Long Range) egy nagy hatótávolságú, kis teljesítményű vezeték nélküli kommunikációs technológia, amelyet úgy terveztek, hogy nagy távolságokra, jellemzően akár 10 kilométeres távolságokra is összekapcsolja az eszközöket. Általában intelligens épületekben használják egymástól távol lévő eszközök, például kültéri érzékelők és működtetők összekapcsolására. [33]

- **KNX RF**

A KNX RF (Radio Frequency) az épületautomatizáláshoz használt KNX protokollcsalád részét képező vezeték nélküli kommunikációs szabvány. Az épületautomatizálási

rendszerben lévő eszközök rádiófrekvenciás kommunikációval történő összekapcsolására szolgál. A KNX RF szabványosított kommunikációs interfészt biztosít az épületautomatizálási rendszer különböző eszközei, például érzékelők, működtetők és vezérlők számára. [34]

A vezeték nélküli kommunikációs technológiák döntő szerepet játszanak az épületirányítási rendszerek átjárhatóságában, biztonságában és hatékonyságában. Az intelligens épület egyedi követelményeitől, például a hatótávolságtól, az adatátviteli sebességtől és az energiafogyasztástól függően ajánlott e technológiák kombinációját használni.

Kommunikációs védelem

A kiberbiztonság az épületirányítási rendszerek kommunikációjának másik kritikus szempontja. A szabványosított kommunikációs protokollok gyakran tartalmaznak olyan biztonsági funkciókat, mint a titkosítás, a hitelesítés és az integritás ellenőrzése, amelyek biztosítják az átvitt adatok titkosságát, hitelességét és integritását. [3].

Az épületirányítási rendszerek kommunikációs biztonságának biztosítása érdekében ajánlott a beépített biztonsági funkciókkal rendelkező szabványosított kommunikációs protokollok használata. Ez segít megvédeni a továbbított adatokat a jogosulatlan hozzáféréstől, módosítástól vagy nyilvánosságra hozataltól, ezáltal növelve az épületirányítási rendszer biztonságát és megbízhatóságát.

Kommunikáció hatékonysága

A hatékonyság szintén lényeges szempont az épületirányítási rendszerek kommunikációjában. A szabványosított kommunikációs protokollok gyakran tartalmaznak adattömörítést, hibaérzékelést és -javítást, valamint a szolgáltatásminőség (QoS) kezelését a hatékony kommunikáció biztosítása érdekében. [32]

A BACnet szabvány például számos szolgáltatást tartalmaz, például a ReadPropertyMultiple szolgáltatást és a WritePropertyMultiple szolgáltatást, amelyek lehetővé teszik egy BACnet objektum több tulajdonságának egyetlen kéréssel történő olvasását és írását, ezáltal csökkentve a kommunikációs többletköltséget. [35]

A hatékony kommunikáció biztosítása érdekében az épületirányítási rendszerekben ajánlott a beépített hatékonysági jellemzőkkel rendelkező szabványosított kommunikációs protokollok használata. Ez segít csökkenteni a kommunikációs többletköltséget, ezáltal javítva az épületfelügyeleti rendszer teljesítményét és reakciókészségét.

AZ ADATBIZTONSÁG ÉS AZ ÉPÜLETÜZEMELTETÉS ÉRTÉKELÉSE

Az adatbiztonság kritikus fontosságú az épületirányítási rendszerek számára, különösen az intelligens épületekben, amelyek számos IoT-eszközre támaszkodnak különböző funkciók, például az energiagazdálkodás, a biztonság és a kényelem szempontjából. Az épületirányítási rendszerek adatbiztonságának értékelésére összpontosítása a cél ezen fejezetben.

Értékelési kritériumok és mérőszámok

Az épületirányítási rendszerek adatbiztonságának értékelése különböző kritériumok és mérőszámok értékelését foglalja magában. Ezek a következők lehetnek:

- **Bizalmasság:** Annak biztosítása, hogy az IoT-eszközök és az épületirányítási rendszer között továbbított adatok csak az arra jogosultak számára legyenek hozzáférhetők. Ez magában foglalja a titkosítási algoritmusok és biztonságos kommunikációs protokollok végrehajtását az adatokhoz való jogosulatlan hozzáférés megakadályozása érdekében.
- **Sértetlenség:** Annak biztosítása, hogy az IoT-eszközök és az épületirányítási rendszer között továbbított adatokat az átvitel során ne hamisítsák meg vagy ne változtassák meg. Ez magában foglalja az ellenőrző összegek és digitális aláírások végrehajtását az adatok integritásának.
- **Rendelkezzésre állás:** Annak biztosítása, hogy az IoT-eszközök és az épületirányítási rendszer között továbbított adatok szükség esetén rendelkezésre álljanak. Ez magában foglalja a redundancia és a failover mechanizmusok megvalósítását az adatok folyamatos rendelkezésre állásának biztosítása.
- **Hitelesítés:** Csak engedélyezett eszközök és rendszerek kommunikálhatnak az épületirányítási rendszerrel. Ez magában foglalja a hitelesítési mechanizmusok, például jelszavak, digitális tanúsítványok és biometrikus adatok bevezetését az eszközök és rendszerek személyazonosságának ellenőrzésére.
- **Engedélyezés**: Annak biztosítása, hogy csak az engedélyezett eszközök és rendszerek férhessenek hozzá az épületirányítási rendszer adataihoz és módosíthassák azokat. Ez magában foglalja a hozzáférés-szabályozási mechanizmusok, például a hozzáférés-szabályozási listák és a szerepkör-alapú hozzáférés-szabályozás megvalósítását, hogy az eszközökhöz és rendszerekhez rendelt jogosultságok alapján korlátozzák az adatokhoz való hozzáférést.
- **Letagadásmentesség:** Annak biztosítása, hogy az üzenet küldője ne tudja letagadni az üzenet elküldését, a címzett pedig ne tudja letagadni az üzenet fogadását. Ez magában foglalja a digitális aláírások és időbélyegzők alkalmazását az adatok eredetének és kézhezvételének bizonyítására.
- **Rugalmasság:** Annak biztosítása, hogy az épületirányítási rendszer gyorsan helyre tudjon állni bármilyen biztonsági incidensből, és továbbra is megfelelően működjön. Ez magában foglalja az incidensekre való reagálási eljárások, valamint a biztonsági mentési és helyreállítási mechanizmusok végrehajtását, hogy a rendszer a biztonsági incidens után visszaálljon a normál állapotba.
- **Ellenőrizhetőség:** Annak biztosítása, hogy az épületirányítási rendszerben minden tevékenységet naplóznak és ellenőrizhetővé tesznek. Ez magában foglalja a naplózási mechanizmusok és ellenőrzési nyomvonalak bevezetését a rendszerben végzett valamennyi tevékenység rögzítése és a végrehajtott tevékenységek elszámoltathatóságának biztosítása érdekében.

Sérülékenységvizsgálat és eredmények

Az épületirányítási rendszerek kiber,- és adatbiztonságának értékeléséhez sérülékenységvizsgálatot kell lefolytatni a végrehajtott biztonsági intézkedések hatékonyságának értékelésére. Ezek a kísérletek magukban foglalhatják különböző kibertámadások - például adatlefoglalás, adatmanipuláció és szolgáltatásmegtagadási támadások - szimulálását, és az épületirányítási rendszer e támadásokra adott válaszának értékelését.

Értelmezés és következtetések

A vizsgálatok eredményei értelmezhetők az épületirányítási rendszerben végrehajtott biztonsági intézkedések hatékonyságának meghatározása érdekében. Tegyük fel, hogy az épületirányítási rendszer sikeresen megakadályozza a szimulált kibertámadásokat, és biztosítja az adatok titkosságát, sértetlenségét és rendelkezésre állását. Ebben az esetben megállapítható, hogy a bevezetett biztonsági intézkedések hatékonyak. Ha azonban az épületirányítási rendszer nem tudja megakadályozni a szimulált kibertámadásokat, vagy bármilyen sebezhetőséget azonosítanak, az azt jelenti, hogy a potenciális biztonsági kockázatokkal foglalkozni kell. E megállapítások következményei között szerepelhet a végrehajtott biztonsági intézkedések felülvizsgálatának, további biztonsági ellenőrzések végrehajtásának vagy az épületirányítási rendszer újratervezésének szükségessége a biztonság fokozása érdekében.

KÖVETKEZTETÉSEK ÉS JÖVŐBELI IRÁNYOK

Az IoT-eszközök és a felhőkörnyezetek integrálása az intelligens épületekben számos kihívást jelent, többek között az adatbiztonság, az adatvédelem és az interoperabilitás terén. Ez a publikáció feltárta ezeket a kihívásokat, és lehetséges megoldásokat javasolt. Az épületirányítási rendszerek adatbiztonságának értékelése különböző kritériumok értékelését foglalja magában, beleértve a bizalmasságot, az integritást, a rendelkezésre állást, a hitelesítést, a felhatalmazást, a letagadásmentességet, a rugalmasságot és az ellenőrizhetőséget. A titkosítási algoritmusok, biztonságos kommunikációs protokollok, ellenőrző összegek, digitális aláírások, hozzáférés-szabályozási mechanizmusok, incidensekre reagáló eljárások és naplózási mechanizmusok megvalósítása elengedhetetlen az épületirányítási rendszer biztonságának és integritásának biztosításához.

Az intelligens épületirányítási rendszerek másik jelentős kihívása az interoperabilitás. A különböző eszközök, például érzékelők, működtetők és vezérlők különböző kommunikációs protokollokat, adatformátumokat és interfészeket használhatnak, ami kihívássá teszi integrálásukat egy egységes és működőképes épületirányítási rendszerbe. Biztonsági és adatvédelmi aggályok is felmerülhetnek az IoT-eszközök és a felhőkörnyezetek közötti adattovábbítás során. E kihívások kezelése érdekében ajánlott szabványosított kommunikációs protokollok és interfészek, például BACnet, KNX vagy Zigbee használata, valamint megfelelő biztonsági intézkedések végrehajtása az épületirányítási rendszer biztonságának és integritásának biztosítása érdekében.

Kutatásunkat folytatva a cél egy átfogó és kiterjedt auditálható kiberbiztonsági keretrendszer kidolgozása az okos épületek auditálhatósága szempontjából, ahol a fő fókusz az IoT rendszerekre irányul. Ezzel is segítve a tervezőket, kivitelezőket, döntéshozókat és auditorokat, hogy egy meghatározott irányvonal mentén tudjanak megfelelő döntésket hozni egy intelligen épület IoT kiberbiztonsága kapcsán.

Összefoglalva, az intelligens épületrendszerek adatbiztonságának és átjárhatóságának biztosítása alapvető fontosságú az épületirányítási rendszerek sikeres megvalósításához és működtetéséhez. A szabványosított kommunikációs protokollok és interfészek, valamint a megfelelő biztonsági intézkedések bevezetése megoldhatja ezeket a kihívásokat, és biztosíthatja az intelligens épületrendszerek biztonságos és hatékony működését. A jövőbeni kutatásoknak a fejlettebb biztonsági protokollok és kommunikációs interfészek fejlesztésére

kell összpontosítaniuk, hogy kezelni tudják az intelligens épületrendszerek fejlődő biztonsági fenyegetéseit és interoperabilitási kihívásait.

FELHASZNÁLT IRODALOM[3]

[1] R. A. Abdelouahid, O. Debauche, és A. Marzak, „Internet of things: a new Interoperable IoT platform. Application to a smart building”, *Procedia Comput. Sci.*, köt. 191, o. 511–517, 2021.

[2] W. Granzer, F. Praus, és W. Kastner, „Security in building automation systems”, *IEEE Trans. Ind. Electron.*, köt. 57, sz. 11, o. 3622–3630, 2009.

[3] B. Sándor és Z. Rajnai, „Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View”, *Interdiscip. Descr. Complex Syst. INDECS*, köt. 21, sz. 2, o. 141–147, 2023.

[4] „AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE”, 2022. december 14. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX%3A32022L2555 (elérés 2023. szeptember 1.).

[5] V. M. Rohokale, N. R. Prasad, és R. Prasad, „A cooperative Internet of Things (IoT) for rural healthcare monitoring and control”, in *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, febr. 2011, o. 1–6. doi: 10.1109/WIRELESSVITAE.2011.5940920.

[6] A. Botta, W. De Donato, V. Persico, és A. Pescapé, „Integration of cloud computing and internet of things: a survey”, *Future Gener. Comput. Syst.*, köt. 56, o. 684–700, 2016.

[7] F. Vahid és T. D. Givargis, *Embedded system design: a unified hardware/software introduction*. John Wiley & Sons, 2001.

[8] L. Cui, G. Xie, Y. Qu, L. Gao, és Y. Yang, „Security and privacy in smart cities: Challenges and opportunities”, *IEEE Access*, köt. 6, o. 46134–46145, 2018.

[9] W. Stallings, „CRYPTOGRAPHY AND NETWORKSECURITY PRINCIPLES ANDPRACTICE”, 2011.

[10] A. Dorri, S. S. Kanhere, R. Jurdak, és P. Gauravaram, „Blockchain for IoT security and privacy: The case study of a smart home”, előadás 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), IEEE, 2017, o. 618–623.

[11] D. S. Abd Elminaam, H. M. Abdual-Kader, és M. M. Hadhoud, „Evaluating The Performance of Symmetric Encryption Algorithms.”, *Int J Netw Secur*, köt. 10, sz. 3, o. 216–222, 2010.

[12] N. AlFardan, D. J. Bernstein, K. G. Paterson, B. Poettering, és J. C. Schuldt, „On the security of {RC4} in {TLS}”, előadás 22nd USENIX Security Symposium (USENIX Security 13), 2013, o. 305–320.

[13] D. Coppersmith, „The Data Encryption Standard (DES) and its strength against at

[14] A. Juels, „Minimalist cryptography for low-cost RFID tags”, előadás Security in Communication Networks: 4th International Conference, SCN 2004, Amalfi, Italy, September 8-10, 2004, Revised Selected Papers 4, Springer, 2005, o. 149–164.

[15] T. Dierks és E. Rescorla, „The transport layer security (TLS) protocol version 1.2”, 2070–1721, 2008.
[16] W. Simpson, „PPP challenge handshake authentication protocol (CHAP)”, 2070–1721, 1996.
[17] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, és H. Levkowetz, „Extensible authentication protocol (EAP)”, 2070–1721, 2004.
[18] J. Granjal, E. Monteiro, és J. Sá Silva, „Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues”, *IEEE Commun. Surv. Tutor.*, köt. 17, sz. 3, o. 1294–1312, 2015, doi: 10.1109/COMST.2015.2388550.
[19] A. Menezes, P. Sarkar, és S. Singh, „Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography”, előadás International Conference on Cryptology in Malaysia, Springer, 2016, o. 83–108.
[20] A. Bogdanov *és mtsai.*, „PRESENT: An ultra-lightweight block cipher”, előadás Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9, Springer, 2007, o. 450–466.
[21] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, és L. Wingers, „The SIMON and SPECK families of lightweight block ciphers”, *Cryptol. Eprint Arch.*, 2013.
[22] E. Rescorla és N. Modadugu, „Datagram transport layer security version 1.2”, 2070–1721, 2012.
[23] R. Yu, G. Xue, V. T. Kilari, és X. Zhang, „Deploying robust security in internet of things”, előadás 2018 IEEE Conference on Communications and Network Security (CNS), IEEE, 2018, o. 1–9.
[24] L. Sweeney, „k-anonymity: A model for protecting privacy”, *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, köt. 10, sz. 05, o. 557–570, 2002.
[25] A. Machanavajjhala, D. Kifer, J. Gehrke, és M. Venkitasubramaniam, „l-diversity: Privacy beyond k-anonymity”, *ACM Trans. Knowl. Discov. Data TKDD*, köt. 1, sz. 1, o. 3-es, 2007.
[26] N. Li, T. Li, és S. Venkatasubramanian, „t-closeness: Privacy beyond k-anonymity and l-diversity”, előadás 2007 IEEE 23rd international conference on data engineering, IEEE, 2006, o. 106–115.
[27] A. C. Yao, „Protocols for secure computations”, előadás 23rd annual symposium on foundations of computer science (sfcs 1982), IEEE, 1982, o. 160–164.
[28] D. Bogdanov, S. Laur, és J. Willemson, „Sharemind: A framework for fast privacy-preserving computations”, előadás Computer Security-ESORICS 2008: 13th European Symposium on Research in Computer Security, Málaga, Spain, October 6-8, 2008. Proceedings 13, Springer, 2008, o. 192–206.
[29] A. Shamir, „How to share a secret”, *Commun. ACM*, köt. 22, sz. 11, o. 612–613, 1979.
[30] W. Granzer és W. Kastner, „Security analysis of open building automation systems”, előadás Computer Safety, Reliability, and Security: 29th International Conference, SAFECOMP 2010, Vienna, Austria, September 14-17, 2010. Proceedings 29, Springer, 2010, o. 303–316.
[31] J. Han, C.-S. Choi, W.-K. Park, I. Lee, és S.-H. Kim, „Smart home energy management system including renewable energy based on ZigBee and PLC”, *IEEE Trans. Consum. Electron.*, köt. 60, sz. 2, o. 198–202, 2014.

[32] W. Kastner, G. Neugschwandtner, S. Soucek, és H. M. Newman, „Communication systems for building automation and control”, *Proc. IEEE*, köt. 93, sz. 6, o. 1178–1203, 2005.
[33] L. Trinh, V. X. Bui, F. Ferrero, T. Nguyen, és M. Le, „Signal propagation of LoRa technology using for smart building applications”, előadás 2017 IEEE Conference on Antenna Measurements & Applications (CAMA), IEEE, 2017, o. 381–384.
[34] A. S. Shah, H. Nasir, M. Fayaz, A. Lajis, és A. Shah, „A review on energy consumption optimization techniques in IoT based smart building environments”, *Information*, köt. 10, sz. 3, o. 108, 2019.
[35] A. Fernbach, W. Granzer, és W. Kastner, „Interoperability at the management level of building automation systems: A case study for BACnet and OPC UA”, előadás ETFA2011, IEEE, 2011, o. 1–8.