ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

SÁNDOR BARNABÁS

Okos épületek kiberbiztonsági intézkedéseinek vizsgálata

Témavezető: Prof. Dr. Rajnai Zoltán

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024.03.11.

Tartalomjegyzék

1 Summary

In the digital transformation era, smart buildings stand at the forefront of innovation, integrating Internet of Things (IoT) technologies to create more efficient, responsive, and sustainable environments. However, this integration introduces complex cybersecurity challenges, necessitating robust protection mechanisms to safeguard sensitive data and ensure system integrity. This thesis delves into the cybersecurity landscape of smart buildings, focusing on the vulnerabilities introduced by IoT devices and the potential of artificial intelligence (AI) to fortify security measures. The research embarked on a comprehensive examination of existing cybersecurity frameworks, including ISO27001 and ISO30141, alongside an in-depth analysis of the General Data Protection Regulation (GDPR), the Network and Information Systems Directive (NIS2), and the Cyber Resilience Act to understand their applicability and limitations in the context of smart buildings. A significant portion of the study involved conducting interviews with industry professionals, which provided valuable insights into real-world challenges and practices in securing smart building ecosystems.

Key findings highlight a critical gap in cybersecurity frameworks regarding specific IoT vulnerabilities, such as inadequate default configurations, limited update mechanisms, and insecure communication protocols. The research also underscored the potential of AI in enhancing cybersecurity through predictive analytics and anomaly detection, offering a proactive approach to identifying and mitigating threats.

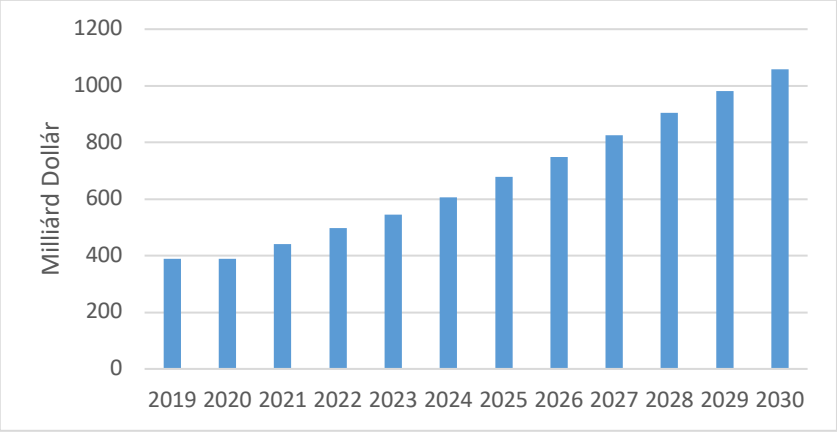
The thesis proposes an integrated cybersecurity framework that combines the rigor of established standards with the adaptability of AI-driven solutions. This framework emphasizes the importance of continuous monitoring, regular updates, and adopting a Zero Trust architecture to ensure comprehensive security across all layers of smart building systems.

In conclusion, this research contributes to the evolving field of smart building cybersecurity by providing a nuanced understanding of the challenges posed by IoT technologies and offering a strategic roadmap for integrating AI into cybersecurity practices. Future research directions include exploring blockchain for secure device authentication, developing energy-efficient security solutions, and enhancing user-centric security frameworks to empower occupants with greater control over their data and privacy.

This thesis advances academic understanding and offers practical insights for industry professionals, paving the way for more secure, intelligent, and user-friendly smart buildings in the digital age.

2 A kutatás előzményei

A dolgok internetének (Internet of Things - IoT) elterjedése az elmúlt években megváltoztatta életmódunkat és a környezettel való interakciónkat. Az IoT iparban 2019 és 2023 között közel 41%-os növekedést volt mérhető a piacon, amely a termékekre és szolgáltatásokra érthető. (1. ábra)



1. ábra: IoT piac globális bevétele 2019 és 2030 között *[1]*

Az egyik ilyen átalakulás az épületek okos terekké alakítása és automatizálása volt, ahol az érzékelők és okos eszközök segítségével történő adatgyűjtés értékes információkkal szolgál az energiahatékonyság, a munkavállalók komfortérzetének, hatékonyságának és az épület általános teljesítményének javításhoz. Azonban ez a fokozott összekapcsolhatóság és információmegosztás kiberbiztonsági kockázatot hordoz magában, amelyet nem lehet figyelmen kívül hagyni. Más IoT-rendszerekhez hasonlóan az okos épületek is ki vannak téve olyan kiberfenyegetéseknek, amelyek veszélyeztethetik a munkavállalók magánszféráját vagy fizikai biztonságát, illetve károsíthatják a berendezéseket és ezáltal megzavarhatják a vállalat működését. Ezért egyre fontosabbá válik, hogy hatékony kiberbiztonsági intézkedéseket hozzunk az okos épületek biztonságos működésének biztosítása érdekében.

Értekezésem bevezetőjében áttekintést kívánok nyújtani arról, hogy az IoT hogyan alakította át az épületeket különböző célú adatgyűjtést alkalmazó okos terekké. Fontos kiemelnem, hogy ezek a fejlesztések tudományos aggályokat vetnek fel a biztonsági kérdésekkel kapcsolatban. Az okos eszközök és rendszerek potenciális sebezhetősége komoly veszélyt jelent a munkavállalók biztonságára és magánéletére, miközben a kibertámadások által okozott berendezések károsodása miatt működési zavarok felléphetnek. Ezért szükség van olyan mélyreható kutatásra, amely célja olyan átfogó megoldások nyújtása, amelyek hatékonyan csökkentik az IoT-alapú okos épületekhez kapcsolódó biztonsági kockázatokat. Ugyanakkor kiemelném az okos épületekben a megnövekedett összekapcsolhatóság és adatmegosztás

biztonsági kockázatait is. A bevezetőben végül hangsúlyt fogok fektetni arra, hogy az innovatív épületkörnyezetekben hatékony kiberbiztonsági intézkedésekre van szükség a munkavállalók bizonyos fokú magánszférájának és biztonságának védelme, valamint a zavartalan működés biztosítása érdekében.

A téma aktualitását alátámasztja, hogy a 2023. március 3-án megalakult Magyar Okosotthon és Épületautomatizálási Szövetség, rövid nevén Okosotthon Szövetség. A szövetség 14 tagvállalattal kezdte meg működését. A Szövetség célja, hogy egységes kommunikációval segítse a végfelhasználókat és a szakembereket a piac és a hozzá kapcsolódó megoldások megismerésében, valamint, hogy közelebb hozza a szakértőket és a döntéshozókat a hatékony és sikeres együttműködés érdekében. Továbbá céljai között szerepel az is, hogy egyfajta tájékozódási pontként, valamint szakmai fórumként szolgáljon az okosotthonok és az épületautomatika területén működő vállalkozások és szakemberek, a képző intézmények és egyéb szervezetek, valamint az állami döntéshozók számára. A szervezet számára kiemelten fontos a kiberbiztonság, így önálló Oktatási Szakosztállyal rendelkezik, melynek jelenleg én töltöm be az elnöki szerepét. Célunk, hogy a hazai szakmában iránymutatást adjunk a szakembereknek és a végfelhasználóknak. Ebbe beletartoznak a tervező és kivitelező mérnökök, akik akár egy komplex okos épületet is tervezhetnek. Ennek érdekében 2023-ban együttműködési megállapodást kötöttünk az Óbudai Egyetem - Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán indult Domotika szakmérnök/szaktanácsadó képzéssel, ahol kiemelt oktatási területek közé tartozik a kiberbiztonság.

3 Célkitűzések

Az értekezésem célja az okos épületek IoT-rendszerei együttműködő védelmi stratégiájának vizsgálata és kidolgozása az érdekelt felek - köztük a gyártók, a szolgáltatók és a felhasználók - közötti fenyegetés-felderítési információmegosztás beépítésével. A cél az okos épületek kiberbiztonságának fokozása és a kiberfenyegetések mérséklése. Az alábbi konkrét kutatási célokat tűztem ki.

- Az okos épületek IoT-érintettjei - köztük a gyártók, szolgáltatók és felhasználók - jelenlegi helyzetének, valamint a fenyegetésekkel kapcsolatos információk megosztásával kapcsolatos meglévő gyakorlatuknak és képességeiknek a feltárása.
- Elemezni a fenyegetésinformációk megosztásának, mint közös védelmi stratégiának az okos épületek IoT-rendszereihez kapcsolódó előnyeit és kihívásait.
- A fenyegetésekkel kapcsolatos információk hatékony és biztonságos megosztása keretrendszerének kidolgozása az érdekelt felek között, figyelembe véve a magánélet védelmével kapcsolatos aggályokat, a jogi megfontolásokat és az okos épületrendszerek sokszínűségét.
- A különböző folyamatok és technológiák vizsgálata és elemzése a fenyegetésekkel kapcsolatos információk időben és hatékonyan történő gyűjtésére, elemzésére és terjesztésére.
- Kísérletek elvégzése annak felmérésére, hogy a fenyegetésekkel kapcsolatos információk megosztása milyen hatással van a rendszerbiztonság javítására, beleértve a kiberfenyegetések észlelését és mérséklését az okos épületek IoT-környezetében.
- Iránymutatás és ajánlás kidolgozása az érdekel felek számára a hatékony fenyegetettségi információk megosztására vonatkozó gyakorlatok megvalósítására és elfogadására vonatkozóan, beleértve az információmegosztás, a bizalomépítés és az együttműködésen alapuló védelmi stratégiák legjobb gyakorlatait.

E célok elérésével ez a kutatás hozzájárul az okos IoT-épületek kiberbiztonságának fejlesztéséhez azáltal, hogy az érdekelt felek közötti fenyegetés-felderítési információk megosztásának beépítésével együttműködő védelmi stratégiát hozna létre. Ez az együttműködésen alapuló megközelítés elősegíti az erősebb biztonsági helyzet kialakulását, lehetővé téve az érdekeltek számára, hogy proaktívan észleljék az okos épületek IoT-rendszereinek kiberfenyegetéseit, reagáljanak azokra, és enyhítsék azokat.

4 Vizsgálati módszerek

Kutatásom alapját a primer kutatása adja, amely során versenyszférában szerzett saját tapasztalataimra építve vizsgáltam meg több aspektusból az okos épületeket kiberbiztonsági szempontból. Ebben az esetben a kutatási módszer egy összehasonlítóelemzés volt. Ezt továbbá segítette, hogy részt vettem Magyarország egyik legmodernebb és egyedülálló okos épületének a MOL Campus kiberbiztonsági szempontból fontos tényezőinek kezelésében is. Összehasonlító elemzést végeztem néhány kiemelt meglévő kiberbiztonsági keretrendszeren és szabványon. Továbbá a terület komplexitásának és újdonságtartalmának köszönhetően szakértői mélyinterjúkat készítetek hazai szakemberekkel, akiknek a kiberbiztonság és okos épületek a szakterülete. Használtam továbbá logikai kutatási módszerek is, mint az indukció, a dedukció, az analízis a szintézis és az absztrakció.

5 Új tudományos eredmények

Értekezésemben a kiberbiztonság és az okos épületek kapcsolatát vizsgáltam. A primer kutatásom során összehasonlító elemzést végeztem néhány kiemelt kiberbiztonsági keretrendszeren és szabványon, ahol megvizsgáltam, hogy az okos épületeknél hogyan alkalmazható és milyen hiányosságokkal rendelkezik. Ezeket alátámasztottam szakmai interjúkkal, melyeket olyan hazai szakemberekkel készítettem, akik a kiberbiztonság és az okos épületek területén több éves tapasztalattal rendelkeznek. Tekintettel arra, hogy én is gyakorló szakember vagyok, így résztvevői megfigyelés keretében beépítettem a saját tapasztalataim, melyeket az elmúlt közel 15 év során szereztem. Elkészítettem egy kiberbiztonsági ellenőrzőlistát, melyet az okos épületek tervezésekor és üzemeltetésekor lehet használni a kiberbiztonság növelés érdekében. A szekunder kutatáshoz forrásokat dolgoztam fel dokumentumelemzés formájában. Kutatási eredményeimet értekezésem logikai felépítése mentén ismertettem, így voltak olyan kutatási eredményeim melyek nem az empirikus, hanem a teoretikus részeknél szerepeltek. Ezekben az esetekben a megfogalmazással, illetve a táblázatok forrásának feltüntetésével egyértelműen utaltam erre.

Három hipotézist vizsgáltam értekezésem során, melyekkel kapcsolatban az alábbi megállapításokat teszem:

T1: Bizonyítottam, hogy összeállítható egy kiberbiztonsági ellenőrzőlista, ami segíti az a kiberbiztonsági szempontoknak való megfelelést az okos épületekben. Erre kidolgoztam az ellenőrzőlista egy alkalmazható változatát. [S1] [S2] [S6]

T2: Bizonyítottam, hogy összeállítható egy olyan referenciamodell, amely az okos épületeket ért kibertámadásokat csökkentheti. [S2] [S3] [S4]

T3: Összehasonlítóelemzéssel igazoltam, hogy a meglévő kiberbiztonsági keretrendszerekből és szabványokból hiányzik az okos épületekre vonatkozó kiberbiztonsági ajánlás. Ennek érdekében javaslatokat tettem azok bővítésére. [S5]

6 Az eredmények hasznosítási lehetősége

Értekezésem célja az volt, hogy azon kiberbiztonsági szakemberek és szervezetek számára segítsek, akik okos épületek IoT rendszereit tervezik és/vagy üzemeltetik. Olyan problémákra adtam javaslatot, melyek súlyos hiányosságok a különféle kiberbiztonsági keretrendszerekben és szabványokban az okos épületek kiberbiztonságát tekintve. Értekezésem ajánlom:

- Kiberbiztonsági tervezők számára, akik IoT rendszereket terveznek okos épületekbe.
- Kiberbiztonsági üzemeltetők számára, akik a meglévő rendszereket átveszik üzemeltetésre.
- IoT szakemberek számára, akik növelni szeretnék a kiberbiztonságot az IoT eszközeik, rendszereik területén.
- Vállalatok számára, akik okos épületet terveznek, vagy üzemeltetnek.
- Eredményeimet ajánlom széles körben felhasználni a kiberbiztonság területén műszaki ajánlás szintjén.

7 Új kutatási irányra tett javaslatok

A kutatást az alábbi irányokban folytatnám a jövőben, tekintettel arra, hogy az okos épületek és IoT eszközök és rendszerek folyamatosan terjednek el és így válnak a kibertámadások célpontjaivá.

- MI-vezérelt prediktív kiberbiztonság intelligens épületek számára

  Az intelligens épületek potenciális kiberbiztonsági fenyegetéseinek előrejelzésére alkalmas MI-algoritmusok kifejlesztésének és megvalósításának vizsgálata. Ebben a kutatásban olyan gépi tanulási modelleket vizsgálhat, amelyek a múltbeli adatokat elemzik a minták azonosítása és a jövőbeli sebezhetőségek vagy támadások előrejelzése érdekében.

- Blokklánc az intelligens épületek fokozott IoT-biztonságáért

  A blokklánc-technológia alkalmazásának vizsgálata az intelligens épületekben található IoT-eszközök biztonságának és integritásának javítása érdekében. Ez a kutatás olyan decentralizált biztonsági protokollokra összpontosíthat, amelyek a blokkláncot használják az adatintegritás és a biztonságos eszköz-eszköz kommunikáció biztosítására.

8 Irodalmi hivatkozások listája/ Irodalomjegyzék

[1] A. Jay, „Number of Internet of Things (IoT) Connected Devices Worldwide 2024: Breakdowns, Growth & Predictions”, Financesonline.com. Elérés: 2024. február 4. [Online]. Elérhető: https://financesonline.com/number-of-internet-of-things-connected-devices/

[2] F. Mattern és C. Floerkemeier, „From the Internet of Computers to the Internet of Things”, in *From Active Data Management to Event-Based Systems and More: Papers in Honor of Alejandro Buchmann on the Occasion of His 60th Birthday*, K. Sachs, I. Petrov, és P. Guerrero, Szerk., Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, o. 242–259. doi: 10.1007/978-3-642-17226-7_15.

[3] K. Ashton, „That “Internet of Things” Thing: In the Real World Things Matter More than Ideas”, *RFID J.*, köt. 22, sz. 7, o. 97–114, 2009.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, és E. Cayirci, „Wireless sensor networks: a survey”, *Comput. Netw.*, köt. 38, sz. 4, o. 393–422, 2002, doi: 10.1016/S1389-1286(01)00302-4.

[5] R. Want, „An introduction to RFID technology”, *IEEE Pervasive Comput.*, köt. 5, sz. 1, o. 25–33, 2006, doi: 10.1109/MPRV.2006.2.

[6] T. Givargis és F. Vahid, „Platune: A tuning framework for system-on-a-chip platforms”, *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, köt. 21, sz. 11, o. 1317–1327, 2002, doi: 10.1109/TCAD.2002.804107.

[7] C. Perera, A. Zaslavsky, P. Christen, és D. Georgakopoulos, „Sensing as a service model for smart cities supported by internet of things”, *Trans. Emerg. Telecommun. Technol.*, köt. 25, sz. 1, o. 81–93, 2014, doi: 10.1002/ett.2704.

[8] 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, doi: 10.1016/j.future.2015.09.021.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, és M. Ayyash, „Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, *IEEE Commun. Surv. Tutor.*, köt. 17, sz. 4, o. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[10] J. Tisóczki, „A mesterséges intelligencia alkalmazása az egészségügyi ellátási folyamatokban”, *Biztonságtudományi Szle.*, köt. 4, sz. 2. Ksz., o. 137–153, 2022.

[11] M. A. Abid *és mtsai.*, „Evolution towards Smart and Software-Defined Internet of Things”, *AI*, köt. 3, sz. 1, o. 100–123, 2022, doi: 10.3390/ai3010007.

[12] K. Lalitha, D. R. Kumar, C. Poongodi, és J. Arumugam, „Healthcare Internet of Things– The Role of Communication Tools and Technologies”, in *Blockchain, Internet of Things, and Artificial Intelligence*, Chapman and Hall/CRC, 2021, o. 331–348.

[13] R. S. Bisht, S. Jain, és N. Tewari, „Study of wearable IoT devices in 2021: Analysis & future prospects”, in *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, IEEE, 2021, o. 577–581. doi: 10.1109/ICIEM51511.2021.9445334.

[14] M. Wu és J. Luo, „Wearable technology applications in healthcare: a literature review”, *Online J Nurs Inf.*, köt. 23, sz. 3, 2019, [Online]. Elérhető: https://www.proquest.com/openview/6c96964dfb83ca06895f330233831a50/1?pq-origsite=gscholar&cbl=2034896

[15] M. S. Aliero, K. N. Qureshi, M. F. Pasha, és G. Jeon, „Smart Home Energy Management Systems in Internet of Things networks for green cities demands and services”, *Environ. Technol. Innov.*, köt. 22, o. 101443, 2021, doi: 10.1016/j.eti.2021.101443.

[16] S. Ahmetoglu, Z. Che Cob, és N. Ali, „Internet of Things Adoption in the Manufacturing Sector: A Conceptual Model from a Multi-Theoretical Perspective”, *Appl. Sci.*, köt. 13, sz. 6, Art. sz. 6, jan. 2023, doi: 10.3390/app13063856.

[17] B. Sándor és Z. Rajnai, „Okos épületek és az IoT: A globális gyakorlatok átfogó áttekintése”, *Biztonságtudományi Szle.*, köt. 5, sz. 2, o. 33–46, 2023.

[18] S. Selvaraj és S. Sundaravaradhan, „Challenges and opportunities in IoT healthcare systems: a systematic review”, *SN Appl. Sci.*, köt. 2, sz. 1, o. 139, dec. 2019, doi: 10.1007/s42452-019-1925-y.

[19] S. B. Junaid *és mtsai.*, „Recent Advances in Artificial Intelligence and Wearable Sensors in Healthcare Delivery”, *Appl. Sci.*, köt. 12, sz. 20, o. 10271, 2022, doi: 10.3390/app122010271.

[20] M. R. M. Kassim, „IoT Applications in Smart Agriculture: Issues and Challenges”, in *2020 IEEE conference on open systems (ICOS)*, IEEE, 2020, o. 19–24. doi: 10.1109/ICOS50156.2020.9293672.

[21] W.-S. Kim, W.-S. Lee, és Y.-J. Kim, „A review of the applications of the internet of things (IoT) for agricultural automation”, *J. Biosyst. Eng.*, köt. 45, o. 385–400, 2020, doi: 10.1007/s42853-020-00078-3.

[22] „State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally”, IoT Analytics. Elérés: 2024. február 4. [Online]. Elérhető: https://iot-analytics.com/number-connected-iot-devices/

[23] „Matter Specification, Version 1.0”. Connectivity Standards Alliance, Inc., 2022. szeptember 28. Elérés: 2023. december 19. [Online]. Elérhető: https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001_Matter-1.0-Core-Specification.pdf

[24] Connectivity Standards Alliance, „Matter 1.2 Arrives with Nine New Device Types & Improvements Across the Board”. Elérés: 2024. január 8. [Online]. Elérhető: https://csa-iot.org/newsroom/matter-1-2-arrives-with-nine-new-device-types-improvements-across-the-board/

[25] „Typical Thread Network Topologies - Smart Homes with Matter & Commercial Buildings > Thread Group”. Elérés: 2024. február 4. [Online]. Elérhető: https://www.threadgroup.org/news-events/blog/ID/291/Typical-Thread-Network-Topologies--Smart-Homes-with-Matter-Commercial-Buildings

[26] D. Coppens, A. Shahid, S. Lemey, B. Van Herbruggen, C. Marshall, és E. De Poorter, „An overview of UWB standards and organizations (IEEE 802.15. 4, FiRa, Apple): Interoperability aspects and future research directions”, *IEEE Access*, köt. 10, o. 70219–70241, 2022, doi: 10.1109/ACCESS.2022.3187410.

[27] „Thread 1.2 for Smart Buildings White Paper”. Thread Group, Inc., 2022. Elérés: 2023. december 19. [Online]. Elérhető: https://portal.threadgroup.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=3065

[28] P. Domingues, P. Carreira, R. Vieira, és W. Kastner, „Building automation systems: Concepts and technology review”, *Comput. Stand. Interfaces*, köt. 45, o. 1–12, 2016, doi: 10.1016/j.csi.2015.11.005.

[29] F. Mofidi és H. Akbari, „Intelligent buildings: An overview”, *Energy Build.*, köt. 223, o. 110192, 2020, doi: 10.1016/j.enbuild.2020.110192.

[30] 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, doi: 10.7906/indecs.21.2.2.

[31] B. Sandor és Z. Rajnai, „Smart Building IoT Cybersecurity: A Review of Threats and Mitigation Technique”, előadás 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics (SISY), IEEE, 2023, o. 321–326.

[32] M. M. Froufe, C. K. Chinelli, A. L. A. Guedes, A. N. Haddad, A. W. Hammad, és C. A. P. Soares, „Smart buildings: Systems and drivers”, *Buildings*, köt. 10, sz. 9, o. 153, 2020, doi: 10.3390/buildings10090153.

[33] B. Sándor és Z. Rajnai, „Az IoT-eszközök és a felhőkörnyezetek interoperabilitásának értékelése intelligens épületrendszerekben”, *Biztonságtudományi Szle.*, köt. 5, sz. 3, o. 47–61, 2023.

[34] J. Aftab, B. Ron, és R. Michael, „The Edge Amsterdam – showcasing an exemplary IoT building”. University of Cambridge, 2018. augusztus 20. Elérés: 2024. január 8. [Online]. Elérhető: https://www.cdbb.cam.ac.uk/news/2018CaseTheEdge

[35] K. Khurshid, A. Danish, M. U. Salim, M. Bayram, T. Ozbakkaloglu, és M. A. Mosaberpanah, „An in-depth survey demystifying the Internet of Things (IoT) in the construction industry: Unfolding new dimensions”, *Sustainability*, köt. 15, sz. 2, o. 1275, 2023, doi: 10.3390/su15021275.

[36] Construction Week, „Burj Khalifa has world’s third-fastest elevator”. Elérés: 2023. január 10. [Online]. Elérhető: https://www.constructionweekonline.com/projects-tenders/article-20616-burj-khalifa-has-worlds-third-fastest-elevator

[37] B. Deborah, „Apple Park”. Elérés: 2024. január 8. [Online]. Elérhető: https://arquitecturaviva.com/works/apple-park-1

[38] Green Building Magazine, „The Crystal - A Landmark Global Urban Sustainability Centre”. Elérés: 2024. január 8. [Online]. Elérhető: https://gbplusamag.com/the-crystal/

[39] S. K. Baduge *és mtsai.*, „Artificial intelligence and smart vision for building and construction 4.0: Machine and deep learning methods and applications”, *Autom. Constr.*, köt. 141, o. 104440, szept. 2022, doi: 10.1016/j.autcon.2022.104440.

[40] B. Pardamean, H. H. Muljo, T. W. Cenggoro, B. J. Chandra, és R. Rahutomo, „Using transfer learning for smart building management system”, *J. Big Data*, köt. 6, sz. 1, o. 110, dec. 2019, doi: 10.1186/s40537-019-0272-6.

[41] H. Farzaneh, L. Malehmirchegini, A. Bejan, T. Afolabi, A. Mulumba, és P. P. Daka, „Artificial intelligence evolution in smart buildings for energy efficiency”, *Appl. Sci.*, köt. 11, sz. 2, o. 763, 2021, doi: 10.3390/app11020763.

[42] T. A. Dovramadjiev, R. Dimova, D. Pavlova, és R. V. Filchev, „Applications of artificial intelligence in people & lifestyle based on education experience”, *Biztonságtudományi Szle.*, köt. 4, sz. 1. Ksz., o. 35–48, 2022.

[43] M. Klees és S. Evirgen, „Building a smart database for predictive maintenance in already implemented manufacturing systems”, *Int. Conf. Ind. Sci. Comput. Sci. Innov.*, köt. 204, o. 14–21, jan. 2022, doi: 10.1016/j.procs.2022.08.002.

[44] R. Panchalingam és K. C. Chan, „A state-of-the-art review on artificial intelligence for Smart Buildings”, *Intell. Build. Int.*, köt. 13, sz. 4, o. 203–226, okt. 2021, doi: 10.1080/17508975.2019.1613219.

[45] D. Sembroiz, D. Careglio, S. Ricciardi, és U. Fiore, „Planning and operational energy optimization solutions for smart buildings”, *Inf. Sci.*, köt. 476, o. 439–452, febr. 2019, doi: 10.1016/j.ins.2018.06.003.

[46] M. Tavakoli, F. Shokridehaki, M. Funsho Akorede, M. Marzband, I. Vechiu, és E. Pouresmaeil, „CVaR-based energy management scheme for optimal resilience and operational cost in commercial building microgrids”, *Int. J. Electr. Power Energy Syst.*, köt. 100, o. 1–9, szept. 2018, doi: 10.1016/j.ijepes.2018.02.022.

[47] A. Pejić és P. S. Molcer, „Predictive machine learning approach for complex problem solving process data mining”, *Acta Polytech. Hung.*, köt. 18, sz. 1, o. 45–63, 2021.

[48] Y. Xu, P. Ahokangas, M. Turunen, M. Mäntymäki, és J. Heikkilä, „Platform-Based Business Models: Insights from an Emerging AI-Enabled Smart Building Ecosystem”, *Electronics*, köt. 8, sz. 10, Art. sz. 10, okt. 2019, doi: 10.3390/electronics8101150.

[49] L. P. Kaelbling, M. L. Littman, és A. W. Moore, „Reinforcement learning: A survey”, *J. Artif. Intell. Res.*, köt. 4, o. 237–285, 1996, doi: 10.1613/jair.301.

[50] J. Reynolds, Y. Rezgui, A. Kwan, és S. Piriou, „A zone-level, building energy optimisation combining an artificial neural network, a genetic algorithm, and model predictive control”, *Energy*, köt. 151, o. 729–739, máj. 2018, doi: 10.1016/j.energy.2018.03.113.

[51] M. K. M. Shapi, N. A. Ramli, és L. J. Awalin, „Energy consumption prediction by using machine learning for smart building: Case study in Malaysia”, *Dev. Built Environ.*, köt. 5, o. 100037, márc. 2021, doi: 10.1016/j.dibe.2020.100037.

[52] Z. Liu, X. Zhang, Y. Sun, és Y. Zhou, „Advanced controls on energy reliability, flexibility and occupant-centric control for smart and energy-efficient buildings”, *Energy Build.*, köt. 297, o. 113436, okt. 2023, doi: 10.1016/j.enbuild.2023.113436.

[53] B. Qolomany *és mtsai.*, „Leveraging Machine Learning and Big Data for Smart Buildings: A Comprehensive Survey”, *IEEE Access*, köt. 7, o. 90316–90356, 2019, doi: 10.1109/ACCESS.2019.2926642.

[54] D. J. Fehér és B. Sándor, „Effects of the WPA2 KRACK Attack in Real Environment”, előadás 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), IEEE, 2018, o. 000239–000242.

[55] martinekuan, „Azure Cosmos DB in IoT workloads - Azure Solution Ideas”. Elérés: 2024. február 4. [Online]. Elérhető: https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/articles/iot-using-cosmos-db

[56] Forescout Research Labs, „The Enterprise of Things Security Report”, Forescout Research Labs, Version 01_21, 2021. Elérés: 2024. január 9. [Online]. Elérhető: https://www.forescout.com/resources/the-annual-connected-enterprise-report/

[57] A. G. Masid, J. B. Higuera, J.-R. B. Higuera, és J. A. S. Montalvo, „Application of the SAMA methodology to Ryuk malware”, *J. Comput. Virol. Hacking Tech.*, köt. 19, sz. 2, o. 165–198, jún. 2023, doi: 10.1007/s11416-022-00434-1.

[58] Forescout Vedere Labs, „The 5 Riskiest Connected Devices in 2023: IT, IoT, OT, IoMT”. Elérés: 2023. december 9. [Online]. Elérhető: https://www.forescout.com/blog/riskiest-connected-devices-it-iot-ot-iomt/

[59] Forescout Vedere Labs, „R4IoT: Next-Generation Ransomware”, Version 01_03, jún. 2022. o. 13-14. Elérés: 2023. január 5. [Online]. Elérhető: https://www.forescout.com/resources/r4iot-next-generation-ransomware-report

[60] CyberMDX és Vedere Labs, „Access:7 - How Supply Chain Vulnerabilities Can Allow Unwelcomed Access to Your Medical and IoT Devices”, Version B, 2022. Elérés: 2024. január 9. [Online]. Elérhető: https://www.forescout.com/resources/access-7-supply-chain-vulnerabilities-can-allow-unwelcomed-access-to-your-medical-and-iot-devices/

[61] dos S. Daniel, D. Stanislav, W. Jos, és A. Amine, „Amnesia:33 - How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices”, Forescout Research Labs, Version 12_20, 2020. o. 4. Elérés: 2023. december 31. [Online]. Elérhető: https://www.forescout.com/resources/amnesia33-identify-and-mitigate-the-risk-from-vulnerabilities-lurking-in-millions-of-iot-ot-and-it-devices/

[62] S. Rose, O. Borchert, S. Mitchell, és S. Connelly, „Zero Trust Architecture”, National Institute of Standards and Technology, aug. 2020. doi: 10.6028/NIST.SP.800-207. o. 5.

[63] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, és R. Doss, „Zero Trust Architecture (ZTA): A Comprehensive Survey”, *IEEE Access*, köt. 10, o. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.

[64] S. H. Li, „An overview of sustainable assessment tools of BREEAM, LEEDv4 and GB”, 7th International Conference on Energy and Environment of Residential …, nov. 2016. doi: 10.4225/50/581076f34a16a.

[65] A. Ferreira, M. D. Pinheiro, J. de Brito, és R. Mateus, „A critical analysis of LEED, BREEAM and DGNB as sustainability assessment methods for retail buildings”, *J. Build. Eng.*, köt. 66, o. 105825, máj. 2023, doi: 10.1016/j.jobe.2023.105825.

[66] P. Wu, Y. Song, X. Hu, és X. Wang, „A Preliminary Investigation of the Transition from Green Building to Green Community: Insights from LEED ND”, *Sustainability*, köt. 10, sz. 6, Art. sz. 6, jún. 2018, doi: 10.3390/su10061802.

[67] Dombora S. és Horváth G. K., „Információbiztonság integrált megvalósítása MSZ ISO/IEC 27001:2014, és IBTV. (NIST SP 800-53 rev 4) alapon”, előadás Kommunikáció 2015, Budapest: NKE Szolgáltató Kft., nov. 2015, o. 43–55. Elérés: 2024. január 10. [Online]. Elérhető: https://www.puskashirbaje.hu/pdf/Kommunikacio_2015-NSZTK.pdf

[68] ISO/IEC CD 30141:20160910 - "Information technology – Internet of Things Reference Architecture (IoT RA)". 2016, o. 44. Elérés: 2024.01.10. [Online] Elérhető: https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf

[69] J. T. F. T. Initiative, „Guide for Conducting Risk Assessments”, National Institute of Standards and Technology, NIST Special Publication (SP) 800-30 Rev. 1, szept. 2012. doi: 10.6028/NIST.SP.800-30r1.

[70] Joint Task Force Interagency Working Group, „Security and Privacy Controls for Information Systems and Organizations”, National Institute of Standards and Technology, szept. 2020. doi: 10.6028/NIST.SP.800-53r5.

[71] K. Kent és M. Souppaya, „Guide to Computer Security Log Management”, National Institute of Standards and Technology, NIST Special Publication (SP) 800-92, szept. 2006. doi: 10.6028/NIST.SP.800-92.

[72] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, és R. McQuaid, „Developing Cyber-Resilient Systems: A Systems Security Engineering Approach”, National Institute of Standards and Technology, NIST Special Publication (SP) 800-160 Vol. 2 Rev. 1, dec. 2021. doi: 10.6028/NIST.SP.800-160v2r1.

[73] M. Ogata, J. Franklin, J. Voas, V. Sritapan, és S. Quirolgico, „Vetting the Security of Mobile Applications”, National Institute of Standards and Technology, NIST Special Publication (SP) 800-163 Rev. 1, ápr. 2019. doi: 10.6028/NIST.SP.800-163r1.

[74] M. Fagan *és mtsai.*, „IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements”, National Institute of Standards and Technology, NIST Special Publication (SP) 800-213, nov. 2021. doi: 10.6028/NIST.SP.800-213.

[75] M. Fagan, K. Megas, K. Scarfone, és M. Smith, „Foundational Cybersecurity Activities for IoT Device Manufacturers”, National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR) 8259, máj. 2020. doi: 10.6028/NIST.IR.8259.

[76] European Union Agency for Cybersecurity, *Baseline security recommendations for IoT in the context of critical information infrastructures*. European Network and Information Security Agency, 2017. doi: 10.2824/03228.

[77] Európai Bizottság, *AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról (CRA)*. o. 93. Elérés: 2024. január 22. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52022PC0454

[78] Európai Unió, *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (GDPR)*. 2016, o. 88. Elérés: 2023. október 10. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32016R0679

[79] Európai Unió, *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE (NIS 2 irányelv)*. 2022, o. 73. Elérés: 2024. január 10. [Online]. Elérhető: https://eur-lex.europa.eu/eli/dir/2022/2555

[80] D. J. Fehér és B. Sándor, „Log File Authentication and Storage on Blockchain Network", in *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, szept. 2018, o. 000243–000248. doi: 10.1109/SISY.2018.8524848.

[81] D. J. Fehér és B. Sándor, „Examining the Relationship between the Bitcoin and Cybercrime", in *2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2019, o. 121–126. doi: 10.1109/SACI46893.2019.9111568.

[82] B. Sándor, „ Vulnerability Analysis of a Smart Heating System", Műszaki Tudományos Közlemények, 2019. vol. 9., 211-214., 4 p., doi: 10.33895/mtk-2018.09.48.

9 Publikációk

9.1 A tézispontokhoz kapcsolódó tudományos közlemények

S1. Sándor Barnabás: Vulnerability Analysis of a Smart Heating System. In: *Műszaki Tudományos Közlemények*, 2019. vol. 9., 211-214., 4 p., doi: 10.33895/mtk-2018.09.48

S2. Sándor Barnabás, Fehér Dávid János: Effects of the WPA2 KRACK Attack in Real Environment. In: 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), 239-242., 4 p., doi: 10.1109/SISY.2018.8524769

S3. Sándor Barnabás, Rajnai Zoltán: „Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View" in 2023 Interdisciplinary Description of Complex Systems (INDECS), Vol. 21 No. 2, 141-147., 7 p., doi: 10.7906/indecs.21.2.2

S4. Sándor Barnabás, Rajnai Zoltán: Okos épületek és az IoT: A globális gyakorlatok átfogó áttekintése" Biztonságtudományi Szemle, 2023. Vol. 5. No. 2, 33-46., 14 p., ISSN 2676-9042

S5. Sándor Barnabás, Rajnai Zoltán: Smart Building IoT Cybersecurity: A Review of Threats and Mitigation Technique" in 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics (SISY), 321-326., 6p., doi: 10.1109/SISY60376.2023.10417954

S6. B. Sándor, Z. Rajnai, „Az IoT-eszközök és a felhőkörnyezetek interoperabilitásának értékelése intelligens épületrendszerekben" Biztonságtudományi Szemle, 2023. Vol. 5. No. 3, 47-61., 15 p., ISSN 2676-9042

9.2 További tudományos közlemények

S7. Fehér Dávid János, Sándor Barnabás: „Log File Authentication and Storage on Blockchain Network” in 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), 243-248., 6 p., doi: 10.1109/SISY.2018.8524848

S8. Sándor Barnabás, Nagy Rudolf: Transzformátortüzek kialakulásának és tulajdonságainak vizsgálata” Védelem Tudomány, 2018.Vol III., No 4., 73-91., 19 p., ISSN 2494-6194

S9. Fehér Dávid János, Sándor Barnabás: „Common Scam Threat Examination on Real Environment”, Tavaszi Szél Tanulmánykötet, 2019. II. Kötet, 493-507., 12 p., ISBN 978-615-5586-61-3

S10. Sándor Barnabás, Fehér Dávid János: „Examining the Relationship between the Bitcoin and Cybercrime” in 2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI), 121-126., 6 p., doi: 10.1109/SACI46893.2019.9111568

S11. Sándor Barnabás, Fehér Dávid János: „Whom and What Can We Trust?: How Can We Steal Data With a USB Cable”, Tavaszi Szél Tanulmánykötet, 2019. II. Kötet, 74-81., 8 p., ISBN 978-615-5586-61-3

S12. Fehér Dávid János, Sándor Barnabás: „Cloud SaaS Security Issues and Challenges” in 2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI), 131-134., 4 p., doi: 10.1109/SACI46893.2019.9111529

Tisóczki József, Sándor Barnabás: „Digitális selyemút és egészségügyi informatika kapcsolatának vizsgálata”, Térerő - Erőtér: Tanulmányok a Kárpát-medencei geopolitikai konferencia előadásaiból, 2019., 152-161., 10 p., ISBN 9788081223365

S13. Sándor Barnabás, Fehér Dávid János: „Kiberbiztonsági bérek megoszlásának felmérése Magyarországon”, Vállalkozásfejlesztés a XXI. században, 2019. IX/1. tanulmánykötet, 227-238., 12 p., ISBN 978-963-449-166-8

S14. Sándor Barnabás, Nagy Rudolf: „Adatközpontok tűzbiztonságának vizsgálata” Védelem Tudomány, 2020.Vol V. No 1., 72-85., 14 p., ISSN 2494-6194

S15. Sándor Barnabás, Nagy Rudolf: „Description and investigation of IT systems used in disaster management” Védelem Tudomány, 2021.Vol VI. No 2., 239-242., 16 p., ISSN 2494-6194

S16. Sándor Barnabás: Warflying – 2.4 GHhz and 5 GHz wireless network detection by drone in critical infrastructure, in 2020 Cyber Security Review, ISSN 2055-6969, https://www.cybersecurity-review.com/articles/warflying-2-4-ghz-and-5-ghz-wireless-network-detection-by-drone-in-critical-infrastructure/

Elérhetőségek és azonosítók

- **MTMT azonosító:** 10064423
- **ODT:** 32485
- **ORCID:** 0000-0001-7133-8082
- **Google Scholar:** scholar.google.com/citations?user=pSqxGQUAAAAJ&hl
- **ResearchGate:** www.researchgate.net/profile/Barnabas-Sandor
- **Web of Science:** M-7380-2018
- **IEEE Xplore ID:** 37086507551
- **Academia:** independent.academia.edu/BarnabasSandor
- **Web:** www.sandorbarnabas.hu
- **LinkedIn:** www.linkedin.com/in/sandorbarnabas