BLOCKCHAIN-BASED SECURITY FRAMEWORK FOR IOT DEVICES

BLOKKLÁNC ALAPÚ BIZTONSÁGI KERETRENDSZER IOT ESZKÖZÖKRE

OLÁH Norbert[1] – NAGY Csaba Norbert[2]

Abstract

Nowadays, various Internet of Things (IoT) devices arise in many application areas (e.g. smart city, Internet of Drones). However, security incidents show that these systems are vulnerable. In our proposed solution, we explore the advantages and disadvantages of IoT devices and current relevant security issues. We suggested a solution to increase the security level of IoT systems, for which we proposed the application of blockchain technology. Our proposed framework considers the design considerations related to IoT (resource-constrained devices, scalability). We developed a user-friendly platform for the distributed storage of IoT device attributes on a permissioned (private) blockchain. The device manager has several features to provide a higher security level and fulfil security requirements (e.g. password setting, firmware update, two-factor authentication method).

Keywords

Security, IoT, Blockchain, Password setting, Firmware update

Absztrakt

Napjainkban a különböző Internet of Things (IoT) eszközök számos alkalmazási területen jelennek meg (pl. okosváros, drónok hálózata). Azonban a biztonsági incidensek azt mutatják, hogy sérülékenyek ezek a rendszerek. Az általunk javasolt megoldásban megvizsgáltuk az IoT eszközök előnyeit és hátrányait, illetve aktuális releváns biztonsági problémákat. Megoldást kerestünk az IoT rendszerek biztonsági szintjének növelésére, amelyre a blokklánc technológiát alkalmaztuk. Az általunk javasolt keretrendszer figyelembe veszi az IoT-val kapcsolatos tervezési szempontokat (erőforrás korlátozott eszközök, skálázhatóság). Kialakítottunk egy felhasználóbarát platformot, amely képes az IoT eszközök attribútumait egy engedélyköteles blokkláncon elosztott módon tárolni. Az eszközkezelő számos funkcióval rendelkezik, melyek növelik a biztonsági követelmények magasabb szintű megvalósítását. (pl. jelszó beállítás, firmware frissítés)

Kulcsszavak

Biztonság, IoT, Blokklánc, Jelszóbeállítás, Firmware frissítés

[1] olah.norbert@inf.unideb.hu | ORCID: 0000-0002-0007-8508 | Assistant Professor, University of Debrecen, Faculty of Informatics, Department of Data Science and Visualization| adjunktus, Debreceni Egyetem, Informatikai Kar, Adattudomány és Vizualizáció Tanszék

[2] nagy.csaba@inf.unideb.hu | ORCID: 0009-0009-0678-281X | technician, University of Debrecen, Faculty of Informatics, Department of Data Science and Visualization| technikus, Debreceni Egyetem, Informatikai Kar, Adattudomány és Vizualizáció Tanszék

BEVEZETÉS

A dolgok internete (IoT) napjaink egyik robbanásszerűen fejlődő területe. A fogalmat 1999-ben Kevin Ashton alkotta meg a Procter & Gamble számára tartott előadásában. A dolgok internetét, azaz az Internet of Things-t (IoT) egy olyan technológiaként fogalmazta meg, amely az 1983-ban megjelent RFID (Radio Frequency Indentification) segítségével több eszközt kapcsol össze. Napjainkban az IoT eszközökből álló rendszerek az életünk minden területén megjelennek, ilyen alkalmazásai többek között okosvárosok, az okosotthonok, az intelligens tömegközlekedés, az intelligens egészségügy vagy a dolgok ipari környezete (IIoT). Az IoT eszközök piaca dinamikusan nő, ahol a 2015-ös becslésben mért 15 milliárd eszközről 2025-re több mint 75 milliárd eszközt jósolnak a kutatók ([1]). Ez az előrejelzés azt jelenti, hogy 2 év múlva átlagosan minden embernek a Földön 5-10 személyes IoT eszköz lesz a birtokában.

Az IoT rendszerek terjedését és alkalmazását nagyban segíti annak számos előnye. Az IoT érzékelők működtetésével a vállalkozásoknak nagy mennyiségű valós idejű információ áll a rendelkezésére, melynek elemzésével képesek optimalizálni a munkafolyamatokat, csökkenthetik a működési költségeket és jobb ügyfélélményt biztosíthatnak. A szenzorok mellett a különböző beavatkozó eszközök (aktuátorok) fokozhatják a termelékenységet és növelhetik a munkahelyi biztonságot. Erre példa az autógyártó Ford, ahol speciális IoT technológiát és az életfunkciókat érzékelő technológiát használnak a munkavállalók túlzott fizikai terhelés elleni védelmére és a munka optimalizálására, amely 70%-ban csökkentette a sérülések számát ([2]). Azonban az előnyök mellett számos kihívás és probléma jellemzi még ezeket a rendszereket, ahol kibervédelmi szempontból az IoT eszközök sokszor nem megfelelően védettek. Az egyre érzékenyebb iparágakban, például az egészségügyben és a pénzügyekben használt IoT eszközöknél felmerülő adatvédelmi hiányosságok kezelésére egyre nagyobb motivációja van a rendszer fenntartóinak. A [3]-ban a szerzők kimutatták, hogy a jelenleg használt rendszerek többsége nem képes olyan erős biztonsági szolgáltatásokat és mechanizmusokat integrálni, amelyek megőrizhetnék a biztonságát a betegek személyes adatainak. Emellett súlyosbítja a helyzetet, hogy a kriptográfiai megoldások és a különböző biztonsági intézkedések integrálása az IoT eszközökbe nehézségekbe ütközhet, mivel az eszközök sokszor erőforrás korlátozottak. Emiatt ezek az eszközök nem képesek használni a különböző kriptográfiai primitíveket, illetve nagy eszközpark esetében a skálázhatóság, az interoperabilitás és a heterogenitás egyaránt a felmerülő kihívások közé tartozhat. Így az összes eszköz megfelelő beállítása, konfigurálása és folyamatos karbantartása sok időt, erőfeszítést és költséget jelent. Fontos, hogyha az így kialakított implementációnál akár egyetlen biztonsági rés is marad az elegendő ahhoz, hogy a támadók súlyos károkat okozzanak a rendszereinkben. Ezért az eszközöket többek között védeni kell a különböző aktív és passzív támadásokkal szemben. A passzív támadások kategóriájában a támadók általában a kommunikációt hallgatják le a felek között, hogy hasznos információkat gyűjtsenek. A passzív támadások közé tartozik a lehallgatások és a forgalomelemzések. Az aktív támadások esetén a támadó hatással van a kiválasztott rendszer funkcióira és működésére. Ennek hatásai a biztonsági mechanizmusok (behatolásérzékelés) által is észlelhető. Az ilyen típusú támadások következményeként például a hálózati szolgáltatások sérülhetnek. Az aktív támadások közé sorolhatók: zavarás (jamming), elárasztás (flooding), szolgáltatásmegtagadás (DoS) vagy Sybil típusú támadások ([4]).

A TUDOMÁNYOS ÉS GYAKORLATI MEGOLDÁSOK

A tudományos irodalomban számos cikkben foglalkoznak az IoT rendszerek biztonságának növelésével, ahol az egyik legfontosabb cél az eszközök által generált és továbbított adatok bizalmasságának, integritásának és rendelkezésre állásának védelme, amelyet (CIA) hármasaként ismerünk ([5]). Ezek a biztonsági elvek ugyanúgy vonatkoznak az IoT eszközökre és rendszerekre, mint az informatikai (IT) rendszerekre és online hálózatokra. Ha ezen alapvető biztonsági követelmények egyike sérül, abban az esetben az érintett egyénre vagy szervezetre nézve komoly következményekkel járhat. A Nemzeti Szabványügyi és Technológiai Intézet (NIST) a FIPS 199 szabványban ([6]) meghatározza a bizalmasság, az integritás vagy a rendelkezésre állás elvesztése miatti alacsony, közepes és magas potenciális hatásokat. Az adott támadásokra sok enyhítő és ellenintézkedést lehet implementálni, azonban az IoT rendszerek hálózatának összekapcsoltsága és heterogenitása miatt a biztonsági stratégiának általában átfogóbb, többszintű és több rétegre kiterjedő megközelítést alkalmaznak. A javasolt megoldások során figyelembe kell venni az IoT sajátosságokat például a [7] cikkben a szerzők állítása szerint a biztonsági incidensek 95%-a emberi hibákból származik. Javaslatuk egy új IoT alapú kiber-fizikai emberi rendszert (CPHS) tartalmazott, melynek egyik fontos eleme az emberi faktor, mivel a rendszer biztonságát nem csak az IoT rendszerek, hanem az emberi interakciók is befolyásolják. Ennek a felügyeletére a szerzők egy behatolástűrő rendszert (Intrusion Tolerant System, ITS) vezettek be, melynek célja az emberi hibákból származó támadások hatékony megelőzése. Egyes ötletek ([8], [9]) az architektúra rétegeit vizsgálják és kompromisszumot keresnek annak érdekében, hogy biztosítsák a megfelelő funkcionalitást és kezeljék a korlátozott eszközképességeket. A keletkező adatok védelmét a tárolás és a küldés során különböző kriptográfia primitívekkel garantálhatják, ahol olyan szempontok teljesülését vizsgálják, mint a végponttól végpontig terjedő biztonság, a különböző entitások hitelesítése vagy a hozzáférésellenőrzés.

Az IoT-hoz hasonlóan a blokklánc is viszonylag új technológia, ami megmagyarázza, hogy a blokklánc alapú alkalmazások miért korlátozottak. Mindazonáltal decentralizált jellegükből adódóan a blokkláncok számos előnyt kínálnak, amelyeket már megvalósítottak az IoT eszközökben. Emellett a blokkláncoknak az IoT eszközök sebességére gyakorolt negatív hatásai is sokszor nem relevánsak vagy kezelhetőek. Egy komplex blokklánc alapú gyakorlati megvalósítás az IoT rendszerek védelmére az Európai Unió által finanszírozott GHOST projekt, melynek célja egy megfizethető, kulcsrakész, védelmi megoldás kifejlesztése a kiberfenyegetések ellen okosotthonokra ([10]). A megoldás egy központi átjáróra támaszkodik, amely az okosotthon hálózatból érkező összes adatforgalmat összesíti. A GHOST különböző megközelítéseket követ a kiberfenyegetések és kockázatok észlelésére számos kiemelt technológiát alkalmazva, mint például a gépi tanulás, a behatolásérzékelés és megelőzés és a blokklánc. A GHOST autonóm módon értékeli a kockázatot az otthoni hálózat állapotával szemben, és intuitív és felhasználóbarát felületet biztosít a végfelhasználók számára a biztonsági preferenciák és beavatkozások kezeléséhez. A blokkláncokon alapuló IoT a mindennapi életünk gyakorlatilag összes területén megjelent és a fogyasztók egy része nincs vele tisztában, hogy aktívan használja ezt a technológiát. A blokklánc alapú IoT rendszerek használatának egyik fontos szempontja a kriptográfiailag védett nem manipulálható adatbázisok használata ([11], [12]). A GHOST mellett számos egyéb blokklánc alapú alkalmazást javasoltak az ellátási láncokba, az autóiparban, vagy az villamosenergia

piacokon, mely megoldások az IoT rendszerek biztonságának növelését tűzték ki célul ([13], [14]).

Hozzájárulás

A célunk egy új biztonsági keretrendszer javaslása blokklánc alkalmazásával egy IoT ökoszisztémára. A keretrendszer tartalmaz egy eszközkezelőt, amely az IoT eszközök különböző attribútumait tárolja, mint név, szoftver vagy firmware verzió, típus, tulajdonos és állapot. A blokklánc alkalmazás során egy engedélyköteles blokkláncot alkalmazunk, mivel az egyes szenzitív adatokat tartalmazó attribútumokat titkosítva kell letárolnunk (pl. verzió vagy az IoT eszköz állapota). Az eszközkezelő része egy okosszerződés, melynek célja, hogy ellenőrizhető legyen, ha a felhasználó nem változtatta meg az alapértelmezett jelszót az eszköznél vagy az eszközhöz tartozó szoftver, illetve firmware elavult verzióval rendelkezik. Végezetül a keretrendszer biztonsági mentést nyújt, ahol az IoT rendszer (például okosotthon) beállítások és konfigurációk elosztottan kerülnek tárolásra a blokklánc által. A keretrendszer biztonságosnak tekinthető, mivel a kapcsolódó webalkalmazás megköveteli a felhasználó hitelesítését (tagja-e a blokkláncnak), továbbá a felhasználó és a keretrendszer közötti kommunikáció TLS protokollt alkalmaz. A webszerver és a rajta futó webalkalmazás csak egy felhasználóbarát felületet nyújt a felhasználók számára. A blokklánc biztosítja az elosztott tárolást, illetve az okosszerződés egy elosztott alkalmazás, amely nagyobb rendelkezésre állást biztosít. Így például egy okosotthon beállításait és konfigurációját könnyebb helyreállítani különböző kártékony vagy zsaroló programok fertőzése esetén.

A javasolt rendszerről (lásd 1. ábra) egy prototípust készítettünk, amely egy webes alkalmazás Javascript nyelven implementálva. Az implementáció kialakítása során teszteltük a rendszer funkcionalitását és a biztonsági követelményeket.

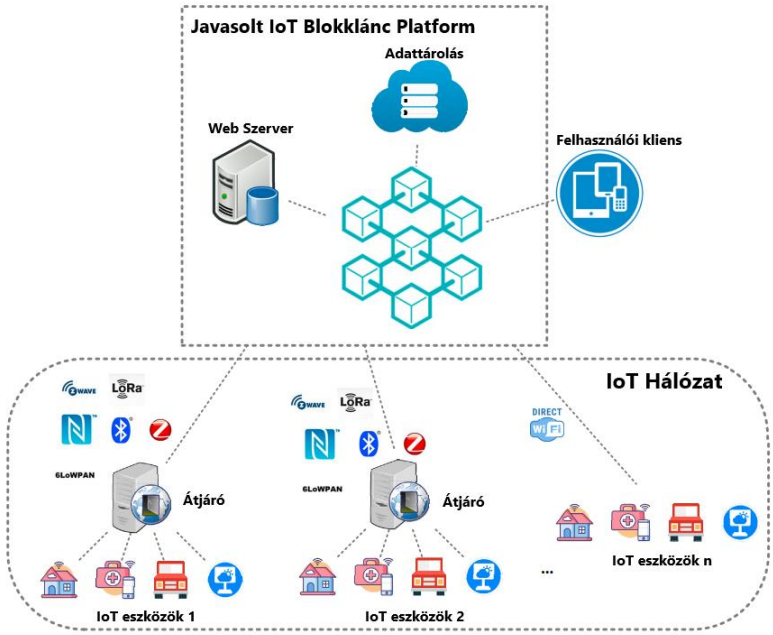
PROTOTÍPUS

Technológiai áttekintés

Az általunk javasolt rendszer implementációja több modulból épül fel. Ennek egyik eleme a Node.js ([15]), amely egy nyílt forráskódú szoftver platform és a webszerverünk elkészítésére alkalmaztuk. A Node.js egy V8 Javascript motorra épül, amely eseményalapú, aszinkron bemenettel és kimenettel rendelkezik a túlterhelés minimalizálása és a skálázhatóság maximalizálása érdekében. A felhasználóbarát felület kialakításához a React ([17]) egy nyílt forráskódú, deklaratív frontend nyelvét vettük igénybe. A webes API felhasználói felületének megjelenítéséhez és kinézetének testre szabásához a React JavaScript könyvtárat alkalmaztuk, ami által különböző komponenseket jeleníthetünk meg, mint például gombok, szöveg dobozok, űrlapok. Emellett szükségünk volt még a Next.js-re ([18]), amely egy nyílt forráskódú webfejlesztői keretrendszer. Ez lehetővé teszi a React alapú web alkalmazások használatát a szerveroldali rendelések és lokális webhelyek generálása érdekében. Támogatja az automatikus kódgyorsítást és adatlekérdezést, amely által a React alapú alkalmazások számára a hatékonyabb és gyorsabb működés biztosítható.

A blokklánc modul fejlesztéséhez először az okosszerződéseket kellett implementálni, ahol a legnépszerűbb objektum-orientált blokklánc programozási nyelvet, a Solidityt választottuk ([16]), amely lehetővé teszi a fejlesztők számára az Ethereum láncra való

alkalmazások fejlesztését. Az okosszerződések programozható logikát és állapotokat tartalmaznak, mint például a változók, a függvények, az objektumok, az öröklődés és az interfészek. Végezetül egy ingyenes kriptovaluta pénztárcára a Metamask-ra ([19]) volt szükségünk, amely elérhető a böngésző bővítményei között. A Metamask a felhasználók számára a fiókcímek tárolását és kezelését, valamint az Ethereum alapú kriptovaluták és tokenek küldését és fogadását támogatja. Emellett a Metamask biztonságos csatlakozást biztosít a decentralizált alkalmazásokhoz webböngészőn vagy mobilalkalmazások beépített böngészőjén keresztül.



1. Ábra: IoT eszközök és blokklánc kapcsolata, saját szerkesztés, saját szerkesztés.

Funkcionalitás

A prototípus fejlesztése számos biztonsági és egyéb funkciót foglalt magába, amellyel menedzselhetővé válnak a hálózatunkra felcsatlakoztatott eszközök. A rendszer skálázható, így lehetővé válik a tetszőleges számú IoT eszköz hozzáadása, illetve azok eltávolítása. Okosszerződések segítségével három alapfunkció kapcsolódik minden IoT eszközhöz, a megtekintés, a szerkesztés és a törlés. A megtekintés funkció aktiválása során a felhasználó részletesebb információt kap az eszközről, megjelenítve a különböző attribútumokat, mint például a MAC cím, a firmware azonosító, a kapcsolódó konfigurációs fájl. A szerkesztés aktiválásával az eszközök adatai szerkeszthetővé válnak, végezetül a törlés funkcióval az adott eszköz eltávolításra kerül a felhasználótól.

A biztonsági funkciók során kiemelendő a szoftver frissítés, amellyel nyomon követhető és ellenőrizhető, hogy az IoT eszközön lévő verzió megegyezik-e az elérhető legfrissebb verzióval. Amennyiben nem, akkor a rendszer figyelmeztetést küld és a felhasználó manuálisan elvégezheti a szükséges frissítéseket. A prototípus forráskódja elérhető az [20] hivatkozáson.

BIZTONSÁGI SZEMPONTOK

A rendszerünk biztonságát formálisan vizsgáltuk, a CIA hármas szempontokat figyelembe véve.

Bizalmasság

Az implementációnk elősegíti az IoT eszközök monitorozását a biztonsági kockázatok csökkentése érdekében. A bizalmasság szempont teljesülését a blokkláncon lévő érzékeny adatok, illetve a felhasználó és a webszerver közötti kommunikációra vizsgáltuk. A felhasználók és a webszerver közötti kommunikációhoz TLS (Transport Layer Security) protokoll alkalmazunk, amely biztosítja kulcscsere mechanizmust a résztvevők között és a munkamenet biztonságát. A blokklánc esetén az egyes érzékeny adatokat tartalmazó attribútumokat AES-GCM szimmetrikus blokktitkosítási algoritmussal vannak ellátva. Az adatok titkosságát így csak a megfelelő visszafejtő kulccsal rendelkező résztvevők képesek megismerni.

Integritás

A rendszerünkben az integritás védelmének biztosítására alkalmazzuk a megfelelő kriptográfiai primitíveket, úgymint hash függvény és digitális aláírások. Emellett a kiberbiztonsági szempontból problémás feladatok is kezelve vannak, így a támadók nem képesek az elavult szoftver vagy eszközkomponensből fakadó hiányosságokat kihasználni. Továbbá a blokklánc alapú alkalmazás tulajdonságai biztosítják, hogy az adatokat ne lehessen manipulálni vagy nyomon követhetőek legyenek az IoT eszközhöz kapcsolódó tranzakciók.

Rendelkezésre állás

Az általunk javasolt keretrendszerben az adatok a blokklánc több csomópontján való tárolásával, illetve az okosszerződések használatával elosztott tárolást és alkalmazást valósítottunk meg, amely növeli az alkalmazás rendelkezésre állását, mivel az adatok és az IoT rendszer funkciói redundánsan tárolódnak, illetve több csomóponton hajtódnak végre. Emellett az elosztott tárolás és alkalmazás lehetővé teszi az adatok és függvények szétosztását a hálózatban ezért lehetőség van arra, hogy a hálózaton belüli replikációkból rövid idő alatt helyreállítsuk azokat például, ha egy adat elveszik vagy kártékony program miatt elérhetetlenné válik. Így a blokklánc alkalmazásával lehetővé válik a leállások minimalizálása, illetve a kártékony programok elleni védelem növelése, amely során hiába fertőzi meg a kártékony program a rendszert, akár több csomópontot egyidőben, a konfigurációs fájlok felhasználásával gyorsan visszaállíthatóvá válik a korábbi, fertőzés előtti állapotába a rendszer.

ÖSSZEFOGLALÁS

A cikkben feltérképezésre került az Internet of Things rendszerek és eszközök széleskörű alkalmazási lehetőségeit, amelyek lefedik az életünk minden területét. Meghatároztuk az IoT rendszerek előnyeit és hátrányait és átfogó képet alkottunk a napjainkban fellelhető aktuális problémákról és sérülékenységekről. Elengedhetetlen volt még az IoT eszközök biztonságát tárgyalni, hiszen a kisebb és a komplex rendszerek is sok kis különböző eszköz összeségéből épülnek fel. Ezáltal a legkisebb alkotó elem biztonságát is magas szinten kell kezelni, azonban a legtöbb IoT eszköz korlátozott erőforrással rendelkezik, ami

miatt nem alkalmazható hagyományos kriptográfiai megoldások. Felmértük a blokklánc technológia fontosságát napjainkban. Egy engedélyköteles blokkláncot alkalmaztunk, ahol az érzékeny adatokat tartalmazó attribútumokat titkosítva tároljuk. A keretrendszer megalkotása során egy eszközkezelőt valósítottunk meg, amely az IoT eszközök különböző attribútumait tárolja. Ezek mellett ismertetésre került az Ethereum és okosszerződések alkalmazási és működési feltételei a biztonsági keretrendszerünkben. Taglaltuk az okosotthon rendszer résztvevőit és javaslatot készítettünk a saját implementációnkról más rendszerekkel összevetve. Végezetül a CIA hármas paramétereit határoztuk meg a rendszerünkre való tekintettel.

FELHASZNÁLT IRODALOM

[1] Friedman, V., *On the edge: Solving the challenges of edge computing in the era of iot.* 2018. [Online] Elérhető: https://www.databank.com/resources/blogs/solving-edge-computing-challenges-in-era-of-iot/

[2] Center Ford Media, *"Ford reduces production line injury rate by 70 percent for its more than 50.000 industrial athletes".* 2015. [Online] Elérhető: https://media.ford.com/content/fordmedia/fna/us/en/news/2015/07/16/ford-reduces-production-line-injury-rate-by-70-percent.html

[3] Gope, P. & Hwang, T. BSN-Care: *A secure IoT-based modern healthcare system using body sensor network.* IEEE sensors journal, 16(5), 1368-1376. 2015.

[4] Butun, I., Österberg, P., & Song, H. *Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures.* IEEE Communications Surveys & Tutorials, 22(1), 616-644. 2019.

[5] Sadique, K. M., Rahmani, R., & Johannesson, P. *Towards security on internet of things: applications and challenges in technology.* Procedia Computer Science, 141, 199-206. 2018.

[6] Division, NIST Computer Security, F. I. P. S. *Standards for Security Categorization of Federal Information and Information Systems*, NIST FIPS 199, 2004.

[7] Kumar, S. A., Bhargava, B., Macêdo, R., & Mani, G., *Securing iot-based cyber-physical human systems against collaborative attacks.* In 2017 IEEE International Congress on Internet of Things (ICIOT) (pp. 9-16). IEEE. 2017.

[8] Rajendran, G., Nivash, R. R., Parthy, P. P., & Balamurugan, S., *Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures.* In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE. 2019.

[9] Ahmed, A. W., Khan, O. A., Mian, M. A., & Shah, M. A., *A comprehensive analysis on the security threats and their countermeasures of IoT.* International Journal of Advanced Computer Science and Applications, 8(7). 2017.

[10] Collen, A.; Nijdam, N.A.; Augusto-Gonzalez, J.; Katsikas, S.K.; Giannoutakis, K.M.; Spathoulas, G.; Gelenbe, E.; Votis, K.; Tzovaras, D.; Ghavami, N.; et al. *GHOST—Safe-Guarding Home IoT Environments with Personalised Real-Time Risk Control. In Security in Computer and Information Sciences*; Springer: Cham, Switzerland, pp. 68–78. 2018.

[11] Mazzei, D., Baldi, G., Fantoni, G., Montelisciani, G., Pitasi, A., Ricci, L., & Rizzello, L., *A Blockchain Tokenizer for Industrial IOT trustless applications.* Future Generation Computer Systems, 105, 432-445. 2020.
[12] Cullen, A., Ferraro, P., King, C., & Shorten, R., *On the resilience of DAG-based distributed ledgers in IoT applications.* IEEE Internet of Things Journal, 7(8), 7112-7122. 2020.
[13] Alshaikhli, M., Elfouly, T., Elharrouss, O., Mohamed, A., & Ottakath, N., *Evolution of Internet of Things from blockchain to IOTA: A survey.* IEEE Access, 10, 844-866. 2021.
[14] Minoli, D., & Occhiogrosso, B. *Blockchain mechanisms for IoT security.* Internet of Things, 1, 1-13. 2018.
[15] Node.js, 2023. [Online] Elérhető: https://nodejs.org/en/about
[16] Solidity, 2023. [Online] Elérhető: https://dev.to/envoy_/history-and-origin-of-solidity-2mhl
[17] React, 2023. [Online] Elérhető: https://en.wikipedia.org/wiki/React_(JavaScript_library)
[18] Next.js, 2023. [Online] Elérhető: https://vercel.com/home
[19] Metamask, 2023. [Online] Elérhető: https://docs.metamask.io/guide/
[20] Github prototípus, 2023. [Online] Elérhető: https://github.com/ncsn/SmarthomeBlockchain

PÁLYÁZATRA UTALÓ MEGJEGYZÉS

A KULTURÁLIS ÉS INNOVÁCIÓS MINISZTÉRIUM ÚNKP-23-1 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.