Securitatea rețelelor și sisteme de comunicații în medii Smart

Mihail DUMITRACHE[1,2], Ionuț-Eugen SANDU[1,3]

[1] Institutul Naţional de Cercetare-Dezvoltare în Informatică - ICI Bucureşti

[2] Universitatea București – Facultatea de Litere

[3] „Lucian Blaga" University of Sibiu, 10 Victoriei Blvd., Sibiu, 550024 Romania

mihail.dumitrache@ici.ro, ionut.sandu@ici.ro

Rezumat: Internet of Things (IoT) este o paradigmă care schimbă modul cum trebuie abordată securitatea, deoarece posibilitatea de atac este acum mai extinsă ca niciodată. Dispozitivele IoT sunt utilizate din ce în ce mai mult în diferite industrii având roluri importante pentru viața de zi cu zi a oamenilor, iar din acest motiv atât producătorii de dispozitive IoT, cât și cei care integrează și livrează proiecte IT ce cuprind dispozitive IoT trebuie să aibă în vedere problemele de securitate și de confidențialitate. Alegerea dispozitivelor IoT, a protocoalelor de comunicații, precum și a mecanismelor de securitate trebuie efectuată în concordanță cu nivelul de confidențialitate al informațiilor aflate atât în tranzit, cât și păstrate pe diverse sisteme de stocare. Asigurarea unui nivel de securitate mai mare decât este cazul se traduce prin costuri operaționale suplimentare și/sau utilitate redusă, pe când asigurarea unui nivel inferior face ca sistemul respectiv să nu fie de încredere, deci să nu fie utilizat de către consumatori. Prezentul studiu a avut drept obiectiv prezentarea principalelor cerințe de securitate ale unei infrastructuri IoT și sisteme și protocoale de comunicații în mediu Smart.

Cuvinte cheie: Internet of Things (IoT), Smart, securitatea rețelelor, sisteme de comunicații, protocoale de comunicații.

Network security and communication systems in Smart environments

Abstract: The Internet of Things (IoT) is a paradigm that changes the way we should handle security, since possibilities of attack are now more extensive than ever before. IoT devices are employed more and more in various industries having important roles in the everyday life, and, for this reason, both the IoT device manufacturers and those who integrate and deliver IT projects involving IoT devices must take into account the security and confidentiality aspects. Selection of IoT devices, communication protocols, and security mechanisms must be done according to the level of confidentiality of both the data that is transmitted and the data kept on various storage media. Ensuring a higher-than-necessary security level translates into additional operational costs and/or reduced functionality, while a lower-than-necessary security level leads to customers not trusting and not using the device/system. This paper aims to present the main security requirements of an IoT infrastructure, and communication systems and protocols within Smart environments.

Keywords: Internet of Things (IoT), Smart, network security, communication systems, communication protocols.

1. Introducere

Infrastructura IoT conține o gamă largă de componente tehnologice precum Cloud, Big Data, dispozitive mobile și dispozitive inteligente. Fiecare dintre aceste componente tehnologice este susceptibilă la diferite tipuri de vulnerabilități de securitate, ceea ce le poate face ineficiente. Este foarte important ca toate componentele infrastructurii IoT să fie protejate în mod adecvat împotriva diferitelor tipuri de atacuri (Alexandru, Vevera & Ciupercă, 2019), folosind diverse tehnici, care trebuie întotdeauna revizuite și adaptate în funcție de evoluția atacurilor cibernetice.

Informația și metodele de comunicare sunt componente fundamentale pentru securizarea dispozitivelor inteligente. Securizarea infrastructurii IoT necesită o abordare riguroasă având la bază strategia de securitate în profunzime (security-in-depth). Această abordare necesită asigurarea

https://doi.org/10.33436/v30i1y202005

datelor în cloud, protejarea integrității datelor în timpul tranzitului prin internetul public, precum și securizarea tuturor dispozitivelor. Fiecare dintre aceste elemente contribuie împreună la asigurarea unui nivel de securitate superior al unei infrastructuri IoT (Raj & Raman, 2017).

Pentru a menține sau a spori calitatea vieții în condițiile creșterii numărului de rezidenți, tehnologiile ITC sunt tot mai utilizate pentru a implementa proiecte din aria Smart City care să aducă beneficii comunităților (Petre, Cohal & Boncea, 2018).

Sistemele IoT sunt reprezentate de dispozitive interconectate și dependente unele de altele. Întotdeauna tehnologiile noi sunt vulnerabile la atacuri, de aceea este de maximă importanță analiza vulnerabilităților și amenințărilor cu care s-au confruntat soluții deja existente astfel încât să fie redus pericolul ca aceste vulnerabilități să fie prezente în tehnologii nou lansate (Zamfiroiu, Boncea & Petre, 2019). Nivelul de securitate al unui sistem IoT este dat de cea mai slabă componentă, în sensul în care dacă un dispozitiv este compromis, efectul se va propaga asupra tuturor componentelor care depind de el direct sau indirect. De aceea abordarea unei strategii de tipul ”defense in depth” va ajuta la îmbunătățirea nivelul securității sistemelor IoT. Securitatea nu trebuie privită punctual, ci trebuie abordată în ansamblul ei încă din faza de proiectare a sistemelor IoT, astfel încât probabilitatea ca persoanele rău intenționate să reușească să obțină acces la informații confidențiale să fie cât mai redusă.

2. Cerințe de securitate ale unei infrastructuri IoT

Principalele aspecte de securitate, care trebuie avute în vedere pentru securitatea componentelor tehnologice ale informațiilor, care sunt aplicabile unei infrastructuri IoT, sunt:

Triada CIA - **Confidențialitate**, **Integritate** și **Disponibilitate** (Confidentiality, Integrity and Availability - CIA) reprezintă cele trei cerințe fundamentale care trebuie avute în vedere în faza de proiectare și dezvoltare a infrastructurii IoT, acestea fiind prezentate în Figura 1.

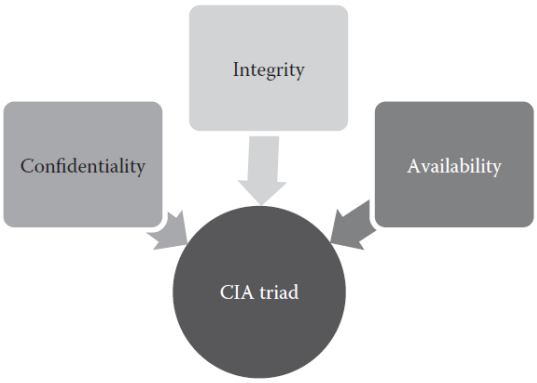

Figura 1. Triada CIA - Confidențialitate, Integritate și Disponibilitate (Raj and Raman, 2017)

Confidențialitatea - reprezintă cerința prin care se asigură că numai utilizatorii autorizați vor avea acces la informațiile de bază. Cu alte cuvinte, se asigură confidențialitatea prin împiedicarea accesului neautorizat la informațiile stocate sau transmise prin intermediul infrastructurii IoT.

Integritatea - reprezintă cerința prin care se asigură că numai utilizatorii autorizați au permisiunea de a modifica informațiile de bază. Modificarea informațiilor implică operațiunile de scriere, ștergere și/sau actualizare. Prin urmare utilizatorii neautorizați nu vor putea să modifice informațiile în niciun fel.

Disponibilitatea - reprezintă cerința prin care se asigură faptul că utilizatorii autorizați au acces la informațiile necesare în momentul în care acestea sunt necesare. Asigurarea disponibilității presupune că infrastructura IoT are capacități de toleranță la erori prin asigurarea unor componente de backup pentru fiecare dintre nivelurile infrastructurii IoT și anume: servere, stocare și comunicare.

Cadrul **Autentificarea**, **Autorizarea** și **Auditarea –** AAA - reprezintă cerința de securitate de o importanță majoră pentru infrastructura IoT.

Autentificarea - reprezintă procesul prin care se verifică dacă credențialele unui utilizator sunt valide, astfel încât utilizatorilor care nu au credențiale valide să nu li se permită accesarea informațiilor. Cea mai simplă modalitate de autentificare se bazează pe utilizator și parolă. Dar, pe măsură ce tehnicile de hacking evoluează zilnic, este foarte important să se utilizeze tehnici de autentificare mai complexe. Un astfel de mecanism de autentificare, care se utilizează din ce în ce mai des, se numește autentificare multifactorială. Autentificarea multifactorială este o metodă de autentificare care utilizează o combinație de parametri. Un exemplu de mecanism de autentificare multifactorială este descris mai jos:

- primul factor: un nume de utilizator și o parolă, care vor fi unice pentru fiecare utilizator și care uneori pot fi unice și pentru sesiunea specifică;
- al doilea factor: o cheie secretă, care este creată de un generator de numere aleatorii sau o expresie-cheie secretă, care este cunoscută numai de utilizator sau care răspunde la o întrebare secretă specifică unui anumit utilizator;
- al treilea factor: acesta ar putea fi orice parametru biometric al utilizatorului, care ar putea fi folosit ca semnătură biometrică a utilizatorului. Acesta ar putea include aspecte precum recunoașterea irisului, recunoașterea amprentei digitale, recunoaștere vocală, recunoaștere facială etc.

O autentificare multifactorială utilizează o combinație a tuturor parametrilor menționați mai sus pentru a verifica acreditările unui utilizator. În unele cazuri, numai doi factori menționați mai sus pot fi utilizați pentru autentificare, aceasta numindu-se autentificare cu doi factori.

Autorizarea - reprezintă procesul prin care se asigură că un anumit utilizator are drepturi de a efectua operațiuni specifice pe un anumit obiect. Aceasta se realizează prin acordarea de diferite tipuri de permisiuni diferitelor tipuri de utilizatori pe baza unor roluri predefinite. De exemplu, un director executiv al stației de pompieri va putea să citească datele referitoare la alte departamente ale orașului, cum ar fi departamentul de apă, fără posibilitatea de editare a acestor date. Permisiunile de editare pot fi acordate numai supraveghetorilor orașului sau directorilor din cadrul departamentului de apă al orașului. Diferitele tipuri de permisiuni pentru diferiți utilizatori sunt cartografiate și stocate într-un tabel denumit “Lista control acces” - Control Access List (ACL). Diferitele tipuri de permisiuni, care sunt oferite utilizatorilor, sunt clasificate astfel:

- numai citire (read-only) - utilizatorul are doar permisiunea de a citi un obiect. Utilizatorul nu poate șterge sau edita obiectul respectiv. Aceste tipuri de permisiuni sunt acordate utilizatorilor care nu au drepturi de a efectua modificări asupra datelor.
- citire și scriere (read-write) - utilizatorul are permisiunea de a citi și modifica un obiect. Aceste tipuri de permisiuni sunt acordate utilizatorilor care au autoritatea de a valida drepturile și permisiunile de acces ale altor utilizatori.

Auditarea - reprezintă activitatea desfășurată periodic pentru a evalua eficacitatea măsurilor de securitate implementate în infrastructura IoT. Procesul de audit este realizat cu ajutorul jurnalelor de audit, care urmăresc operațiile efectuate de diferiți utilizatori.

Securitatea în profunzime (Defense-in-Depth) - reprezintă un mecanism care ar trebui utilizat pentru a oferi un nivel ridicat de securitate infrastructurii IoT. Acest mecanism asigură existența mai multor niveluri de securitate în cadrul unei infrastructuri IoT, pentru a se asigura că, chiar dacă securitatea la un nivel este compromisă din anumite motive, securitatea de la alte niveluri ar trebui să poată proteja infrastructura IoT în ansamblul ei. Această abordare presupune existența mai multor niveluri de securitate, de aceea este considerată o abordare stratificată a implementării securității ce conferă o securitate sporită infrastructurii IoT. O arhitectură la nivel înalt a mecanismului Defence-in-Depth este prezentată în Figura 2 (Raj & Raman, 2017).

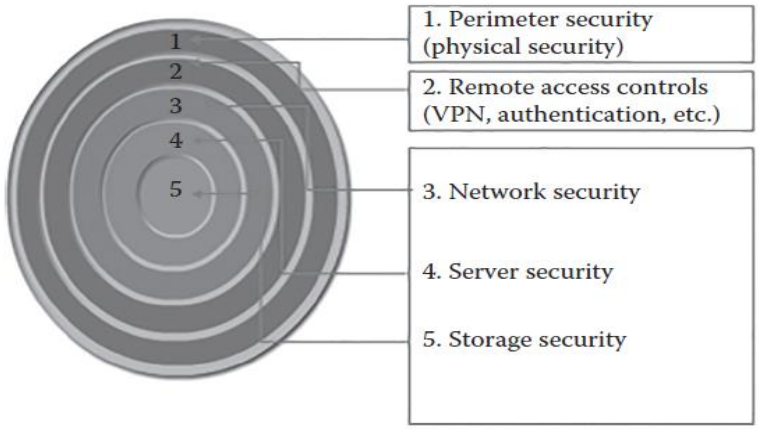

Figura 2. Arhitectură la nivel înalt a mecanismului Defence-in-Depth (Raj & Raman, 2017)

Tipurile de amenințări din ce în ce mai numeroase pot fi clasificate în funcție de modul în care acționează asupra datelor (divulgare, modificare, distrugere sau blocarea accesului) sau în funcție de principiile de bază privind securitatea informațiilor care sunt încălcate. În Figura 3 sunt descrise o serie de exemple de atacuri (Curtea de Conturi Europeană, 2019), unde:

- lacăt = securitatea nu este afectată;
- semn de exclamare = securitatea este pusă în pericol.

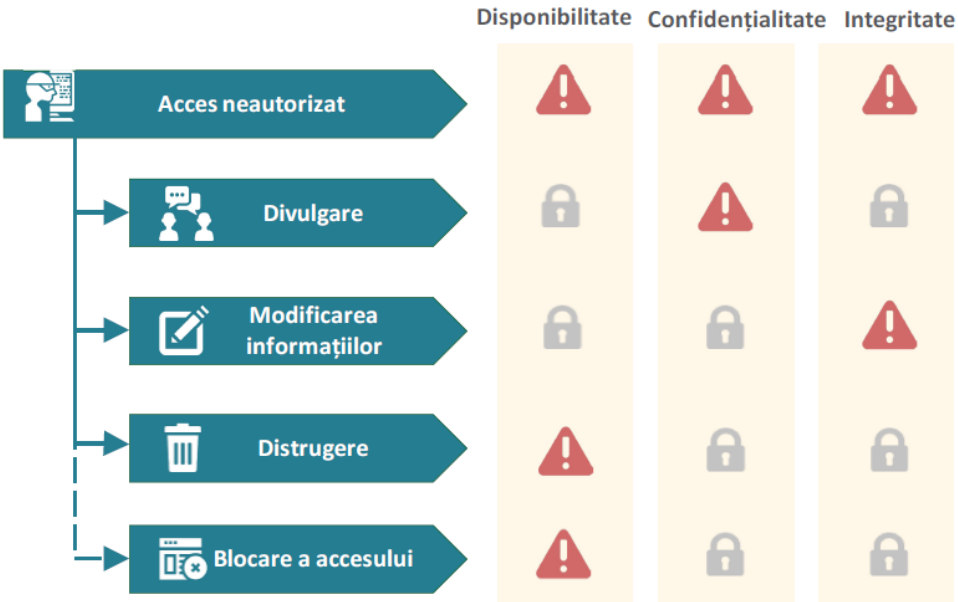

Figura 3. Tipuri de amenințări și principiile de securitate (Curtea de Conturi Europeană, 2019)

Sistemele de apărare devin mai puțin eficiente odată cu creșterea gradului de complexitate al atacurilor asupra sistemelor informatice.

3. Sisteme de comunicații în medii Smart

IoT - reprezintă mai mult decât dispozitive conectate, care în mod ideal necesită o infrastructură IoT organizată și dedicată, având patru etape distincte pentru a reflecta transferul de date de la dispozitivele IoT la analiza finală. Prelucrarea datelor poate avea loc în fiecare dintre aceste patru etape. Aceste etape sunt (O'Dwyer, 2018):

- **Senzorul sau dispozitivul de acționare** - de exemplu, un senzor poate colecta date pentru a monitoriza temperatura apei, în timp ce, un dispozitiv de acționare va efectua o

funcție fizică, cum ar fi închiderea sau deschiderea unei supape când se atinge o temperatură predefinită.

- **Internet Gateways** - datele generate de senzori sunt colectate și convertite în format digital, apoi sunt transmise prin intermediul unui protocol ales, fie pe Wi-Fi, pe rețea de cablu sau pe Internet. Acest lucru permite ca toate datele să fie trimise pentru procesare, deoarece analiza în timp real este intensivă și poate încetini rețeaua.
- **Edge IT** - o etapă intermediară necesară pentru efectuarea de analize suplimentare înainte de a trimite date către centrul de date (Data Center). Acest lucru are scopul de a reduce traficul către centrul de date și de a asigura că lățimea de bandă a rețelei nu este depășită. De exemplu, dacă nu dorim să avem nevoie de toate datele de pe toate dispozitivele, ci numai de datele care satisfac anumite criterii definite pentru acțiuni ulterioare.
- **The Data Center or Cloud** - este posibilă o analiză detaliată a datelor rămase, iar rapoartele generate sunt trimise la rețeaua on-premise. Atunci când procesarea și analiza intensivă a datelor are loc în afara locației, nu există probleme referitoare la lățimea de bandă a rețelei.

Potrivit SaM Solutions arhitectura unui sistem de tip Smart este compusă din trei niveluri: dispozitivele inteligente din teren, concentratoarele de comunicație (gateway) și concentratoarele de date / centre de date (data system) (Figura 4) (Sakovich, 2018).

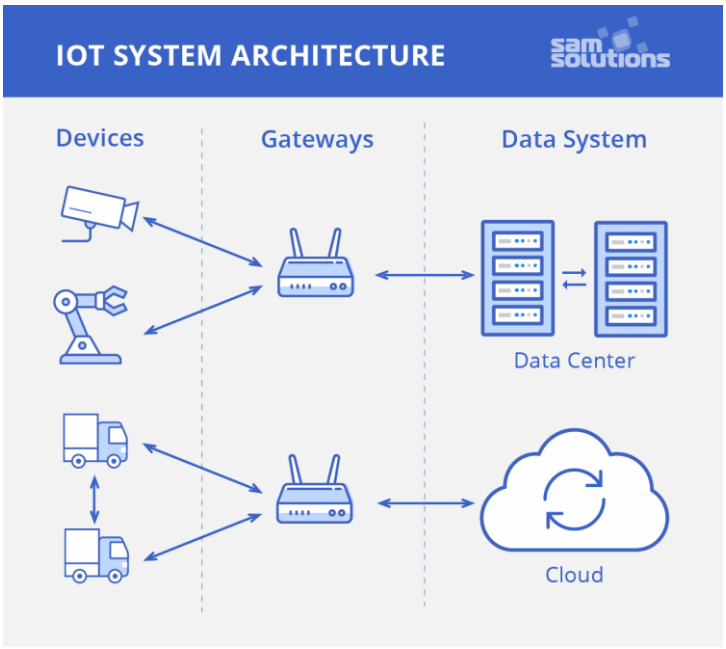

Figura 4. Arhitectura unui sistem de tip Smart (Sakovich, 2018)

(Sursa: https://www.sam-solutions.com/blog/wp-content/uploads/2018/08/111@2x-704x624.png)

Datele sunt transportate între aceste niveluri folosind una dintre cele patru metode:

Dispozitiv la Dispozitiv (D2D) - comunicație directă între două obiecte Smart în care dispozitivele fac schimb de informații instantaneu fără un intermediar. De exemplu, roboții industriali și senzorii sunt conectați în mod direct pentru a-și putea coordona acțiunile și executa corect procesul de asamblare.

Dispozitiv la Gateway - comunicația dintre senzori și nodurile concentratoare (Gateway-uri). Gateway-urile sunt noduri ale rețelelor Smart cu o putere computațională mult mai mare decât cea a senzorilor și îndeplinesc două funcții de bază: consolidarea datelor primite de la senzori și

redirectarea către centrele de date; analizarea datelor primite de la senzori, iar în cazul în care sunt detectate probleme, returnarea acestora.

Gateway la Data System - transmisia datelor de la Gateway către cel mai potrivit concentrator de date (Centru de Date) din rețea.

Data System la Data System - transferul informației între centrele de date.

În prezent există foarte multe categorii de dispozitive IoT, care variază foarte mult în funcție de nivelurile de securitate furnizate. Unele dintre ele se conectează utilizând protocoale bazate pe proximitate, cum ar fi Bluetooth, RFID (identificarea frecvențelor radio) sau Wi-Fi, în timp ce altele folosesc GPS, 4G sau sunt conectate prin cablu. Conectarea acestora este adesea la fel de facilă ca și scanarea dispozitivelor din apropiere, prin introducerea unui cod scurt (a cărei valoare implicită poate fi sau nu modificată) sau prin utilizarea unei forme de autentificare multifactor pentru a verifica permisiunile dispozitivului și ale utilizatorului.

4. Protocoale de comunicații în medii Smart

Primul dispozitiv conectat la rețeaua globală a fost un automat Coca-Cola și se întâmpla în 1982. Acesta era capabil să mențină controlul temperaturii aparatului și să contorizeze numărul de sticle conținute de acesta. Totuși, mai târziu, în 1999, se consideră că a fost formulat termenul de Internet of Things de către cercetătorul Kevin Ashton.

La baza comunicației dintre componentele unei rețele Smart stau protocoalele de comunicație. După 2010 dispozitivele Smart au cunoscut o creștere considerabilă iar lumea Internet of Things a dezvoltat un internet diferit ce necesita standarde și protocoale de comunicație specifice. Există totuși protocoale (de ex. HTTP) ce pot fi folosite și în mediile Smart.

Protocoalele IoT - reprezintă seturi de reguli și norme care permit ca două sau mai multe entități din infrastructura IoT să comunice între ele prin transmiterea de informații, însă trebuie avut în vedere că acest transfer de date trebuie să se realizeze în condiții de securitate.

Protocoalele IoT se pot împarți în două tipuri de bază: protocoale de rețea IoT și protocoale de date IoT (*Top 15 Standard IoT Protocols,* 2020).

Bluetooth - Protocolul Bluetooth introdus recent printre protocoalele IoT este protocolul BLE sau Bluetooth Low-Energy. Trebuie menționat faptul că BLE nu este proiectat pentru a transfera fișiere mari și va merge optim cu transferuri mici de date. Acesta este motivul pentru care Bluetooth este unul dintre cele mai folosite protocoale IoT (Figura 6).

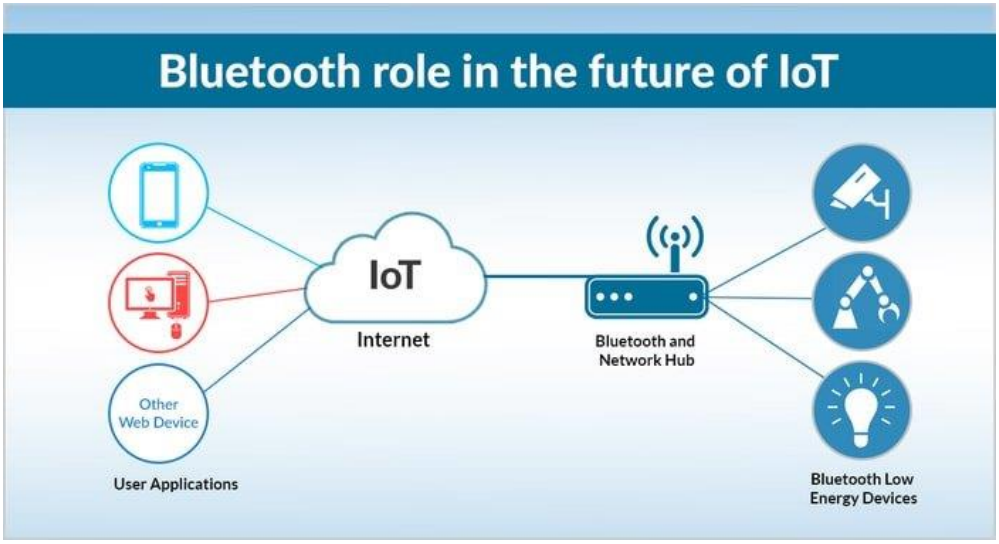

Figura 6. Rolul Bluetooth în IoT [5]

(Sursa: https://www.ubuntupit.com/wp-content/uploads/2018/11/Bluetooth.jpg)

Pentru integrarea dispozitivelor IoT, **WiFi**-ul este o alegere preferată de mulți producători de echipamente deoarece are atât rate rapide de transfer de date, cât și capacitatea de a controla o cantitate mare de date, standardul WiFi 802.11 oferind posibilitatea de a transfera sute de megabiți în numai o secundă. Singurul dezavantaj al acestui protocol IoT este că poate consuma o putere excesivă pentru o parte din aplicația IoT. Acesta se întinde pe o distanță de aproximativ 50 m, iar împreună cu standardele IP permite accesul la infrastructura IoT Cloud. Frecvențele sunt benzi de 2,4 GHz și 5 GHz.

LoRaWAN (**Lo**ng **Ra**nged **W**ide **A**rea **N**etwork) - este un protocol folosit pentru rețele distribuite pe distanțe mari care sunt alcătuite din milioane de dispozitive cu putere redusă. Acest protocol este folosit în special în orașele inteligente și în industrii pentru comunicații bidirecționale protejate. Rețeaua LoRaWAN poate să conțină noduri, stație de bază, server de rețea și server de aplicații.

ZigBee - este primul protocol standard deschis care oferă o conectivitate la Internet pentru a controla, cu costuri reduse, dispozitive cu consum redus, folosind rețeaua fără fir având la bază IPv6. La fel ca Bluetooth, există o gama largă de utilizatori de ZigBee (Figura 7). Acest protocol a fost conceput mai mult pentru zona industrială, mai puțin pentru consumatori și de obicei funcționează la o frecvență de 2,4 GHz. În prezent s-a ajuns la versiunea ZigBee 3.0, fiind un protocol ușor de utilizat.

Figura 7. Integrarea ZigBee în IoT (*Top 15 Standard IoT Protocols,* 2020)

(Sursa: https://www.ubuntupit.com/wp-content/uploads/2018/11/zigbee.jpg)

MQTT (Message Queue Telemetry Transport) - reprezintă protocolul dezvoltat în 1999 de Arlen Nipper (Arcom) și Andy Stanford-Clark (IBM) fiind folosit cu precădere pentru monitorizarea infrastructurii IoT dintr-o altă locație.

CoAP (Constrained Application Protocol) - este un protocol IoT definit în RFC 7252, fiind dezvoltat în principal pentru gadget-urile inteligente restricționate.

DDS (Data Distribution Service) - reprezintă un standard pentru comunicarea de înaltă performanță, extensibilă, în timp real între diverse dispozitive, fiind dezvoltat și proiectat de către OMG (Object Management Group).

NFC (Near Field Communication) - prin acest protocol clienții pot să se conecteze la dispozitivele electronice și să efectueze tranzacții de plată sau să utilizeze conținut digital fără contact. Funcționează la distanțe de 4 cm între dispozitive, permițând dispozitivelor să facă transfer de informații neexistând implementate standarde se securitate.

GSM (Global System for Mobile Communications) - este un protocol IoT de comunicare care poate să transmită o cantitate mare de date, dar trebuie avut în vedere costul care poate fi ridicat și consumul de energie.

AMQP (Advanced Message Queuing Protocol) - Protocolul de mesagerie avansată a mesajelor - este un protocol de aplicație, orientat spre mesaj și conceput pentru medii middleware, fiind definit în standardul internațional ISO/IEC 19464:2014.

RFID (Radio Frequency Identification) - este un protocol care funcționează cu ajutorul tehnologiei wireless putând să identifice obiecte cu ajutorul câmpurilor electromagnetice. Cea mai bună caracteristică a acestui protocol este că nu are nevoie de alimentare de la sursă.

Z-Wave - este un protocol de comunicații fără fir, utilizat în principal pentru automatizarea unei case cum ar fi controlul iluminatului, sisteme de securitate, termostate, ferestre, încuietori, piscine și uși de garaj. Un sistem Z-Wave poate fi controlat prin intermediul internetului de la un telefon inteligent, tabletă sau computer, precum și local, printr-un difuzor inteligent, tastatură wireless sau panou montat pe perete.

Sigfox - este cunoscut ca una dintre cele mai bune tehnologii alternative care poartă atât atributele celulare cât și WiFi. Dat fiind faptul că protocolul Sigfox IoT a fost dezvoltat și conceput pentru aplicațiile M2M (Machine-to-machine communication), acesta poate trimite doar date de nivel scăzut.

KNX - este unul dintre cele mai vechi și populare protocoale de comunicație folosite în aplicațiile de automatizări de tipul Smart Home. Implementările bazate pe acest standard sunt foarte flexibile din punctul de vedere al mediului de transmisie. Se pot folosi atât medii cu perechi de fire răsucite, fire folosite pentru alimentarea cu energie, ethernet, infraroșu sau radio.

Un pas deosebit de important pentru IoT este noua tehnologie 5G care nu va fi doar o generație de comunicații mobile. Această tehnologie este deja considerată structura unificatoare care va conecta miliarde de dispozitive în unele dintre cele mai rapide, mai fiabile și mai eficiente moduri cu putință. Impactul unei tehnologii care oferă atât de multe posibilități va fi unul revoluționar. Noul sistem de comunicare ar trebui să transforme lumea senzorilor conectați și să remodeleze industrii întregi. O astfel de revoluție ar impune, firește, activități de cercetare și dezvoltare în ceea ce privește coexistența și interoperabilitatea între dispozitive și senzori cu rețelele 5G.

5. Concluzii

Cazurile de utilizare a dispozitivelor IoT sunt foarte variate, dar tendințele actuale sugerează că, deși poate dura un timp pentru a fi filtrate, toți producătorii de dispozitive vor face selecția și în funcție de cum este abordată securitatea. O abordare similară cu dispozitivele IoT este cunoscută sub numele de infrastructură de chei publice (PKI), unde certificatele digitale demonstrează autenticitatea site-ului sau, în acest caz, dispozitivului IoT. Certificatele digitale asigură un nivel de încredere într-un dispozitiv IoT care, combinat cu aplicațiile IoT pentru monitorizarea infrastructurii, ar putea identifica și împiedica accesul la dispozitivele necertificate sau cu securitate slabă.

Indiferent de metoda de autentificare folosită în IoT, accentul se pune pe asigurarea unui nivel optim de securitate. În anumite condiții autentificarea cu doi factori este suficientă, în alte situații, pentru confort se alege un mecanism SSO (single sign-on). De asemenea, pentru a gestiona toate dispozitivele, se poate folosi Azure IoT. În cazul în care există cerințe specifice, pentru a se asigura calitatea serviciilor, este indicată utilizarea unui client MQTT (Message Queuing Telemetry Transport).

Metodele de autentificare IoT sunt necesare pentru a se asigura securitatea dispozitivelor IoT, existând totodată mai multe modalități de a atinge acest obiectiv. Securitatea trebuie abordată în ansamblu, însă trebuie să ne asigurăm că fiecare dispozitiv în parte este construit în mod securizat.

Progresele înregistrate în domeniul tehnologiilor IoT, precum dispozitivele/senzorii 5G, sunt compatibile cu o varietate de domenii de aplicare. Se preconizează că integrarea lor în industrie va

revoluționa industria actuală prin crearea unor mașini mai inteligente, prin crearea de conexiuni între ele și permițându-le să comunice una cu alta și să se controleze una pe alta pentru automatizare comună și optimizare inteligentă.

Confirmare

Acest articol a fost realizat în cadrul proiectului *„Studiu privind securitatea comunicațiilor de date în medii smart”* finanțat de Planul sectorial al Ministerului Comunicațiilor și Societății Informaționale (MCSI), Contract 64/30.05.2018. Mulțumim colegilor din proiect pentru colaborare.

BIBLIOGRAFIE

1. Alexandru, A., Vevera, V., Ciupercă, E. M. (2019). *National Security and Critical Infrastructure Protection*. Proceedings of the International conference KNOWLEDGE-BASED ORGANIZATION, Vol. XXV, No 1.
2. Curtea de Conturi Europeană (2019). *Provocări pentru o politică eficace a UE în domeniul securității cibernetice*, https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_ro.pdf.
3. O'Dwyer, M. (2018). *Internet of Things 101 - IoT Device Authentication Explained*, https://blog.ipswitch.com/internet-of-things-101-iot-device-authentication-explained.
4. Sakovich, N. (2018). *Internet of Things (IoT) Protocols and Connectivity Options: An Overview*, https://www.sam-solutions.com/blog/internet-of-things-iot-protocols-and-connectivity-options-an-overview/.
5. Pethuru Raj, Anupama C. Raman (2017). *The Internet of Things. Enabling Technologies, Platforms, and Use Cases*, Boca Raton: Taylor & Francis, CRC Press.
6. Petre, I., Cohal, A. M., Boncea, R. (2018). *Platforma de e-Participare pentru facilitarea implicării cetățenilor în inițiativele Smart City*. Revista Română de Informatică şi Automatică, ISSN 1220-1758, vol. 28(2), pp. 5-14, 2018.
7. *Top 15 Standard IoT Protocols* (2020), disponibil la adresa: https://www.ubuntupit.com/top-15-standard-iot-protocols-that-you-must-know-about/.
8. Zamfiroiu, A., Boncea, R., Petre, I. (2019). *Cloud Computing Vulnerabilities Analysis*. Proceedings of the 2019 4th International Conference on Cloud Computing and Internet of Things (CCIOT), pp. 48–53, DOI: https://doi.org/10.1145/3361821.33&61830.

Mihail DUMITRACHE este absolvent al Facultății de Electrotehnică, Universitatea Politehnica din București, specializarea Inginerie Asistată de Calculator, inginer și doctor în Inginerie Electrică. Deține studii masterale în specializarea Inginerie Electrică, Universitatea Politehnica din București și în specializarea Administrație Publică Electronică, Universitatea din București. Și-a început activitatea profesională în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică - ICI București în anul 2002 ca programator. În prezent este Cercetător Științific III, șef serviciu Administrare domenii RoTLD și Lector Universitar la Universitatea din București. Este autor și coautor al unor studii și articole de specialitate.

Mihail DUMITRACHE PhD graduated from "Politehnica" University of Bucharest, Faculty of Electrical Engineering, with an Engineer's Degree and, later on, a PhD in Computer Assisted Engineering. In between, he obtained two Master's Degrees, one in Electrical Engineering, at "Politehnica" University of Bucharest and one in Electronic Public Administration, at Bucharest University. His professional career started at the National Institute for Research and Development in Informatics, ICI Bucharest in 2002 as a computer programmer. Currently, he is Scientific Researcher Grade III and Head of the .ro Domain Administration Department (RoTLD), and also Lecturer at the University of Bucharest. He is author and co-author of several scientific studies and articles.

Ionuț-Eugen SANDU este licențiat în Știința Sistemelor și a Calculatoarelor (2006), obține master în Administrație Publică Electronică în anul 2007. Din anul 2010 devine cercetător științific în cadrul departamentului de Administrare Domenii .RO. din Institutului Național de Cercetare-Dezvoltare în Informatică - ICI București, iar începând cu anul 2015 devine șef serviciu tehnic RoTLD și Cercetător Științific gradul III în cadrul aceluiași institut. Are responsabilități de administrare sisteme, dezvoltare de noi servicii, dezvoltare și mentenanță a infrastructurii de comunicații, precum și relația cu partenerii. În prezent este șeful departamentului RoTLD și Cloud Computing.

Ionuț-Eugen SANDU graduated university with a BS în Computer and Systems' Science (2006) and obtained a Master's Degree in Electronic Public Administration in 2007. In 2010, he became Scientific Researcher within the .ro Domain Administration Department (RoTLD) of the National Institute for Research and Development in Informatics, ICI Bucharest, and since 2015 is Scientific Researcher Grade III and Head of the Technical Division of RoTLD, with responsibilities in systems' administration, development of new services, development and maintenance of communication infrastructures. He is also in charge with maintaining a close relationship with RoTLD's Partners. Currently, he is Head of the "RoTLD and Cloud Computing" Department.