ANALELE ŞTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IASI
TOMUL LXIII, ŞTIINȚE JURIDICE, 2017, NR. II

CARE ESTE RELAȚIA DINTRE SECURITATE, CONFIDENȚIALITATE ŞI INTERNETUL LUCRURILOR?

WHAT IS THE RELATION BETWEEN SECURITY, CONFIDENTIALITY AND THE INTERNET OF THINGS?

MIRCEA GEORGESCU[1]
ROXANA IBĂNESCU

Rezumat: În urma cercetărilor realizate asupra rețelelor a luat naştere o nouă tehnologie numită Internetul Lucrurilor ce îşi propune să creeze noi valori prin realizarea schimbului de informații şi cunoştințe dintre oameni şi obiecte. Acesta este diferit față de predecesori săi (Internetul tradițional, Internetul Mobil, rețeaua de senzori etc.), axându-se în special pe modele de servicii omniprezente, arhitecturi de rețea eterogene şi acces universal pentru oameni, lucruri, obiecte şi procese. Inovațiile şi cercetările viitoare realizate asupra aplicațiilor şi serviciilor IoT sunt impulsionate de potențialul mare de piață şi de profit. Cu toate acestea, IoT propune noi domenii de studiere a vulnerabilității în securitatea sistemelor şi probleme mai dificile de confidențialitate. Industria din ziua de astăzi şi organizațiile guvernamentale subliniază securitatea cibernetică şi asigurarea confidențialității ca fiind priorități de top al domeniului IT. Amenințările online sunt prezentate atât de persoane fizice, cât şi de grupuri organizate cu intenții de realizare a unor furturi de secrete comerciale, acțiuni de perturbare şi invazie a sistemelor în scopuri activiste şi de spionaj.
Cuvinte cheie: Internetul Lucrurilor, securitate, confidențialitate

Abstract: As a result of future research on networks, a new technology called the Internet of Things has been created, which aims to create new values through the exchange of information and knowledge between people and objects. This technology is different from its predecessors (Traditional Internet, Mobile Internet, Sensor Network etc.), focusing in particular on ubiquitous service models, heterogeneous network architectures and universal access for people, things, objects and processes. Innovations and future research on IoT applications and services are

[1] Universitatea „Alexandru Ioan Cuza" Iaşi, Facultatea de Economie şi Administrare a Afacerilor, Iaşi, Romania, mirceag@uaic.ro, roxana_hucanu@yahoo.com

driven by the high potential for market and profit. However, IoT proposes new areas to study vulnerability in system security and more difficult confidentiality issues. Today's industry and government organizations underline cyber security and privacy as top IT priorities. Online threats are presented by both individuals and groups organized with intent to commit commercial theft, disturbance actions and invasion of systems for activist and espionage purposes.
Keywords: Internet of Things, Security, Data Privacy

1. Introducere

„Internet of Things" (abv. IoT), în traducere din limba engleză, Internetul Lucrurilor sau Internetul Obiectelor, reprezintă o lume fascinantă în care lucruri obişnuite din viața de zi cu zi sunt conectate la Internet. În cadrul acestei lumi digitale, senzorii şi dispozitivele de comunicații sunt integrate în lucruri fizice cu scopul de a facilita comunicarea între lucruri sau între lucruri şi ale dispozitive precum servere cloud, calculatoare, telefoane inteligente şi tablete. Potrivit companiei Cisco Internet Business Solutions Group (IBSG), Internetul Lucrurilor reprezintă acea perioadă de timp în care există mai multe obiecte conectate la Internet decât oameni[2].

Termenul „Internet of Things" a fost utilizat pentru prima dată în cadrul laboratorului MIT[3] în anul 1999, de către Kevin Ashton, cu scopul de a ilustra puterea de conectare a etichetelor RFID[4] utilizate în lanțuri de aprovizionare pentru a controla stocurile de bunuri fără a fi nevoie de intervenție umană[5]. În contextul actual, Internetul Lucrurilor se referă la dispozitive care au un grad înalt de conectivitate, la sisteme şi servicii care interacționează unele cu altele şi acoperă o gamă largă de protocoale, domenii şi aplicații. Putem aduce în discuție o multitudine de arii de aplicabilitate, printre care se numără: energia, transport, clădiri, locuințe, sănătate, oraşe, vânzări, agricultură şi altele. De exemplu, ne putem gândi la o casa inteligentă din viitor, ce presupune pornirea automată a televizorului pe un canal preferat sau a muzicii ambientale atunci când telefonul inteligent al proprietarului sau utilizatorului înregistrat în aplicațiile inteligente specifice casei inteligente, va părăsi automobilul sau va intra pe uşa casei.

[2] D. Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, s.l.: Cisco Internet Business Solutions Group (IBSG), 2011.
[3] MIT – Massachusetts Institute of Technology.
[4] RFID – Radio Frequency Identification.
[5] K. Ashton, *That 'Internet of Things' Thing*, 2009, [Online] la: http://www.rfidjournal.com/articles/view?4986, accesat la 30.08.2017.

Telefonul va fi în permanență conectat la Internet şi va comunica cu sistemul automatizat de acasă. Acesta poate iniția anumite protocoale, precum deschiderea uşilor sau iluminarea automată prin aprinderea becurilor din încăperi. Sau, de exemplu, am putea folosi unele dispozitive precum brățările de fitness pentru măsurarea frecvenței cardiace şi a temperaturii şi să comunicăm mai apoi sistemului automatizat al casei toate aceste informații pentru a crea o temperatură ideală în camere, în funcție de informațiile obținute. Informațiile obținute pot fi împărtăşite cu diferite părți interesate şi folosite în luarea deciziilor sau pentru îmbunătățirea informațiilor de afaceri.

Utilizarea acestei tehnologii a condus către o îmbunătățire a vieții noastre de zi cu zi, ajutându-ne la şi uşurându-ne totodată realizarea sarcinilor zilnice. Însă folosirea acestei tehnologii vine şi cu părți mai puțin bune, printre care se numără invizibilitatea colectării datelor, fapt ce poate conduce la o sacrificare a confidențialității utilizatorilor tehnologiei Internetului Lucrurilor[6]. Prin utilizarea acestei tehnologii viața ne este îmbunătățită şi realizarea sarcinilor de zi cu zi este cu mult uşurată. Însă odată cu toate aceste beneficii, ea vine şi cu părți mai puțin bune, printre care se numără şi invizibilitatea colectării datelor, rezultând o sacrificare majoră a confidențialității[7]. Odată cu utilizarea aplicațiilor şi serviciilor se aşteaptă de la furnizorii serviciilor o livrare automată a serviciilor personalizate pe baza informațiilor colectate de la aplicațiile utilizate, protejarea informațiilor de acces neautorizat şi nedistribuirea acelor date cu persoane terțe[8].

Existența şi utilizarea aplicațiilor IoT determină crearea unor provocări privind securitatea întregului ecosistem al IoT, din motive legate de extinderea „Internetului" prin rețeaua tradițională (Internet, rețea de date celulare, rețea de senzori), conectarea la rețea a obiectelor datorită faptului că fiecare obiect va fi conectat la Internet şi a comunicării dintre obiecte. Compania Gartner plasează securitatea în fruntea listei sale de top 10 tehnologii IoT pentru 2017 şi 2018, afirmând faptul că securitea IoT va fi complicată de faptul că multe „lucruri" utilizează procesoare simple şi

[6] G.A. Fink, D.V. Zarzhitsky, T.E. Carroll, E.D. Farquhar, *Security and privacy grand challenges for the internet of things. In Collaboration Technologies and Systems (CTS)*, International Conference on, 2015, pp. 27–34.

[7] Ibidem.

[8] G. Sun, S. Huang, Y. Yang, Z. Wang, *A privacy protection policy combined with privacy homomorphism in the Internet of Things. Computer Communication and Networks (ICCCN)*, 23rd International Conference on, 4-7 08, 2014, pp. 1-6.

sisteme de operare care nu ar putea să sprijine abordări sofisticate[9]. Prin urmare, ar trebui acordată o mai mare atenție către chestiunilor de cercetare privind confidențialitatea, autenticitatea şi integritatea datelor în Internetul Lucrurilor.

2. Considerații privind securitatea şi confidențialitatea datelor generate de IoT

Întrucât ne bazăm pe dispozitive conectate pentru a ne face viața mai uşoară, trebuie să luăm în considerare un aspect foarte important şi anume, securitatea. Securitatea este definită ca fiind un set de mecanisme întreprinse pentru a proteja datele sensibile la atacuri cibernetice şi pentru a garanta confidențialitatea, integritatea şi autenticitatea datelor. Toți participanții din ecosistemul IoT trebuie să-şi asume responsabilitatea privind securitatea datelor, a dispozitivelor şi serviciilor oferite prin implementarea şi respectarea celor mai bune practici[10].

2.1. Elemente arhitecturale specifice securității

Înaintea altor discuții privind securitatea, se impune realizarea unei descrieri şi analize a arhitecturii securității. Arhitectura este compusă din patru niveluri: aplicație, rețea, suport şi percepție (vezi Figura 1). În unele sisteme, nivelul de procesare este reprezentat de tehnologiile de suport ale rețelei, cele precum middleware, computing, network processing[11].

[9] O. David, *Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018*, [Online] la: https://www.iotcentral.io/blog/gartner-identifies-the-top-10-internet-of-things-technologies-for.

[10] K. Sarah, *9 IoT Security Threats To Watch*, [Online] la: http://www.crn.com/slide-shows/internet-of-things/300089496/black-hat-2017-9-iot-security-threats-to-watch.htm/pgno/0/2, accesat la 30.09.2017.

[11] K. Zhao, L. Ge, *A survey on the internet of things security*, în Proceedings – 9th International Conference on Computational Intelligence and Security, CIS 2013, 14 12, pp. 663-667.

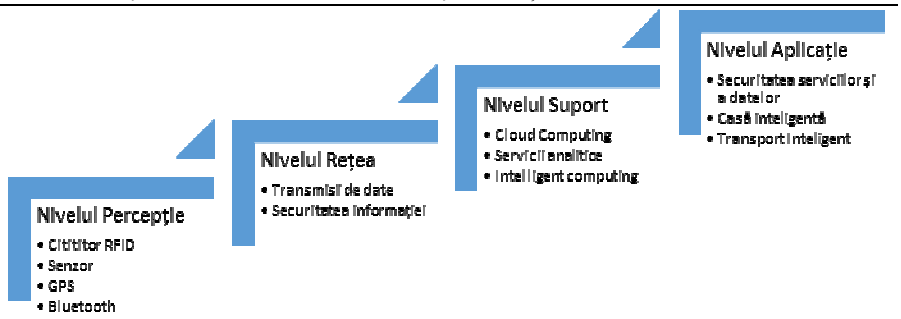

Figura 1. Arhitectura securității IoT

A. *Percepție*

Toate informațiile din lumea reală sunt colectate prin intermediul nivelului percepție utilizând dispozitive fizice ce au integrate senzori, etichete RFID, sisteme GPS și echipamente bluetooth. Datele colectate conțin informații cu privire la proprietățile obiectelor, condițiile de mediu și altele. Senzorii reprezintă factori cheie pentru acest nivel, fiind utilizați în capturarea datelor și transformarea lumii reale, fizice într-o lume digitală.

- *Caracteristici de securitate:* Nivelurile de percepție sunt foarte simple, cu capacități de stocare mici și putere de calcul relativ mică. Din acest motiv este foarte greu să se creeze un sistem de securitate prin care să se realizeze o protecție eficientă a acestuia, determinând apariția unor probleme de comunicare și imposibilitatea aplicării unor algoritmi de criptare a cheilor publice. Datele obținute de la senzori necesită protecție din punct de vedere al integrității, confidențialității și autenticității.
- *Cerințe de securitate:* La acest nivel, autentificarea este folosită cu scopul de a asigura confidențialitatea transmiterii datelor dintre nivele și pentru a preveni accesul ilegal, în acest fel procesul de criptare al datelor devenind necesar.

B. *Rețea*

Împreună cu procesarea inițială a datelor preluate din stratul de percepție este realizată transmiterea fiabilă a datelor, clasificarea informațiilor și polimerizarea. Transmiterea informațiilor se bazează pe câteva rețele de bază, esențiale pentru schimbul de informații realizat dintre

dispozitive, rețele (precum internet, acele rețele „fără fir”, sateliți, comunicații mobile), infrastructura de rețea şi protocoale de comunicații.

- *Caracteristici de securitate:* Mecanismul de securitate al acestui strat este unul de mare importanță pentru Internetul Lucrurilor. Chiar dacă rețeaua centrală este relativ sigură, atacurile de interceptare de genul „Man-In-The-Middle”, mesajele contrafăcute, mail-uri de tip spam şi viruşii de calculator încă cauzează pagube mari ce nu pot fi ignorate, întrucât numărul mare de trimiteri de date provoacă aglomerație în rețea.
- *Cerințe de securitate:* Mecanismele de autentificare (pentru a preveni noduri ilegale), confidențialitatea şi integritatea sunt utilizate pentru a asigura securitatea la acest nivel. Un atac special care este foarte grav şi reprezintă o problemă care trebuie rezolvată la acest nivel este atacul DdoS[12] [13].

C. Suport

După ce informațiile trec prin nivelul rețea, acestea urmează să fie preluate de către nivelul percepție al cărui scop este de a oferi o gamă largă de competențe computerizate inteligente, organizându-le cu ajutorul rețelelor grid network şi cloud computing, cu scopul de a crea o platforma fiabilă pentru sprijinirea nivelului aplicație. Acest nivel joacă un rol de punte între nivelul de sus şi cel de jos.

- *Caracteristici de securitate:* Recunoaşterea informațiilor rău intenționate reprezintă o provocare pentru acest strat, datorită faptului că stratul de suport lucrează cu prelucrarea în masă a datelor şi deciziile inteligente.
- *Cerințe de securitate:* Acest strat trebuie să lucreze cu o varietate de aplicații ale arhitecturii securității, plecând de la cloud computing şi până la computere securizate multi-party, colaborând cu aproape toate protocoalele şi toți algoritmii puternici de criptare, tehnologii de securitate ale sistemului puternice şi soluții anti-virus.

[12] DdoS – Distributed Denial of Service reprezintă o încercare de a face indisponibil un serviciu online prin copleşirea acestuia cu trafic din mai multe surse. Acestea vizează o gamă largă de resurse importante, de la bănci la site-uri de ştiri şi reprezintă o provocare majoră pentru asigurarea faptului că omenii accesează şi publică informații importante.

[13] Digital Attack Map, 2017, [Online] la: https://www.digitalattackmap.com/understanding-ddos/, accesat la 20.10.2017.

D. *Aplicație*

Nivelul aplicație este cel mai înalt nivel, fiind un nod terminal. Datorită nevoilor utilizatorilor ce pot accesa această tehnologie IoT folosind televizorul inteligent, calculatorul personal, laptop-ul sau tableta, la acest nivel de aplicație sunt oferite servicii personalizat[14].

- *Caracteristici de securitate:* Datorită faptului că nevoile de securitate sunt diferite, în funcție de aplicația și schimbul de date ce reprezintă principala caracteristică a acestui nivel, pot apărea probleme privind confidențialitatea, controlul accesului și divulgarea informațiilor[15].
- *Cerințe de securitate:* Problemele de securitate apărute la acest nivel pot fi rezolvate prin protejarea confidențialității utilizatorului, utilizând protocoale de autentificare[16] și key-agreement[17]. De asemenea, gestionarea tuturor parolelor și a dispozitivelor ar trebui să se facă într-un mod adecvat.

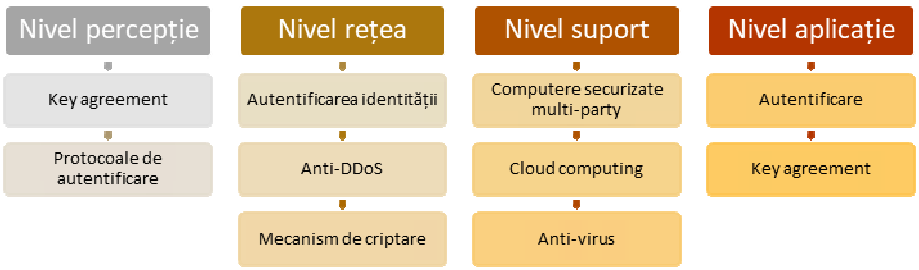

Figura 2. Cerințe specifice nivelurilor arhitecturale

2.2. Servicii de securitate

În arhitectura de securitate a procesului de transmitere a informațiilor trebuie acordată o atenție sporită pentru asigurarea garanției

[14] C. Ding, L. Yang, M. Wu, *Security architecture and key technologies for IoT/CPS*, în ZTE Technology Journal, 2017(1).

[15] Y. Geng și alții, *Security Characteristic and Technology in the Internet of Things* în Journal of Nanjing University of Posts and Telecommunications (Natural Science), 2010, 30(4).

[16] Autentificare – reprezintă procesul prin care o persoană pretinde identificarea în sistem pe baza informațiilor confidențiale stabilite la crearea contului. Acest proces mai poartă denumire de login/log in sau logon/log on.

[17] Key-agreement – reprezintă un protocol prin care două sau mai multe părți implicate pot conveni asupra unei chei partajate către toate dispozivele care vor accesa rețeaua fără fir.

confidențialității, integrității, intimității, autenticității şi instantaneității datelor şi informațiilor ce fac referire în principiu la securizarea rețelelor de telecomunicații şi corespund securității ierarhiei de transmisie a datelor în Internetul obiectelor[18]. Aceste cerințe pot fi observate în Figura 3.

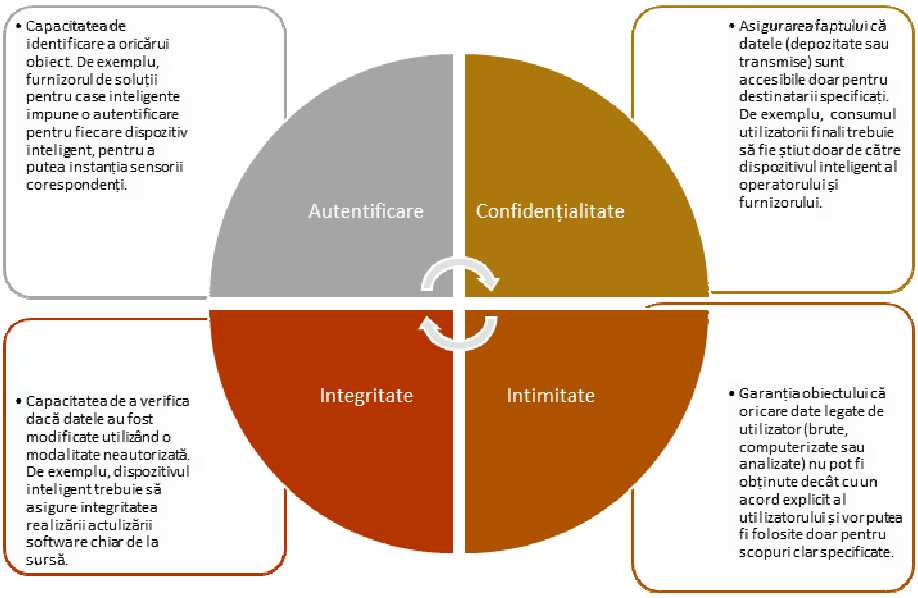

Figura 3. Servicii de securitate ale Internetului Lucrurilor

În acest context, confidențialitatea reprezintă un set de reguli care limitează accesul la informații, integritatea fiind o asigurare a faptului că informațiile sunt exacte şi de încredere, intimitatea – garanția pe care utilizatorii o întreține pentru datele lor sensibile, iar autentificarea este o garanție a accesului fiabil la informații a persoanelor autorizate. Dintre toate cerințele descrise anterior, considerăm că ar trebui să primeze respectarea confidențialității, întrucât aceasta reprezentă un mijloc de protecție a informațiilor care se desfăşoară prin orice mijloc între două părți.

2.3. Provocări privind confidențialitatea

Unele dispozitive inteligente sunt dezvoltate cu scopul de a crea, colecta sau partaja date. Prin urmare, aceste date nu pot fi considerate a fi „date cu caracter personal” şi nu au nici un impact asupra confidențialității

[18] L. Li, *Study on security architecture in the Internet of Things. Measurement, Information and Control (MIC)*, 2012 International Conference on, Volumul 1, pp. 374-377.

sau intimității consumatorilor, nefăcând legătură la legile privind protecția confidențialităților și a datelor. De exemplu, pot fi incluse în această categorie date ce fac referire la starea fizică a mașinilor, la metrici privind starea rețelei sau de diagnosticare internă[19].

Majoritatea serviciilor folosite în Internetul Lucrurilor fac însă referire la crearea și distribuirea datelor cu caracter personal legate de consumatori individuali și care pot avea un impact asupra confidențialității consumatorului, fiind legate de legislația generală de protecție a datelor și confidențialității (vezi Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date). De exemplu, se pot crea analize privind starea de sănătate sau profilul consumatorului în funcție de obiceiurile de cumpărături și de supermarket-urile preferate, cele mai vizitate.

Toți participanții din ecosistemul IoT au obligația de a respecta confidențialitatea persoanelor și de a păstra în siguranță datele personale de identificare. O provocare majoră pentru furnizorii de aplicații IoT este cauzată de legi multiple și adesea inconsistente, legate de confidențialitate și protecția datelor, legi care pot fi aplicate în mod diferit în funcție de sectorul industrial, servicii și tipuri de date implicite în diferite țări. Să luăm exemplul unei mașini inteligente ce călătorește în diferite țări, prin urmare transferurile de date asociate pot fi guvernate de fiecare țară în care mașina trece, folosind diferite jurisdicții legale. Datele obținute de la senzorii instalați în mașină (folosiți pentru a urmări locația mașinii) pot fi folosite pentru a deduce o serie de informații despre locurile frecventate și preferate de către șofer, stilul de viață al acestuia sau hobby-urile, date care pot fi considerate informații personale despre utilizatorul. De asemenea, aceste informații obținute prin intermediul senzorilor de „diagnoză la bord” ar putea fi împărtășite cu societățile de asigurări ce pot utiliza aceste informații pentru a impune o primă mai mare și, prin urmare, să discrimineze conducătorul auto fără cunoștința lui.

O altă provocare este reprezentată de faptul că cele mai multe legi privind protecția datelor solicită societăților (care colectează datele consumatorilor) să obțină consimțământul consumatorului afectat (cunoscut și sub denumirea de „persoana vizată”) înainte de a procesa anumite

[19] T. Victor, *Internet of Things future forecasts: focus on IoT security*, [Online] la: https://www.i-scoop.eu/internet-of-things-guide/iot-security-forecasts/, accesat la 10.10.2017.

categorii de „date cu caracter personal” – cum ar fi datele referitoare la sănătate. Majoritatea legilor definesc „datele personale” ca fiind orice informație ce se referă la o persoană fizică vie (identificată) sau „identificabilă”[20]. Pe măsură ce tot mai multe dispozitive sunt conectate la Internet şi numărul acesta este în creştere[21], tot mai multe date despre persoane vor fi colectate şi analizate şi eventual vor afecta intimitatea lor, fără a fi în mod necesar considerate „date cu caracter personal” prin lege. Se pot obține profiluri detaliate ale utilizatorilor prin combinarea volumelor masive de date, a datelor mari, a stocării în cloud şi a analizelor predictive.

3. Analiza cerințelor de securitate a aplicațiilor din domeniul medical

În acest caz, ne propunem să studiem un Dispozitiv de Monitorizare a ritmului cardiac portabil (dispozitiv de punct final) ce reprezintă un dispozitiv simplu folosit pentru măsurarea şi înregistrarea frecvenței cardiace a utilizatorului, cu scopul de a oferi unele indicații pentru o mai bună securizare a dispozitivului.

Figura 4. Dispozitiv de monitorizare a ritmului cardiac

Dispozitivul a fost dezvoltat cu intenția de urmărire de către utilizatorul final a pulsului pe parcursul zilei, stocându-l atât în aplicație, cât şi în baza de date back-end. Intenția este de a permite utilizatorilor să-şi

[20] S. Gib, *Upcoming IoT regulations and laws: How to survive and stay compliant*, [Online] la: http://www.ioti.com/security/upcoming-iot-regulations-and-laws-how-survive-and-stay-compliant, accesat la 20.10.2017.

[21] E. Rob, *8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, [Online] la: https://www.gartner.com/newsroom/id/3598917, accesat la 02.09.2017.

revizuiască valorile ritmul cardiac în timp pentru a-şi urmări sănătatea generală. Utilizatorii pot viziona îmbunătățirea sau agravarea sănătății lor în timp, în funcție de menținerea unui stil de viață sănătos. Acest lucru permite utilizatorilor să se stimuleze prin evaluarea atât a tendințelor pozitive, cât şi a celor negative citite din datele lor stocate în dispozitivul de monitorizare. Datele pot fi de asemenea utilizate de parteneri pentru a interveni în cazul apariției unor evenimente legate de sănătatea utilizatorului, precum atac de cord sau accident vascular cerebral.

3.1. Privire de ansamblu asupra dispozitivului

În Figura 4 se poate observa care este structura generală, precum şi componența unui dispozitiv simplu de urmărire a ritmului cardiac[22].

Dispozitivul simplu de urmărire a ritmului cardiac este compus din următoarele componente:

- Un emițător cu emisie redusă de energie Bluetooth (BLE) – ce asigură conectivitate fără fir (wireless);
- Microcontroler (MCU) activat pentru BLE – ce are obligația de a analiza datele emise de senzor şi de a alege ce date trebuie transmise prin transmițătorul BLE;
- Un senzor fotografic de lumină ambientală – folosit pentru a captura datele privind frecvența pulsului.

În acest exemplu, folosim o baterie de tip monedă pentru a facilita transmiterea datelor între dispozitive, de la dispozitivul portabil la tabletă, laptop sau smartphone.

3.2. Privire de ansamblu asupra serviciilor

Din perspectiva serviciilor, aplicația poate fi disponibilă pe telefonul inteligent, calculatorul personal sau tabletă, cu scopul de a transmite valorile capturate de la punctul final (în cazul nostru, dispozitivul de monitorizare) către punctul de serviciu final folosind orice conexiune de rețea disponibilă. Punctul de serviciu final pentru aplicație asociază pur şi simplu proprietarul dispozitivului cu valorile capturate şi le stochează într-o bază de date locală a serverului de aplicații. Datele pot fi vizualizate utilizând aplicația mobilă sau utilizând un browser pentru a accesa site-ul

[22] V. Mark, *Wearables Technology Components*, [Online] la: https://www.digikey.com/en/product-highlight/p/panasonic/wearable-technology, accesat la 15.10.2017.

web al serviciului. Pe site-urile furnizorului de servicii, utilizatorii pot vizualiza şi utiliza valorile capturate pentru a efectua mai multe acțiuni (Figura 5).

Figura 5. Fluxul de date al punctului de serviciu final

3.3. Model de securitate

Din ce am observat mai sus, la dispozitivul urmărit, cele mai comune probleme pot apărea atât datorită produsului, cât şi a serviciului utilizat.

Din perspectiva produsului, probleme pot apărea datorită următorilor factori:

- Clonare;
- Personalizarea produsului;
- Personalizarea serviciului;
- Asigurarea confidențialității.

Din perspectiva produsului, probleme pot apărea datorită următorilor factori:

- Clonare;
- Atacarea serviciilor;
- Identificarea comportamentului anormal al punctului final;
- Limitarea compromisului;
- Reducerea pierderii datelor;
- Reducerea exploatării;

- Gestionarea confidențialității utilizatorilor;
- Îmbunătățirea disponibilității datelor.

Având în vedere faptul că dispozitivul de monitorizare are foarte puține funcționalități, putem implementa o securitate minimă asupra punctului final, atât pentru securitatea aplicațiilor, cât și pentru comunicare. Deoarece aplicația specifică sistemului de monitorizare a ritmului cardiac este afișată pe un singur dispozitiv, atât timp cât firmware-ul dispozitivului este blocat, nu există nicio amenințare reală de atac împotriva punctului final în cazul utilizării de date. Deoarece confidențialitatea reprezintă o problemă, trebuie să luăm în considerare cel puțin utilizarea unei autentificări, cu o versiune PSK[23] personalizată a unei baze de calcul de încredere. Acest lucru ar asigura faptul că cheile de criptare sunt unice pentru fiecare punct final, astfel încât un punct final compromis nu poate compromite toate celelalte punctele finale. Dacă cheile personalizate (unice) au fost codificate în microcontrolerul încuiat, ar fi rezonabil să credem că acest caz de utilizare a fost asigurat în mod adecvat de amenințarea cu clonarea, personalizare și problemele de confidențialitate.

Din perspectiva infrastructurii de server, lucrurile sunt diferite, deoarece trebuie să ne asigurăm că:

- Există o securitate front-end care să diminueze efectele unui atac Denial of Service;
- Se impune exercitarea unor controale pentru a limita traficul către sau de la servicii;
- Datoriile din straturile de servicii sunt bine delimitate;
- Asigurăm crearea unei baze de date securizate cu jetoane personalizate PSK;
- Sunt definite măsuri de securitate în sistemul de operare al serviciului;
- Sunt definite valorile pentru evaluarea comportamentul anormal al punctului final.

Sistemul poate fi mai sigur dacă luăm în considerare considerațiile expuse și poate aduce unele modificări simple și eficiente din punctul de vedere al obiectivului, asigurând astfel tehnologia fără a schimba arhitectura. Confidențialitatea este asigurată prin acordarea fiecărui jalon criptografic unic.

[23] Pre-Shared key (PSK) – Cheie de criptare pre-partajată

Concluzii

Internetul obiectelor reprezintă un salt important către o conexiune globală şi generalizată folosită de către orice obiect/dispozitiv de comunicație şi de calcul, indiferent de tehnologia lui de acces, resurse şi locație disponibilă. Securitatea este principala preocupare pentru IoT, împreună cu confidențialitatea datelor, deoarece punerea în aplicare a internetului on-line la scară globală afectează miliarde de persoane şi dispozitive.

În această lucrare am analizat pe scurt principalele probleme de securitate şi provocări pentru Internetul obiectelor cu exemplificare pe domeniul medical şi am analizat din punct de vedere teoretic şi practic un dispozitiv inteligent cu scopul de a furniza unele indicații privind asigurarea unui dispozitiv de tip punct final.